HX2 Reference Guide

(Microsoft® Windows® CE 5.0 Equipped)

Notices

LXE Inc. reserves the right to make improvements or changes in the products described in this guide at any time without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, LXE assumes no liability resulting from any errors or omissions in this document, or from the use of the information contained herein. Further, LXE Incorporated, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Copyright:

This document is copyrighted. All -*ghts are reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form without prior consent, in writing, from LXE Inc.

Copyright © 2007 by LXE Inc. An EMS Technologies Company.
125 Technology Parkway, Norcross, GA 30092 U.S.A. (770) 447-4224

Trademarks:

LXE® and **Spire**® are registered trademarks of LXE Inc. **RFTerm**® is a registered trademark of EMS Technologies Company.

Summit Data Communications, the Summit logo, and "The Pinnacle of Performance" are trademarks of Summit Data Communications, Inc.

Microsoft®, Windows® and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA® and the Stylized M Logo are registered trademarks of **Motorola**®, Inc.

Java® and Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. or other countries, and are used under license.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Wavelink® and Wavelink Avalanche® are registered trademarks and the Wavelink logo, tagline and Avalanche MC are trademarks of Wavelink Corporation, Kirkland, WA.

The **Bluetooth**® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by LXE, Inc. is under license.

PowerScan® is a registered trademark of Datalogic Scanning, Inc., located in Eugene, OR.

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

When this document is in PDF format: "**Acrobat** ® Reader Copyright © 2007 Adobe Systems Incorporated. All rights reserved. Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated" applies.

Important: This symbol is placed on the product to remind users to dispose of Waste Electrical and Electronic Equipment (WEEE) appropriately, per Directive 2002-96-EC. In most areas, this product can be recycled, reclaimed and re-used when properly discarded. Do not discard labeled units with trash. For information about proper disposal, contact LXE through your local sales representative, or visit www lxe com.

Revision Notice

Chapter 1 – Introduction	Updated *Strap Assemblies*. Replaced *Using the 23 Key Keypad* with *HX2 Keypads*. Added *Adjusting the Display Brightness*. Added Ring Scanner Strap Kit, Trigger Assembly 20 pack, and Bluetooth Mobile Barcode Readers to *Accessories*.
Chapter 2 – Physical Description and Layout	Updated Cradle LED indicator segment.
Chapter 3 – System Configuration	Updated Wavelink Avalanche naming conventions in *Wavelink Avalanche Enabler* and *Wavelink Avalanche Enabler Configuration*. Updated *Keypad* section to include keypad control panel options for three keypad configurations. Updated *GrabTime* section. Updated *Bluetooth* sections.
Chapter 4 – Scanner	Added *Length Based Barcode Stripping* instruction.
Chapter 5 – Wireless Network Configuration	Added *EAP-TLS* instruction. Updated *Summit Client Utility* to reflect version differences.
Chapter 6 – AppLock	Added keypress instructions for the Alpha Mode 3 Tap (the original), Dual Alpha and Triple Tap keypads.
Appendix A – Key Maps	Added *Alpha Mode 3 Tap Keypad*, *Dual Alpha Keypad* and *Triple Tap Keypad* keymaps. Added Display Brightness to Alpha Mode 3 Tap keypad.
Appendix B – Technical Specifications	Updated HX2 physical dimensions.
Entire Guide	Added keyed instructions for the Alpha Mode 3 Tap (the original keypad), Dual Alpha and Triple Tap keypads where applicable. Updated *LXEZ Pairing* and Bluetooth instruction where applicable.

Table of Contents

Illustrations

Chapter 1 Introduction

Overview

The LXE® HX2 is a small, lightweight mobile computer designed to be worn on a person's arm or waist. The HX2 is most useful for applications that require computational support while the user's hands are actively engaged with the physical environment, including piece picking to carts, containers or conveyers; case picking; parcel moves; and broken case activities.

The armbands that secure both the unit and its battery keeps the HX2 in the ready position at all times by preventing the unit from rotating around the wearer's arm. The adaptable armbands can be worn close to the elbow or near the wrist.

The primary data inputs are a keypad or a ring scanner. The HX2 is voice ready. Voice can also be used as an input with 3rd party software. Output is presented using the screen display or audio feedback generated by the mobile device and delivered through an internal speaker or audio headset.

The HX2 is powered by a tethered low profile, light and unobtrusive battery. The entire HX2 wearable computer system features breakaway connections at multiple points and a low-profile, smooth design to resist snagging on common warehouse fixtures and equipment.

The HX2 has a Microsoft® Windows® CE 5.0 operating system with an Intel® XScale® PXA255 CPU. The HX2 supports an 802.11b/g WLAN radio and *Bluetooth*® 2.0+EDR radio.

Connectors are available which interface with peripherals such as a Ring Scanner (1D Laser and 2D Imager Ring Scanner), an audio headset, a docking/charging cradle and a tethered battery (see *Components* for port locations).

The QVGA color display with a touch panel has a diagonal viewing area of 2.5" (6.3 cm) in landscape orientation. The display backlight brightness can be adjusted using a series of keypresses. The keypad backlight can be either on or off. The keypad keys can be programmed to perform multi-key functions.

The HX2 hip flip holster, voice case, rubber boot, powered cradle, touchscreen stylus and protective film for the screen are available from LXE as accessories (see *Accessories*).

Note: *Until the tethered battery and backup battery are completely depleted, the HX2 is always drawing power from the batteries (On).*

Note: *If the mobile device has AppLock installed, please refer to Chapter 6 – AppLock for setup and processing information before continuing.*

When to Use This Guide

As the reference for LXE's HX2 computer, this guide provides detailed information on its features and functionality. Use this reference guide as you would any other source book – reading portions to learn about the HX2, and then referring to it when you need more information about a particular subject. This guide takes you through all aspects of installation and configuration for the LXE HX2. Daily operation, installation and safety instructions for the general user are covered in the *HX2 User's Guide*.

This chapter, **"Introduction",** describes this reference guide's structure, describes HX2 components, contains initial setup instruction, briefly describes data entry processes, and explains how to get help. Bluetooth pairing instruction is included.

Chapter 2 "Physical Description and Layout", describes the function and layout of the HX2, controls and connectors. Also describes the power supplies and docking options for the HX2.

Chapter 3 "System Configuration" takes you through the CE 5.0 operating system setup and the HX2 file structure. Avalanche Enabler instruction is included in this chapter.

Chapter 4 "Scanner" describes the function, layout and setup for the LXE Wedge.

Chapter 5 "Wireless Network Configuration" details 2.4GHz wireless client setup. Configuration for WEP and WPA is included.

Chapter 6 "AppLock" covers all aspects of the LXE AppLock program. A mobile device running AppLock becomes a dedicated, single or dual application device.

Appendix A "Key Maps" describes the keypress sequences for the keypad.

Appendix B "Technical Specifications" lists HX2 technical specifications.

Related Manuals

Ring Scanner Programming Guide – contains programming barcodes used when setting up scanner/imager engines in ring barcode readers.

HX2 User's Guide – contains instruction and information directed to the daily HX2 user.

HX2 Multicharger User's Guide – contains user, technical and troubleshooting information for the HX2 battery multi-charger.

HX2 Cradle Reference Guide – contains user, technical and troubleshooting information for the HX2 cradle.

Important Battery Information

Backup Battery -- If the HX2 has been without a power source (connected to a fully charged tethered battery or docked in a powered cradle) for an extended period of time or if HX2 external power sources become completely discharged or dead, a fully charged HX2 backup battery will last for up to 15 minutes. If the backup battery is fully discharged, the HX2 will reset as soon as it is docked in a powered cradle, and the Power button is pressed, or connected to a fully charged tethered battery. A reset will cause loss of data and custom programs in RAM . Always store unused HX2s with a fully charged tethered battery. If possible, ensure the HX2 is periodically docked in a powered cradle to maintain an optimum backup battery charged status.

To check battery status tap ⊞ | **Settings** | **Control Panel** | **Battery** tab.

- Until the tethered battery and backup battery are completely depleted, the HX2 is always drawing power from the batteries (On).
- New Standard / Extended batteries must be fully charged prior to use.
- Whenever possible, place the HX2 in a powered cradle to conserve tethered battery power and recharge the backup battery.
- When a new battery is tethered to the HX2 for the first time (or after the backup battery is depleted), the Time and Date reverts to factory default values.
- Backup battery replacement is performed by LXE.

The HX2 cradle can charge two standard batteries in less than four hours or two extended batteries in less than 8 hours in the battery wells behind the HX2 docking bay. The cradle requires an external power source before battery charging can occur.

The HX2 Multi-Charger can charge up to six batteries at the same time. Each charging bay can accept either battery. The Multi-Charger requires an external power source before charging/analyzing can occur.

Li-Ion Battery

When disposing of the HX2 tethered batteries, the following precautions should be observed: The battery should be disposed of properly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

Document Conventions

ALL CAPS	All caps are used to represent disk directories, file names, and application names.
Menu | Choice	Rather than use the phrase "choose the Save command from the File menu", this manual uses the convention "choose File | Save".
Italics	Indicates the title of a book, chapter or a section within a chapter (*for example, Document Conventions and Document Conventions*).
< >	Indicates a key on the keypad (for example, <Enter> or **Enter**).
	Indicates a reference to other documentation.
ATTENTION	Keyword that indicates vital or pivotal information to follow.
⚠	Attention symbol that indicates vital or pivotal information to follow. Also, when marked on product, means to refer to the manual or user's guide.
⏛	International fuse replacement symbol. When marked on the product, the label includes fuse ratings in volts (v) and amperes (a) for the product.
Note:	Keyword that indicates immediately relevant information.
CAUTION ⚠	Keyword that indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
WARNING ⚠	Keyword that indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
DANGER ⚠	Keyword that indicates a imminent hazardous situation which, if not avoided, will result in death or serious injury.

Getting Started

> *Note:* *The sequence of steps in <u>Getting Started</u> must also be completed when the HX2 returns from a Cold Boot and when a new OS version is loaded. The wireless client, flash card, virtual keyboard and scanner parameters may also need to be reset after a cold reset.*

This section's instructions are based on the assumption that your new device is pre-configured and requires only accessory installation (e.g. stylus, headset, ring scanner, etc.) and a battery. LXE recommends that installation or removal of accessories be performed on a clean, well-lit surface. When necessary, protect the work surface, the mobile device, and components from electrostatic discharge.

Prerequisites

- A fully charged battery is available.
- Optional add-on devices are available (e.g. stylus, headset, ring scanner, hip flip, armband).
- Wireless Client configuration has been completed by the System Administrator.
- Required configured (mappable) keys have been assigned by the System Administrator. For example, the Alpha Mode 3 Tap keypad (the original keypad) does not have a ⊞ button, Control, Shift, Alt or Del key (or the equivalent). Key mapping can be changed to map those specific keys if needed. Refer to Components – Front.
- Optional software and LXE applications have been installed and setup by the System Administrator. If AppLock is installed, and the Dual Alpha or Triple Tap keypad are in use, the AppLock default Administrator Hotkey has been modified.

HX2 Quick Start

1. Mount the armband or the hip flip first (see *Wearable Device Assembly*).
2. Insert the battery in the armband or hip flip battery sleeve.
3. Attach the ring scanner to the HX2.
4. Connect the fully charged battery. (Always connect a fully charged battery to the mobile device at the beginning of the shift or workday.)
5. If the screen does not automatically display, tap the Power key. See *Tapping the Power Key*.
6. Locate the stylus. Calibrate the touchscreen, if necessary. See *Tapping the Touchscreen with a Stylus* and *Calibrating the Touchscreen*.
7. A white screen will appear during the bootup process until all drivers and applications are loaded and installed. Setup screens may appear and disappear while files are loading. After all files are loaded and the Desktop is displayed, adjust audio volume and other parameters if desired.
8. Set up the wireless client and network management programs. Refer to *Chapter 5 – Wireless Network Configuration*.
9. Set up Terminal Emulation parameters. Refer to the *RFTerm Reference Guide* on the LXE Manuals CD.
10. Set up mappable keys. Refer to *Chapter 3 – System Configuration*.
11. Pair Bluetooth devices. Refer to *Bluetooth* later in this chapter.
12. Set the AppLock Administrator hotkey sequence and the User task switching hotkey sequence. Refer to *Chapter 6 – AppLock*.
13. Save your settings to the Registry. Refer to *Saving Settings to the Registry* later in this chapter.

Quick Start Troubleshooting

Can't calibrate the touchscreen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts User access to running programs. Changes or modifications require Administrator access. Refer to *Chapter 6 - AppLock* for setup and processing information.
RFterm® starts after each cold reset and warm reset.	Tap File | Exit to close the RFTerm application. By default RFTerm starts after each cold reset and warm reset.
HX2 seems to lockup as soon as it is warm booted.	There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, Wavelink Avalanche management of the HX2 startup completes, and Bluetooth relationships establish or re-establish. When the desktop appears or an application begins, the HX2 is ready for use.

Setup the Keypad

See *Components – Front* later in this chapter for a graphic representation of all available keypads.

The HX2 has three keypad options:

Alpha Mode 3 Tap	The HX2 default keypad on all HX2s shipped prior to September 2007. Setup requires no user interaction.
Dual Alpha	Set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped. Setup requires no user interaction with the My Device / Windows / Dual_Alpha.reg file.
Triple Tap	Requires file activation to setup the Triple Tap keypad for daily use. Setup requires the My Device / Windows / Triple_Tap.reg file be tapped and the HX2 warmbooted. Warmboot the HX2 by tapping Start | Run and, using the virtual keyboard or SIP, type WARMBOOT. Tap OK.

Setup the Client and Network

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

See *Chapter 5 Wireless Network Configuration* for complete information.

Access Terminal Emulation Parameters

Before you make a host connection, you will, at a minimum, need to know:

- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system

to properly set up your host session.

1. Make sure the mobile client network settings are configured and functional. If you are connecting over wireless LAN (802.11b/g), make sure your mobile client is communicating with the Access Point.
2. From the ⊞ | **Programs**, run **LXE RFTerm**® or tap the **RFTerm** icon on the desktop.
3. Select **Session | Configure** from the application menu and select the "host type" that you require. This will depend on the type of host system that you are going to connect to; i.e. 3270 mainframe, AS/400 5250 server or VT host.
4. Enter the "Host Address" of the host system that you wish to connect to. This may either be a DNS name or an IP address of the host system.
5. Update the telnet port number, if your host application is configured to listen on a specific port. If not, just use the default telnet port.
6. Select **OK**
7. Select **Session | Connect** from the application menu or tap the "Connect" button on the Command Bar. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Barcode, etc., please refer to the *RFTerm Reference Guide* on the LXE Manuals CD.

Saving Settings to the Registry

The HX2 saves the registry when you:

- Tap the ⊞ | **Run** | then type **Warmboot**. Tap OK.
- Perform a Suspend / Resume function (by tapping the Power key and then tapping it again).
- Install Restart in the Start menu by ⊞ | Run | then type CTL RESTART=1 and tap the OK button. Tap ⊞ | Restart.

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g. 0 seconds)

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g. Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

When you tap the ⊞ | **Run** | then type **Coldboot** and tap the OK button, factory default registry settings are loaded during coldboot. All user changes and settings are lost.

Wearable Device Assembly

Armband

Figure 1-1 HX2 Armband, Left Arm Orientation, Ring Scanner, Audio

Prerequisite: Optional add-on devices are available.

- Fasten the armband to your left or right arm before continuing with these directions. See *Connecting the Battery and Ring Scanner*.
- Slide the battery into the battery sleeve on the armband.
- Snap all tethered devices to the connectors at the back of the HX2. See *Connecting the Battery and Ring Scanner* and *Connecting the Audio Cable and a Headset.*
- Snap the HX2 into the armband mounting bracket. See *Mounting Bracket Clips*.
- Attach the battery cable to the battery.
- Connect audio devices (see *Connecting the Audio Cable and a Headset*), if included.
- Slip the ring scanner (if included) over one of your fingers, making sure your thumb or trigger finger can easily reach the Scan button. See *Ring Scanner Strap*.
- Adjust the HX2 arm assembly for comfort. Occasionally check all connectors for stability.

The wearable computer is ready for use.

Hip Flip

The hip flip may be pre-assembled by LXE.

- Unpack the Hip Flip. Slide the belt through the loops on the Hip Flip. Do not put the hip flip on yet.
- Slide the battery into the battery sleeve on the hip flip.
- Snap all tethered devices to the connectors at the back of the HX2. See *Connecting the Battery and Ring Scanner* and *Connecting the Audio Cable and a Headset.*
- Snap the HX2 into the hip flip mounting bracket. See *Mounting Bracket Clips*.
- Attach the battery cable to the battery.
- Put the hip flip on.
- Slip the ring scanner (if included) over one of your fingers, making sure your thumb or trigger finger can easily reach the scan button. *See Ring Scanner Strap.*
- Adjust the HX2 hip assembly for comfort. Occasionally check all connectors for stability.

Figure 1-2 HX2 Hip Flip, Audio

The wearable computer is ready for use. See *Getting Started* and *Connecting the Battery and Ring Scanner* for more detailed instruction.

Ring Scanner Strap

The ring scanner finger loop is located under the ring scanner.

Pull gently on the end of the finger loop strap to separate the hook and loop fabric.

Slide your finger into the opened loop under the ring scanner.

Grasp the end of the finger loop strap and loosen, then tighten, the finger strap until the ring scanner is comfortably snug and the scan aperture is secured in the desired location.

The ring scanner has a built-in quick disconnect designed for occasional safety hazards. It is not intended for frequent, normal removal of the ring scanner from the hand.

Note: *Do not touch, push against or brace your finger on the scan aperture at any time.*

Components

> *Note:*   *The figures on the next few pages assume a fully charged tethered battery is in the battery sleeve (on an armband or hip flip) and positioned at the top of the figure.*
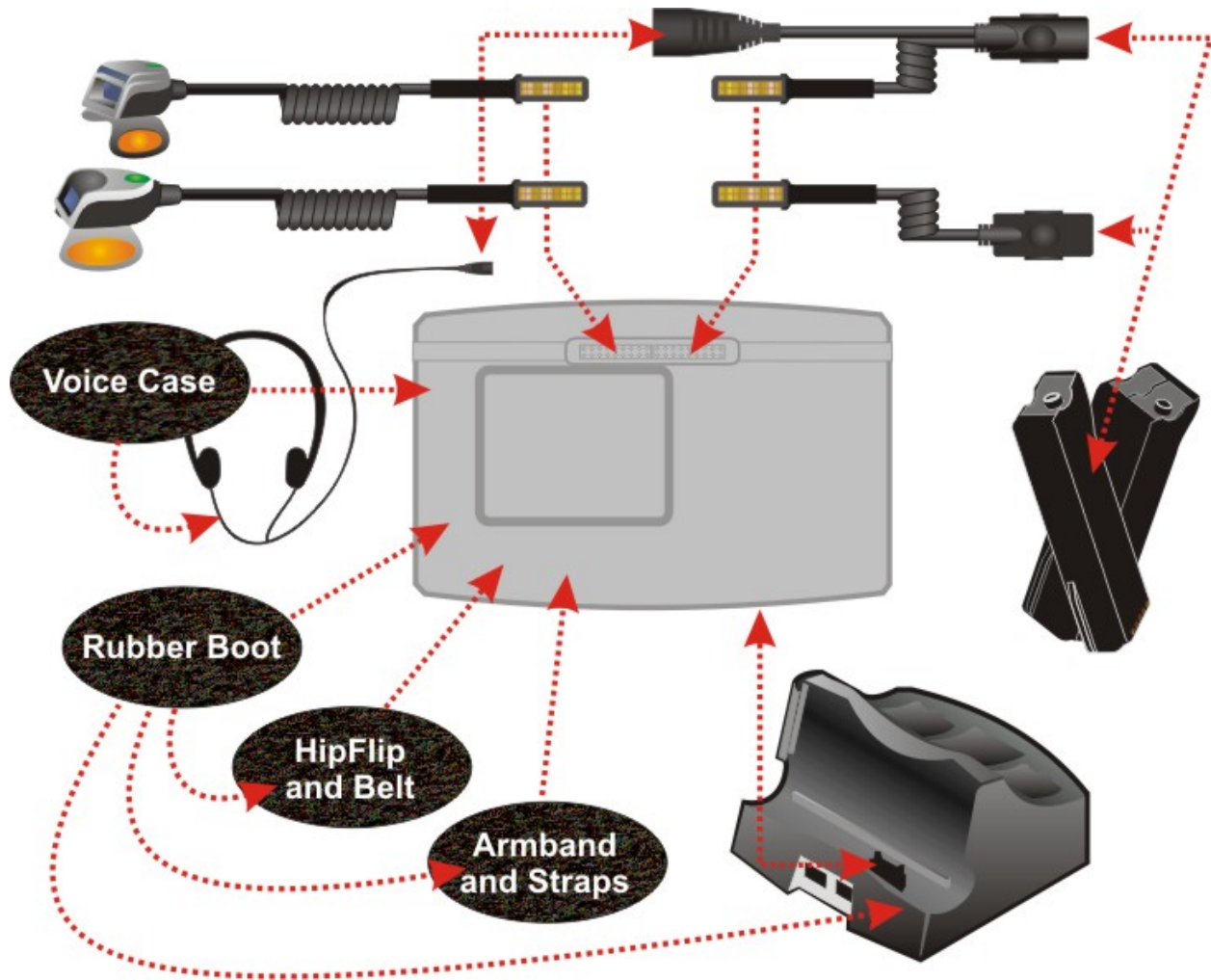
> *Note:*   *New batteries must be charged prior to use. The backup battery is continually recharged by the tethered battery.*

Front

Alpha Mode 3 Tap Keypad

Dual Alpha Keypad

Triple Tap Keypad
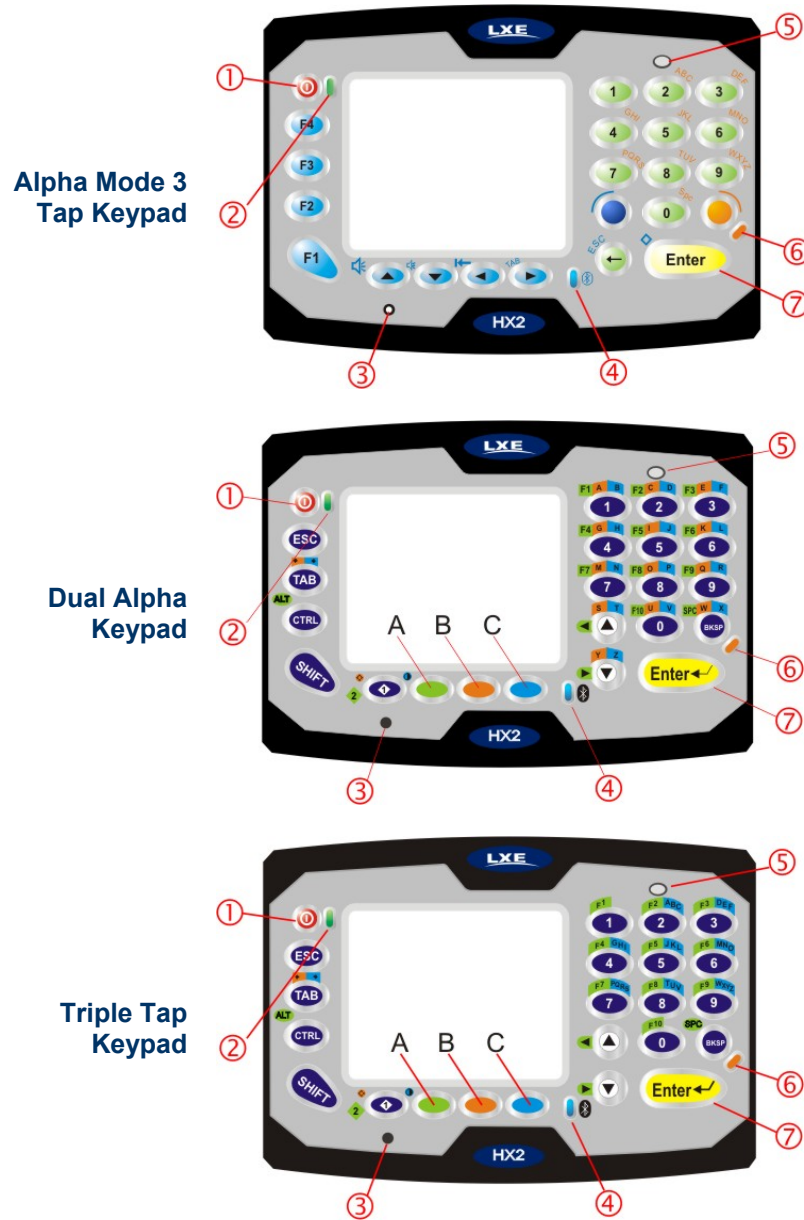
Figure 1-3 Front – Three Keypad Versions

1	On / Off Button	5	Speaker	A	Green Button
2	System Status LED	6	Alpha Mode LED[1]	B	Orange Button
3	Microphone	7	Enter Button	C	Blue Button
4	Bluetooth LED				

See Also: *System Status LEDs* and *HX2 Keypads* later in this chapter.

---

[1] Alpha Mode LED not used with the Dual Alpha Keypad and the Triple Tap Keypad.

Back

> *Note:* *Before connecting cables to the back, make sure the battery sleeve on the armband is uppermost or the left/right directions that follow won't work.*
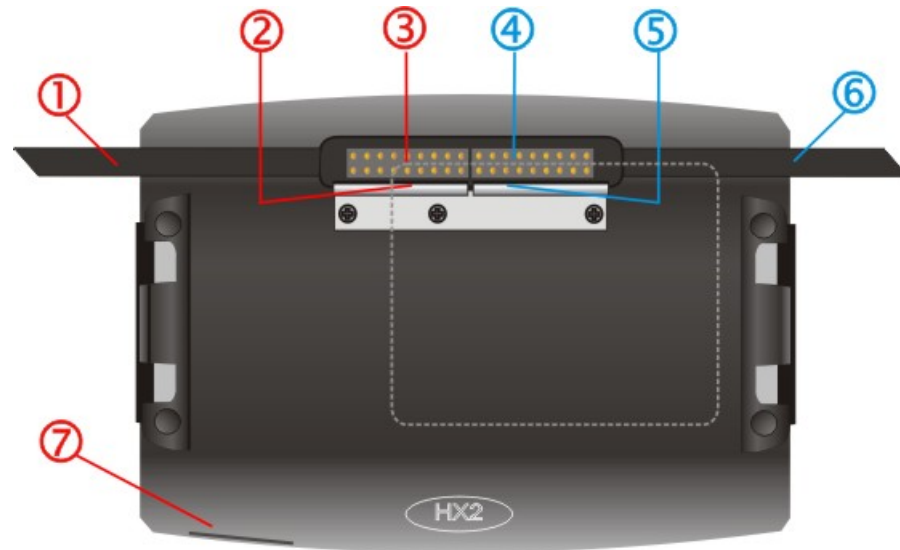
Figure 1-4 Back

Left Arm Use

1	Ring Scanner Tether cable channel
2	Retaining Clip for Ring Scanner Tether Connector
3	Ring Scanner cable connector
4	Battery Cable connector
5	Retaining Clip for Tethered Battery Connector
6	Tethered Battery Cable channel
7	Cradle Connector

Right Arm Use

1	Tethered Battery Cable channel
2	Retaining Clip for Tethered Battery Connector
3	Battery Cable connector
4	Ring Scanner cable connector
5	Retaining Clip for Ring Scanner Tether Connector
6	Ring Scanner Tether Cable channel
7	Cradle Connector

HX2 Connectors

Ring Scanner / Audio / Battery Connection

Figure 1-5 Scanner / Audio / Battery Ports – Connector 1 and 2

Connector 1	Connector 2	• Tethered Ring Scanner (Laser or Imager)
		• Tethered Headset/Microphone and HX2 Battery
		• Tethered Battery

See *Cables*.

Cradle Connection
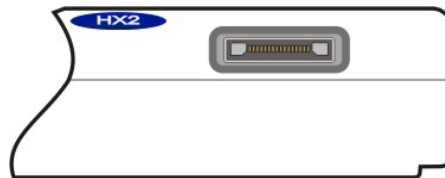
Figure 1-6 Cradle/Power Port – Connector 3

Connector 3 is at the base of the HX2. It connects to the Cradle. When the HX2 is in a powered cradle, the HX2 receives external power through the Cradle connector. USB Keyboard or USB Mouse input is received through the Cradle connector (see figure above) when the HX2 is in a cradle.

Connector 3	• Cradle
	• Cradle Power Input
	• USB Keyboard or mouse through cradle ports

See the *HX2 Cradle Reference Guide* for instruction.

Tethered Ring Scanner / Imager

Figure 1-7 Laser Ring Scanner

Figure 1-8 Imager Ring Scanner

1	Laser /Imager Scan Aperture
2	Scan-in-Progress LED
3	HX2 Connector
4	Scan button (Trigger)

Figure 1-9   Ring Scanner Hook and Loop Strap
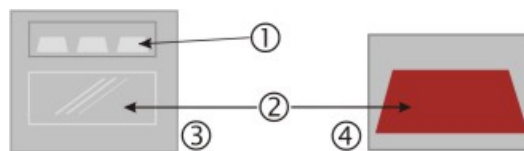
Figure 1-10 Ring Scanner/Imager Apertures

1	Imager – Illumination LEDs
2	Beam Aperture
3	Imager – Clear Glass Lens
4	Laser Scanner – Red Glass Lens

Cables

Figure 1-11 Cable – Battery and HX2 Connectors
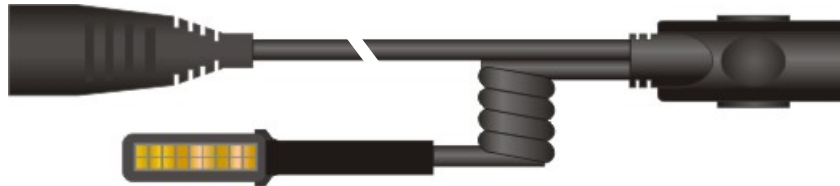
Figure 1-12 Cable – Audio, Battery and HX2 Connectors

Figure 1-13 Cable – Laser Ring Scanner and HX2 Connectors

Figure 1-14 Cable – Imager Ring Scanner and HX2 Connectors

Li-Ion Battery

Main battery charging is handled exclusively by the HX2 Multi-Charger/analyzer and the battery charger integrated into a powered HX2 cradle.

The Standard battery is much thinner than the Extended battery.

Each battery will fit in the battery sleeve on an armband, hip flip and the voice case.

Note: Do not allow water or chemical cleaning agents of any kind to come in contact with the battery charging contacts or the battery cable connector; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Standard Battery

Extended Battery

Figure 1-15 HX2 Standard and HX2 Extended Battery

Battery Charge/Connect
Terminals

HX2 Battery Cable
Connector

Note: When placing the tethered battery in an armband or hip flip battery sleeve, ensure the Battery Charge/Connect terminals are protected from accidental damage by keeping them covered by the sleeve fabric at all times.

Note: New batteries must be charged prior to use. The backup battery is continually recharged by the tethered battery.

Mounting Bracket Clips

Mounting brackets are pre-installed to the back of the HX2. The brackets (one on each side) secure the HX2 to the mounting bracket clips on a hip flip or the armband.
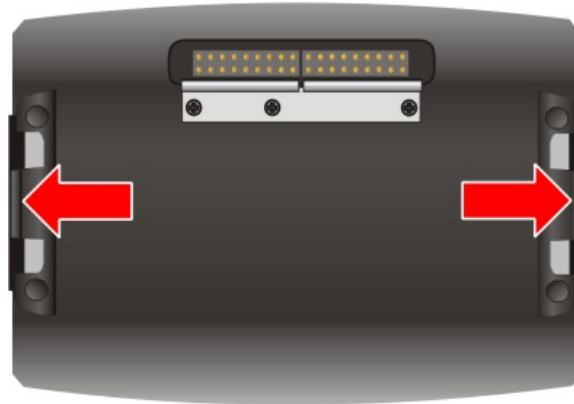
Figure 1-16 Mounting Brackets

The HX2 mount assembly is pre-installed to a hip flip or armband.

Figure 1-17 Armband and Hip Flip Mount Assembly and Clips

Connect

Center the HX2 over the mount assembly and gently push down until both bracket clips (indicated by the arrows shown above) snap over the brackets on the HX2. Carefully test the connection to make sure the HX2 is secured to the armband or hip flip.

Reset the connection by pressing down on either mounting clip to release the HX2 and try again.

Disconnect

Remove the HX2 from the mount assembly by pushing down on either mounting clip, or both, until the HX2 mounting bracket disconnects.

Or you can disconnect from one clip, then lift the HX2 up at a 45 degree angle until the other side disconnects. Lift the HX2 up and away from the mount assembly.

Mounting Devices

Armband

Armband – Top View

1 HX2 Mounting Bracket
2 Bracket Clips
3 Battery Sleeve
4 Stylus Holder
5 Arm Strap Brackets

Armband – Bottom View

1 Removable Mesh Arm Cover
2 Arm Strap Brackets
3 Adjustable Arm Straps

Figure 1-18 Armband / Top and Bottom

Straps

Figure 1-19 Armband Straps

1	Hook Fabric
2	Loop Fabric
3	Connection tabs. Slide through Arm Strap Brackets and press hook and loop fabric together to secure strap to armband.
4	Put this side of the strap on the inside, against the arm
5	Put this side of the strap on the outside

Hip Flip

Figure 1-20 Hip Flip and Belt

1	HX2 Mounting Bracket on Hip Flip
2	Mounting Bracket Clips
3	A Belt inside the Belt Loop
4	Brace (Adjustable)

System Status LEDS

Figure 1-21 System Status LEDs

	LED	Color	Indicates . . .
1	**System Status**	**Green -** Blinking	Display turned off when timer expires. This will help to conserve battery power. Tap the screen or press any key (except the Power button) to turn the display on again. The HX2 is not in Suspend Mode.
		Red - Steady	Main Battery Low. If the main battery is not replaced with a fully charged battery before the main battery fails, the HX2 is turned Off.
		Red - Blinking	Main Battery Power Fail
		Off	Suspend Mode.
2		**Blue -** Blinking Slowly	Bluetooth is active but not connected to a device.
		Blue – Blinking Medium	Bluetooth is paired and connected to a device.
		Blue - Blinking Fast	Bluetooth is discovering nearby Bluetooth devices.
		Off	Bluetooth hardware has been turned off or does not exist in the HX2.
3	**Alpha**	**Amber -** Steady	Alpha mode enabled

When multiple system status conditions are present, the most urgent condition is indicated. The conditions listed above are in increasing order of urgency by LED type.

Note: *The Dual Alpha keypad and the Triple Tap keypad do not use the Alpha LED.*

Assembly

Connecting the Battery and Ring Scanner

> *Note: The unit cannot function unless a battery is securely tethered. Be sure to place the mobile device in Suspend mode before disconnecting a battery, or all unsaved data may be lost.*

The battery and ring scanner should not be exchanged or replaced in a dirty, harsh or hazardous environment. When the tethers are disconnected, any dust or moisture that adheres to the tether connector can potentially cause damage upon cable re-connection.

Follow the numbers in the following tables to connect the battery and ring scanner to the HX2.

> *Note: Before connecting cables to the back, make sure the battery sleeve on the armband is uppermost or the following left/right directions won't work.*
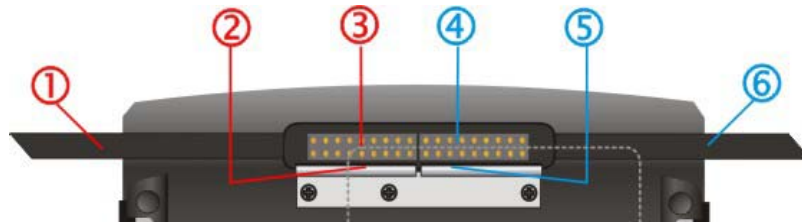
Figure 1-22 Tether the Battery and Ring Scanner – Left / Right

When you want to switch connectors from left to right, or vice versa, first gently press downward on the Retaining Clip, then pinch and pull the cable connector (not the cable!) straight up and away from the HX2. Do not use a metal object, or extreme force, to remove the cable connector from the HX2.

Re-connect cables and reassemble the HX2 body-worn components.

Ring Scanner on the Left Hand

1	Ring Scanner Tether cable channel
2	Retaining Clip for Ring Scanner Tether Connector
3	Ring Scanner cable connector
4	Battery Cable connector
5	Retaining Clip for Tethered Battery Connector
6	Tethered Battery Cable channel

Ring Scanner on the Right Hand

1	Tethered Battery Cable channel
2	Retaining Clip for Tethered Battery Connector
3	Battery Cable connector
4	Ring Scanner cable connector
5	Retaining Clip for Ring Scanner Tether Connector
6	Ring Scanner Tether Cable channel

Attaching the Rubber Boot

The rubber boot is a lightweight, flexible covering for the HX2 housing. The rubber boot cannot protect the HX2 from destructive, excessive force. It is designed to protect the HX2 housing from minor, trivial bumps or jostling.

The rubber boot does not inhibit tethered devices, cradle docking, Hip Flip assembly or Armband assembly.

Note: Remove the rubber boot when placing the HX2 in a voice case.

The rubber boot slips over the front and halfway down the sides of the HX2, leaving the touch screen, keypad, LXE logo and the HX2 logo visible.

Figure 1-23 HX2 Rubber Boot

Gently stretch the rubber boot over each corner of the front housing until the rubber boot is snug. It can be removed for cleaning, if necessary.

Smaller openings are available in the rubber boot to

- allow access to the cradle connector on the bottom of the HX2
- allow audible signals from the internal speaker to be heard
- and allow audible signals to be sent through the internal microphone.

Slipping the HX2 into the Voice Case

The voice case is a sturdy, lightweight covering for the HX2, tethered battery, and voice accessories. The voice case cannot protect the HX2 from destructive, excessive force or a harsh or wet environment. It is designed to protect the HX2 from dirt, dampness, and minor, trivial bumps.

Figure 1-24 HX2 Voice Case

1. Slide the belt through the belt loop on the voice case. Do not put the belt on yet.
2. Attach the battery cable, ring scanner and audio device to the HX2.
3. Slip the HX2 into the voice case. Be sure the screen and keypad are visible through the clear window of the voice case.
4. Slide the battery cable through the protective loop at the bottom of the voice case. Make sure the tethered cable for the ring accessory is on the outside of the voice case.
5. Slip the battery into the battery sleeve and connect the battery to the battery cable. The battery charge terminals (small metallic circles) should always be covered by the sleeve.
6. Press the hook and loop fabric at the top of the device together.
7. The HX2 in the Voice Case is ready for use.
8. Put the belt on. Adjust the belt and voice case for comfort.

Examine the tethers and the hook and loop fabric fastening periodically. If any are loose or unfastened, tighten the tethers and the top fastener before placing the voice case back into service. If the voice case is damaged, it should be removed from service.

Note: The HX2 with a voice case does not fit in the HX2 cradle. Remove the voice case before placing the HX2 in a charged cradle.

Connecting the Audio Cable and a Headset

See section titled *Set the Audio Speaker Volume*.

Note: *The audio option draws power from the tethered battery.The mobile device internal speaker and internal microphone are disabled when a headset and microphone is connected.*

The headset consists of an earpiece, a microphone and an attached cable. The headset attaches to the audio/battery cable which attaches to the HX2. The mobile device internal speaker is disabled when a headset is connected.

Figure 1-25 Audio/Battery Cable and Headset

1   Align the audio connector and the headset quick connect cable end. Firmly push the cable ends together until they click and lock in place.

2   Snap the battery plug into the battery cable connector at the top of the battery.

3   Press the battery/audio connector into either left or right connector on the back of the HX2. The retaining clip will snap into place and secure the cable connection. Place the cable in the cable groove.

Adjust Microphone and Secure the Cable

Do not twist the microphone boom when adjusting the microphone. The microphone should be adjusted to be about two finger widths from your mouth.

Make sure the microphone is pointed at your mouth. Note the small "Talk" label near the mouthpiece. Make sure the Talk label is in front of your mouth. The microphone cable can be routed over or under clothing.

Under Clothing

- Leave the cable exposed only at the top of the collar.
- Be sure to leave a small loop of cable to allow movement of your head.

Over Clothing

- Use clothing clips to hold the cable close to your body.
- Tuck the cable under the belt, but leave a small loop where it goes under the belt.
- Do not wear the cable on the front of your body. It may get in your way or get caught on protruding objects.

When you will be using an audio/battery cable without a headset, disable the **Enable Headset** parameter. See **Start | Settings | Control Panel | Mixer | Input tab**.

Tapping the Power Key

The **Power** key is a round button located above the F4 key.

When a battery is connected to the HX2 for the first time press the Power key. The mobile device begins the startup process. Wait until the Windows CE desktop appears.

Suspend/Resume Mode -- At other times, tapping the Power key places the HX2 immediately in Suspend Mode. Tapping the Power key again immediately returns the HX2 from Suspend.

Power Key Functions

See Also: Sections titled *LED Indicators* and *System Status LED* later in this guide.

- If installed, RFTerm starts up automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- If installed and pre-configured, the wireless client connects automatically during each reboot.
- If installed and pre-configured, Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.
- If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

Hardware Reset

Press and hold the **Power** key for approximately 15 seconds until the display blanks, then release the key. If user data was not saved before the Hardware Reset function started, data loss occurs and unsaved registry settings are lost.

User data is saved whenever a Suspend/Resume function is complete.

Warm Boot

Tap | **Run** and type **warmboot**. Tap the **OK** button. A warm boot does not affect the operating system, but data and programs in RAM are cleared, and registry changes, if any, are saved. Network and Bluetooth connections will need to be re-established.

There may be slight delays while the wireless client connects to the network, re-authorization for voice-enabled applications completes, Wavelink Avalanche management of the HX2 startup completes, or Bluetooth relationships establish or re-establish.

Cold Boot

Tap ⊞ | **Run** and type **coldboot**. Tap the **OK** button. Factory default settings overwrite all previously saved user settings.

Calibrating the touchscreen will need to be performed when the cold boot process is complete.

- Wireless Client configuration will need to be completed by the System Administrator.
- Required mappable keys will need to be configured. For example, there is no ⊞, Control, Shift, Alt or Del key (or their equivalent) available using the HX2 default keypad setting.
- Optional software 2 and LXE application 3 parameters will need to be set up by the System Administrator.

Important -- Because of the extreme nature of the Cold Boot, LXE recommends that the Cold Boot process be used only as an emergency procedure and Warm Boot or Suspend/Resume be used whenever necessary.

Note: Refer to the section titled Power Modes for more information relating to the power states of the HX2.

Note:

The HX2 reloads the operating system upon every warm boot or cold boot. Anything not saved or preserved to the registry is lost.

In *warm boot*, the OS and the CAB files are reloaded from the internal SD card and the preserved registry is also reloaded.

During *cold boot*, the system behavior is identical to warm boot with the addition that the registry is erased, forcing the HX2 to reboot with factory defaults. The registry is recreated when 20 minutes of uptime elapses or upon the first save or suspend function. It is also recreated every 10 registry changes and at every warm boot.

Checking Battery Status

Tap the ⊞ | **Settings** | **Control Panel** | **Battery** icon. Main battery level, backup battery level, status and other details are displayed.

Tapping the Touchscreen with a Stylus

> *Note:* *Always use the point of the stylus for tapping or making strokes on the touchscreen. Never use an actual pen, pencil, or sharp/abrasive object to write on the touchscreen. If the tip of the stylus is dirty, clean the tip with a water moistened cloth before touching the screen with the stylus.*

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. Firmly press the stylus into the stylus holder when the stylus is not in use.

Similar to using a mouse to left-click icons on a desktop computer screen, using the stylus to tap icons on the touchscreen is the basic action that can:

- Open applications
- Choose menu commands
- Select options in dialog boxes or drop-down boxes
- Drag the slider in a scroll bar
- Select text by dragging the stylus across the text
- Place the cursor in a text box prior to typing in data or retrieving data using the ring scanner or an input/output device connected to a serial port.

A stylus can be ordered from LXE. See the section titled *Accessories*.

> *Note:* *A "right mouse click" function must be programmed into the customer application to accept a constant stream of left mouse click messages. An application can choose to interpret this stream of messages as a right mouse click. LXE does not support non-LXE application programming.*

Calibrating the Touchscreen

If the touchscreen is not responding properly to stylus taps, you may need to recalibrate the touchscreen. Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To recalibrate the screen, select ⊞ | **Settings** | **Control Panel** | **Stylus** | **Calibration** tab.

To begin, tap the Recalibrate button on the screen with the stylus.

Follow the instructions on the screen and press the Enter key to save the new calibration settings or press Esc to cancel or quit.

HX2 Keypads

Inserting Characters Using the Input Panel

You can use the Input Panel to insert the following characters:

< >	{ }	[ ]	( )	_	+
: ;	" '	? /	~ `	!	@
#	$	%	^	&	|

See *Input Panel* later in this guide. See *Appendix A Key Maps* for instruction on the specific keypresses to access all allowed keypad functions.

Using the Alpha Mode 3 Tap Keypad

The Alpha and Blue keys do not auto-repeat. The default timeout for Alpha keys is 0.15 second.

Figure 1-26 The 23 Key Keypad (Default)

- When using a sequence of keys that require an alphabet key, first press the Alpha key to force Alpha mode on the numeric keys. See Alpha Modifier Key in the HX2 Reference Guide.
- Double tap the Alpha key for upper case alphabetic characters (similar to CapsLock. Single tap the Alpha key to exit CapsLock mode).
- Single tap the Alpha key to enter and exit Alpha mode.
- Default Alpha mode produces lower case alphabetic characters when numeric keys are pressed.
- Pressing the Alpha key forces "Alpha" mode for all keys.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alpha key to toggle between Alpha and Numeric mode.
- Use the Input Panel to enter characters that are not available using the 23-key keypad.
- When using a sequence of keys that do not include the Alpha key (Orange) but does include a sticky key (Blue), press the Blue key in sequence.

Using the Dual Alpha Keypad

The Dual Alpha keypad modifier keys are the Green, Orange, Blue, Shift and Control keys. See *Appendix A – Key Maps* for all available keypress sequences. Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Figure 1-27 Dual Alpha Keypad

- Any key press exits volume control mode. Any key press exits backlight control mode.
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Orange LED near the Backspace key has no function on this keypad.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Keypad Icons and the Dual Alpha Keypad

When the HX2 has a Dual Alpha keypad, a modifier key icon is displayed in the taskbar. The icon looks like a small cube. The sides of the icon change color when a modifier key is pressed.

	No modifier in focus
	Green modifier key
	Orange modifier key
	Blue modifier key
	Shift modifier key. For example, Shift + Green and Shift + Blue
	When multiple modifier keys are in focus, for example, Green + Orange + 1 to put a double quote ["] on the screen --- the modifier key icon will show an orange side and a green side.

See *Appendix A – Key Maps* for all available keypress sequences.

Using the Triple Tap Keypad

The Triple Tap keypad modifier keys are the Green, Orange, Blue, Shift and Control keys. See *Appendix A – Key Maps* for all available keypress sequences.

Figure 1-28 The Triple Tap Keypad

- Any key press exits volume control mode. Any key press exits backlight control mode.
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Orange LED near the Backspace key has no function on this keypad.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Keypad Icons and the Triple Tap Keypad

When the HX2 has a Triple Tap keypad, a modifier key icon is displayed in the taskbar. The icon looks like a small cube. The sides of the icon change color when a modifier key is pressed.

	No modifier in focus
	Green modifier key
	Orange modifier key
	Blue modifier key
	Shift modifier key. For example, Shift + Green and Shift + Blue
	When multiple modifier keys are in focus, for example, Green + Orange + 1 to put a double quote ["] on the screen --- the modifier key icon will show an orange side and a green side.

See *Appendix A – Key Maps* for all available keypress sequences.

Bluetooth

or   Tap the Bluetooth icon in the taskbar, on the desktop, or in the Control Panel
            to open the LXEZ Pairing application.

Bluetooth is an option and may not be available on all HX2s. The HX2 default Bluetooth
hardware setting is On.

The LXE HX2 *Bluetooth*® module is designed to Discover and pair with nearby LXE Bluetooth
devices. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All
other Bluetooth devices are ignored.

Prerequisite   The Bluetooth devices (printers and/or scanners) have been setup to allow them
                     to be "Discovered" and "Connected/Paired". The System Administrator is
                     familiar with the pairing function of the Bluetooth devices.

Figure 1-29 Bluetooth LXEZ Pairing Display

The Bluetooth remote device should be as close as possible, and in direct line of sight, with the
HX2 during the pairing process.

Initial Use

1. Select Start | Settings | Control Panel | Bluetooth.
2. Tap the Settings Tab.
3. Change the Computer Friendly Name at the bottom of the Settings display. The Bluetooth
   HX2 default name is determined by the LXE factory installed software version. LXE strongly
   urges assigning every HX2 a unique name (up to 32 characters) before Bluetooth Discovery
   is initiated.
4. Check or uncheck the HX2 Bluetooth options on the Settings tab.
5. Tap the OK button to save your changes or the X button to discard any changes.

Settings Tab | Bluetooth Options

Note: These options can still be checked or unchecked whether Bluetooth is enabled or disabled.

As Bluetooth devices pair with the HX2, the name of the device and an icon representing the type of device is displayed in the Devices window. The icon state changes as the paired Bluetooth devices connect and disconnect from the HX2. When the Bluetooth devices are disconnected, the device icon has a red highlight.

Report when connection lost

A dialog box appears on the HX2 display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. This option is enabled by default.

Click the OK button or the X button to remove the dialog box from the screen.

Report when reconnected

A dialog box appears on the HX2 display notifying the user a connection between one (or all) of the previously-paired Bluetooth devices is complete. This option is disabled by default.

Click the OK button or the X button to remove the dialog box from the screen.

Report failure to reconnect

If the reconnect timeout (default is 30 minutes) expires, a dialog box appears on the HX2 display notifying the end-user the connection between one (or all) of the previously-paired Bluetooth devices has failed. This option is enabled by default.

Click the OK button to remove the dialog box from the screen.

Computer is connectable

There is no dialog connected to this checkbox. Enable this checkbox when you want the HX2 to be able to pair with other Bluetooth devices. This option is enabled by default.

Computer is discoverable

There is no dialog connected to this checkbox. Enable this checkbox when you want the HX2 to be Discovered by other Bluetooth devices. This option is disabled by default.

Prompt if devices request to pair

A dialog box appears on the HX2 screen notifying the user a Bluetooth device requests to pair with the HX2. This option is disabled by default.

The requesting Bluetooth device does not need to have been Discovered by the HX2 before the pairing request is received.

Click the Accept button or the Decline button to remove the dialog box from the screen.

Continuous Search

This option is disabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with if the connection is broken (such as the paired device entering

Suspend mode, going out of range or being turned off). When disabled, after being enabled, the HX2 stops searching after 30 minutes. This option draws power from the Main Battery.

Subsequent Use

> *Note:* *Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. A taskbar Bluetooth icon with a red highlight indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.*

1. Tap the **Bluetooth icon** in the taskbar to open the LXEZ Pairing application. Tap the Bluetooth Devices tab, if necessary.
2. Tap the **Discover** button. When the *Bluetooth*® module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
3. Any discovered devices are listed in the Bluetooth Devices window.
4. **Doubletap** a Bluetooth device in the Discovered window to open the Bluetooth device properties menu.
5. Tap Pair as Scanner to set up the HX2 to receive scanner data.
6. Tap Pair as Printer to set up the HX2 to send data to the printer.
7. If paired, tap Disconnect to stop pairing with the device. Tap Delete to remove the device name and data from the HX2 Bluetooth Devices list. Tap OK.
8. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the HX2 display.
9. Whenever the HX2 returns from Suspend Mode, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the HX2.

If the devices cannot connect to the HX2 before the re-connect timeout time period expires (default is approximately 30 minutes for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

> *Note:* *The Bluetooth printer port is COM9.*

See Also: *Chapter 3 – System Configuration,* section titled *Bluetooth.*

Bluetooth Devices

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for each HX2. The System Administrator has also enabled / disabled Bluetooth settings and assigned a Computer Friendly Name for each HX2. See *Chapter 3 System Configuration, Bluetooth control panel applet* and supported Bluetooth printers and scanners.

The Bluetooth taskbar Icon state and Bluetooth LED states change as Bluetooth devices are discovered, pair, connect, and disconnect. The Bluetooth LED is located next to the Right Arrow key on the keypad.

The Bluetooth LED blinks slowly when it is idle. Blinks quickly when the HX2 is discovering other Bluetooth devices. And blinks normally when it is connected. There may be audible or visual signals from paired devices as they re-connect with the HX2. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Taskbar Icon   **Legend**

Bluetooth® module is connected to one or more of the targeted Bluetooth device(s).

HX2 is not connected to any Bluetooth device.

HX2 is ready to connect with any Bluetooth device.

HX2 is out of range of all paired Bluetooth device(s). Connection is inactive.

Bluetooth LED		
	Blue - Blinking Slowly	Bluetooth is active but not connected to a device.
	Blue – Blinking Medium	Bluetooth is paired and connected to a device.
	Blue - Blinking Fast	Bluetooth is discovering other Bluetooth devices.
	Off	Bluetooth hardware has been turned off or does not exist in the HX2.

Note: *When an active paired device, not the HX2, enters Suspend Mode, is turned Off or leaves the HX2 Bluetooth range, the Bluetooth connection between the linked device and the HX2 is lost. There may be audible or visual signals as paired devices disconnect from the HX2. The Bluetooth remote device should be as close as possible, in direct line of sight, with the HX2 during the pairing process.*

See *Accessories* for supported Bluetooth printers and scanners.

AppLock, if installed, does not stop the end-user from using Bluetooth application, nor does it stop authorized Bluetooth-enabled devices from pairing with the HX2 while AppLock is in control. See *Chapter 6 – AppLock* for more information.

See Also: *Chapter 3 – System Configuration*, section titled *Bluetooth*.

Bluetooth Mobile Barcode Reader Setup

Please refer to the mobile Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Please contact your LXE representative for Bluetooth product assistance.

Introduction

LXE supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the HX2 using Bluetooth functions.

- The HX2 must have the Bluetooth hardware and software installed. Contact your LXE representative for details.
- If the HX2 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The HX2 batteries are fully charged. Alternatively, the HX2 may be in a powered cradle.
- The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.
- To open the LXEZ Pairing program, tap **Start | Settings | Control Panel | Bluetooth** or tap the **Bluetooth icon on the desktop** or tap the **Bluetooth icon in the taskbar**.

Figure 1-30 Sample Bluetooth Address Barcode Label

Locate the barcode label, similar to the one shown above, attached to the mobile device. The label is the Bluetooth address identifier for the HX2.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

> **Important**: The HX2 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

HX2 with Label

If the HX2 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the HX2, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the HX2 Bluetooth label, the devices are paired. If not, go to the next step.
3. Open the LXEZ Pairing panel [Start | Settings | Control Panel | Bluetooth].
4. Tap Discover. Locate the Bluetooth scanner in the discovery panel.
5. Tap and hold the stylus on the Bluetooth scanner until the right-mouse-click menu appears.
6. Select Pair as Scanner to pair the HX2 with the Bluetooth mobile scanner.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled *Bluetooth Beep and LED Indications*.

> *Note: After scanning the HX2 Bluetooth label, if there is no beep and no LED flash from the*
> *Bluetooth device, the devices are currently paired.*

HX2 without Label

If the HX2 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the HX2:

First, locate the HX2 Bluetooth address by tapping **Start | Settings | Control Panel | Bluetooth | About** tab.

Figure 1-31 About tab and Bluetooth Address

Next, create a Bluetooth address barcode label for the HX2 [4].

The format for the barcode label is as follows:

- Barcode type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.

Create and print the label.

Scan the HX2 Bluetooth address barcode label with the mobile Bluetooth barcode reader.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled *Bluetooth Beep and LED Indications*.

> *Note: After scanning the HX2 Bluetooth label, if there is no beep and no LED flash from the*
> *mobile Bluetooth device, the devices are currently paired.*

Bluetooth Beep and LED Indications

The following indications relate to the behavior of the mobile Bluetooth scanner, not the HX2.

Beep Type	Behavior
1 beep	Acknowledge label
2 beeps at low frequency	Label rejected
Beep will sound high-low-high-low	Transmission error
Beep will sound low-medium-high	Link successful
Beep will sound high-low-high-low	Link unsuccessful

---

[4]   Free barcode creation software is available for download on the world wide web. Search using the keywords "barcode create".

LED	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the mobile Bluetooth scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact LXE Support for assistance.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the HX2 during the pairing process.

1. Open the LXEZ Pairing panel [Start | Settings | Control Panel | Bluetooth].
2. Tap Discover. Locate the Bluetooth printer in the discovery panel.
3. Tap and hold the stylus on the Bluetooth printer until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the HX2 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer *may* respond with a series of beeps or LED flashes.

Please refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Please contact your LXE representative for Bluetooth product assistance.

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the HX2 and the printer are currently paired.

Data Entry

You can enter data into the HX2 through several different methods. The Ring Scanner aperture provides barcode data entry, the Input/Output (I/O) ports, the built-in microphone and speaker are used to input/output data, and the physical and virtual keypads provide text entry.

Mobile devices with a touchscreen use a stylus to input data, devices connected to the I/O ports and/or the keypad. An input panel (virtual keyboard) is available for applications that expect keyed input.

Keypad Entry

The keypad is used to manually input data that is not collected otherwise. A subset of desktop PC full keyboard functions are provided. Almost every key on the keypad has two or three different functions. The primary function or numeric character is printed on the key.

Please refer to *Appendix A – Key Maps* for instruction on the unique keypresses to access the available keyboard functions.

Stylus Data Entry

Note: *This section is directed to the HX2 daily user. The assumption is that the mobile device has been configured and the touch screen calibrated by the System Administrator prior to releasing the HX2 for daily use. The touch screen should be calibrated before initial use.*

The stylus performs the same function as the mouse that is used to point to and click elements on a desktop computer. The stylus is used in the same manner as a mouse – single tap or double tap to select menu options, drag the stylus across text to select, hold the stylus down to activate slider bars, etcetera.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. The touch screen responds to an actuation force (touch) of 4 oz. (or greater) of pressure.

The stylus can be used in conjunction with the keypad and ring scanner and an input/output device connected to a serial port when the HX2 is docked in a powered cradle.

- Touch the stylus to the field of the data entry form to receive the next data feed.
- The cursor begins to flash in the field.
- The HX2 is ready to accept data from either the physical keypad, virtual keyboard, or an input/output device.

Note: *Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp/abrasive object to write on the touch screen.*

Ring Scanner Data Entry

Read all cautions, warnings and labels **before** using the ring
scanner.
Do not look into the laser's lens.
Do not stare directly into the laser beam.

Barcode Scanner

To scan with the laser barcode scanner, point the ring scanner laser aperture towards a barcode and press the Scan button. You will see a red laser beam strike the barcode. Align the red beam so that the barcode is centered within the beam. The laser beam must cross the entire barcode. Move the ring scanner towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.

There may be an audio response combined with the Scan function.

| Correct Scan | Incorrect Scan | Incorrect Scan |

Figure 1-32 Laser Scan Beam on Linear Barcode

See section titled *Scan Status LED*.

2D Imager

Figure 1-33 Imager Bracketed Crosshair Target on 2D Barcode

To scan with the Imager Ring Scanner, point the scan aperture towards a 2D barcode and press the Scan button. You will see a bracketed crosshair strike the barcode. Align the brackets so that the center of the barcode is covered by the crosshair.

Move the ring scanner towards or away from the barcode until a response is emitted by the HX2 (1 beep, 2 beeps, a WAV file, etc) or the bracketed crosshair times out and disappears.

The Imager LED may illuminate when the Scan button is pressed. There are three options that can be set by the System Administrator using the Scanner control panel applet: Internal illumination, External illumination, or Both. If external illumination or both is chosen, there are three white LEDs located above the imager aperture that will illuminate for the duration of the scan then turn off.

See the previous section titled *Tethered Ring Scanner / Imager* figure titled *Ring Scanner/Imager Apertures*.

Scan Status LED

Figure 1-34 Scan Status LED

The Scan Status LED (oval shaped LED on the top of the ring scanner) turns red when the laser beam is on. Following a barcode scan and read the Scan Status LED turns green for two seconds and the HX2 may beep, indicating a successful scan. If the scan was unsuccessful, the Scan Status LED turns off and a different beep sequence may be heard.

The ring scanner engine and Scan Status LED automatically turn off after a successful or unsuccessful read. The ring scanner is ready to scan again after the Scan button is released, or after the Scan Status LED turns off following a successful scan.

Voice Data

Data is entered into the HX2 by speaking into the headset's microphone (or the internal microphone located below the Up Arrow) when prompted.

Input Panel / Virtual Keyboard

The virtual keyboard is always available when needed e.g. text field input. Tap the **Keyboard** icon in the Taskbar to put the virtual keyboard on the display. Using the stylus:

- Tap the Shift key to type one capital letter.
- Tap the CAPS key to type all capital letters.
- Tap the au key to access symbols.

Figure 1-35 Input Panel / Virtual Keyboard

Some applications do not automatically display the Input Panel. In this case, do the following to use the Input Panel:

- Tap the Input Panel icon in the taskbar.
- Select **Keyboard** from the menu.
- Tap the data entry area on the display when you want to enter data using the Input Panel.

When finished entering data, tap the **Keyboard** icon in the Taskbar. Select **Hide Input Panel**. See *Chapter 3 – System Configuration* for more information.

Entering the AppLock Activation Key

> *Note: The touch screen must be enabled.*

Switchpad Menu   Switchpad Icon in Taskbar
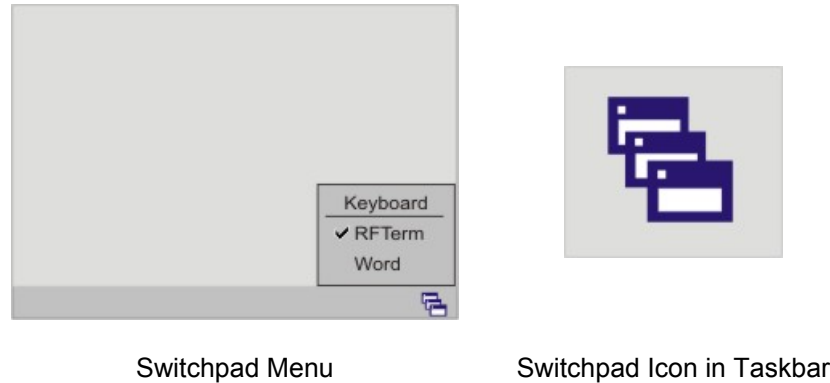
Figure 1-36 Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the HX2 default input method (Input Panel, Transcriber, or custom input method) is activated.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the taskbar. The taskbar is always visible on top of the application in focus.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

The figure shown above is an example and is shown only to aid in describing how the user can switch between applications using a stylus.

Using the Keypad

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See *Chapter 6 – AppLock* for more information.

Setting Timers

Setting the Power Schemes Timers

> *Note:* *Refer to the section titled* *Power Modes* *for information relating to the power states of the mobile device.*

Select | **Settings** | **Control Panel** | **Power** | **Schemes** tab. Change the parameter values and tap OK to save the changes.
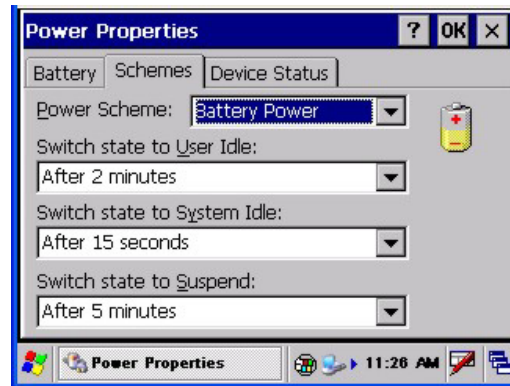
Figure 1-37 Power Properties – Schemes Tab

Battery Power Scheme

Use this option when the mobile device will be running on battery power only.

Switch state to User Idle	Default is After 3 seconds
Switch state to System Idle	Default is After 15 seconds
Switch state to Suspend	Default is After 5 minutes

AC Power Scheme

Use this option when the mobile device will be running on external power (e.g. docked in a powered cradle).

Switch state to User Idle	Default is After 2 minute
Switch state to System Idle	Default is After 2 minutes
Switch state to Suspend	Default is After 5 minutes

The mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to "Never", the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

Because of the cumulative effect, and using the Battery Power Scheme Defaults listed above:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15seconds + 3seconds),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.

See *Chapter 3 – System Configuration* for more information.

Setting The Audio Speaker Volume

Note: *An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.*

The internal speaker is located on the front of the device above the "2" key. The audio volume can be adjusted to a comfortable level for the listener. Operational "beeps" are emitted from the speaker. A Battery/Audio cable is available for headsets, see *Accessories* and *Cables*.

Using the Keypad

Note: *Volume & Sounds (in Settings | Control Panel) must be enabled before the following default key sequences will adjust the volume.*

The volume is increased or decreased one step each time the volume key sequence is pressed.

To adjust speaker volume use the:

- **Blue+Up Arrow** and **Blue+Down Arrow** keys on the Alpha Mode 3 Tap keypad
- **Orange+Diamond 1+Up Arrow** and **Orange+Diamond 1+Down Arrow** keys on the Dual Alpha and Triple Tap keypads

Until the speaker volume is satisfactory.

Using the Touchscreen

Tap 🏁 | **Settings** | **Control Panel** | **Volume & Sounds** | **Volume** tab. Change the volume setting and tap OK to save the change.
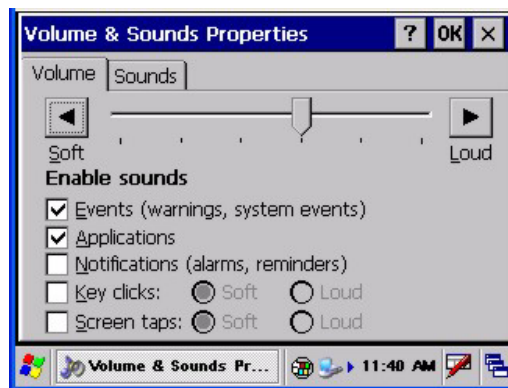
Figure 1-38 Volume & Sounds Properties

You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

As the volume scrollbar is moved between Loud and Soft, the computer will emit a tone each time the volume increases or decreases in decibel range.

See *Chapter 3 – System Configuration* for more information.

Adjusting the Display Backlight Timer

Select | **Settings** | **Control Panel** | **Display** | **Backlight** tab. Change the parameter values and tap OK to save the changes.

Figure 1-39 Setting the Display Backlight Timer

The first option affects the display when the HX2 is running on battery power only. The second option affects the display when the HX2 is running on external power (e.g. docked in a powered cradle).

The default value for the battery power timer is 3 seconds.

The default value for the external power timer is 2 minutes. **The display backlight will remain on all the time when both checkboxes are blank.**

The display backlight timer *dims the backlight* at the end of the specified time.

When the Keypad Backlight is On, it responds to the settings of the Display Backlight Timer. See next segment titled *Turning the Keypad Backlight On or Off*.

See *Chapter 3 – System Configuration* for more information.

Adjusting the Display Brightness

The display brightness is increased or decreased one step each time the adjust brightness key sequence is pressed.

To adjust display brightness:

- **Alpha Mode 3 Tap** keypad – Open the Keypad Control Panel | Keymap tab and map a key to Brightness Up and Brightness Down. Tap OK. Tap the mapped keys to increase or decrease display brightness.
- **Dual Alpha Keypad** and the **Triple Tap Keypad --** Light Blue+Diamond 1+Up Arrow and Light Blue+Diamond 1+Down Arrow keys.

Until the display brightness is satisfactory.

Turning the Keypad Backlight On or Off

Select ⊞ | **Settings** | **Control Panel** | **Display** | **Keypad** | **Alpha** tab.

Note: Alpha tab in the Keypad control panel is not available when the HX2 has a Dual Alpha or Triple Tap keypad.

HX2 Alpha Mode 3 Tap Keypad   Dual Alpha Keypad or Triple Tap Keypad
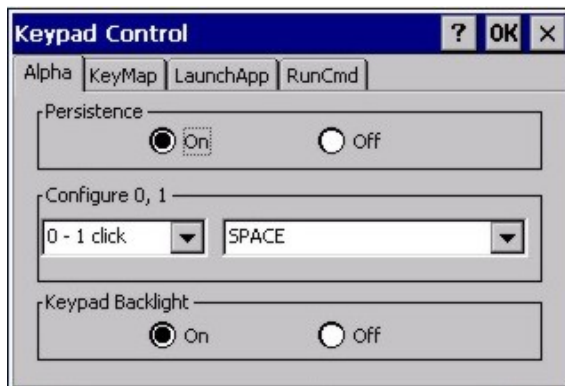
Figure 1-40 Turning the Keypad Backlight On or Off

Tap the Off radio button when the keypad backlight is to remain Off regardless of the OS event in process. The default is On. When On the keypad backlight responds to OS events as designed.

When On, the keypad backlight responds to the settings of the Display Backlight Timer. See previous segment titled *Adjusting the Display Backlight Timer*.

Cleaning the Glass Display/Ring Scanner Aperture

> *Note: These instructions are for components made of glass. If there is a removable protective film sheet on the display screen, remove the film sheet before cleaning the screen.*

Keep fingers and rough or sharp objects away from the ring scanner aperture and the mobile device display. If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex® without vinegar or use Isopropyl Alcohol. Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the glass surface. Use a clean, damp, lint-free cloth. Do not scrub optical surfaces. If possible, clean only those areas which are soiled. Lint/particulates can be removed with clean, filtered canned air.

Applying the Protective Film to the Screen Display

First, clean the display of fingerprints, lint particles, dust and smudges.

Remove the protective film from its container. Remove any protective backing from the film sheet by lifting the backing from a corner of the film. Discard the backing.

Apply the film to the screen starting at one side and smoothing it across the display. If air bubbles appear, raise the film slightly and continue smoothing the film across the display until it covers the glass surface of the display.

If dust, lint or smudges are trapped between the protective film and the glass display, remove the protective film, clean the display and apply the protective film again.

Copy the HX2 LXEbook to the HX2 (Optional)

> *Note: The LXEbook user guides do not contain the illustrations and regulatory information contained in the full user guides on the LXE Manuals CD and on the LXE ServicePass website. See the full format HX2 User Guide HX2 on the LXE Manuals CD.*

Prerequisite: An ActiveSync client relationship has been established between the desktop computer and the HX2.

First, using your desktop computer download *LXEbook – HX2 Users Guide* from the LXE Manuals CD to your desktop computer.

Next, refer to *ActiveSync Processes* and *Initial Install* in Chapter 3 of this guide before connecting the HX2 to your PC.

When the HX2 and the desktop ActiveSync applications are synchronized, tap Explore on the ActiveSync menu on your PC to display the contents of the HX2 folders.

Then, open the folder on your desktop computer containing the downloaded LXEbook. Tap and drag the LXEbook to the My Documents folder on the HX2.

When the file copy process is finished, disconnect the HX2 from the ActiveSync synchronization cable and close ActiveSync.

To view the LXEbook on the HX2, select [icon] | **Programs** | **PDF Viewer** | **File** | **Open**. Locate the LXEbook on the HX2 and "open" the file.

See Also: *Install LXEbooks* on the LXE Manuals CD.

Strap Assemblies

Caution: Do not perform the following procedures if the ring barcode reader is tethered to the HX2. There is a possibility the Scan button may be pressed inadvertently and the laser beam emitted.

LXE recommends that installation or removal of accessories be performed on a clean, well-lit surface. When necessary, protect the work surface, the mobile device, and components from electrostatic discharge.

Note: Do not touch, push on or brace your finger against the scan aperture at any time.

Removing / Replacing the Ring Finger Strap Assembly

Note: Do not pull on the finger strap or the flexible liner to remove the finger strap assembly. This quick disconnect function is designed for occasional safety hazards and is not intended for daily removal.

A 20 pak of Ring Scanner Finger Straps is available from LXE (8600A401RINGSTRAP). See *Accessories*.

Using the Quick Disconnect Function, grasp the finger strap and pull the finger strap out and away from the ring scanner.

Before attaching the finger strap to the trigger module, thread the finger strap, warning label side down, first through the hinge, then under and over the pin next to the scan button.

It should slide easily.

Removing / Replacing the Trigger Module

Equipment Needed: Phillips screwdriver with a blade diameter of 1/8" (.4mm). Not supplied by LXE.

LXE recommends that installation or removal of accessories be performed on a clean, well-lit surface. When necessary, protect the work surface, the mobile device, and components from electrostatic discharge.

A 20 pak of full Trigger assemblies is available from LXE (8600A403TRIGGERKIT). See *Accessories*.

Remove Finger Strap Assembly

Original finger strap assemblies – Remove the flexible liner from the finger strap assembly and discard the flexible liner.

Version 2 finger strap assemblies – Fold the flexible liner back until the screw hole is visible.

1.   Rotate the trigger module until the black screw is visible as shown in the following figure.

2.   Using a Phillips screwdriver with a blade diameter of 1/8" (.4mm) loosen the black screw counter-clockwise and set the screw aside in a safe place.

3.   Remove the trigger module.
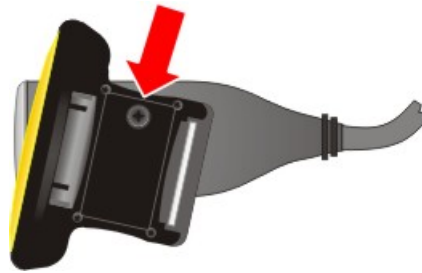
Figure 1-41 Step 1 : Rotate Trigger Module and Remove Screw

Figure 1-42 Step 2 : Rotate Trigger Module again until it pops up. Remove the trigger module.

Replace

1. Position the trigger module on the base of the Ring Scanner, making sure the empty screw hole is visible as shown in the following figure.

2. Find the tiny black screw that you removed previously.
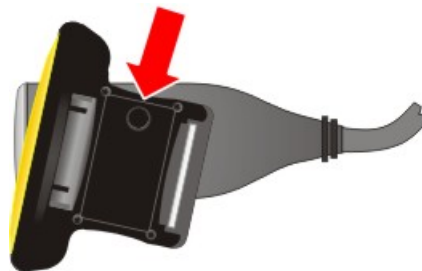
Figure 1-43 Replace Trigger Module

3. Using a Phillips screwdriver with a blade diameter of 1/8" (.4mm) rotate the black screw clockwise until the trigger module is secured to the ring scanner.

4. Install the finger strap. See *Removing / Replacing the Ring Finger Strap Assembly*.

Removing/Replacing the Armband Straps

> *Note: Remove the HX2 and any of its tethered devices from the Armband before removing and replacing the armband straps.*

The armband is a lightweight, sturdy mounting platform for the HX2. There are two armband straps. The shorter strap is used at the end-user wrist area and the longer strap is used at the end-user forearm area. A armband strap replacement kit is available from LXE. See *Accessories*.
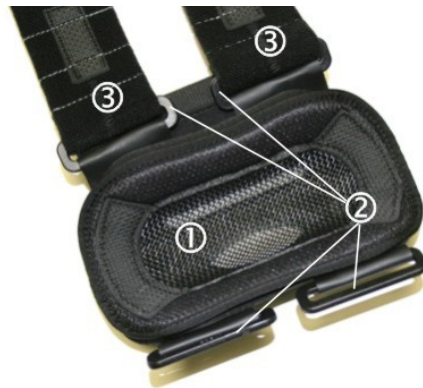
Armband – Bottom View

1 Removable Mesh Arm Cover

2 Arm Strap Brackets

3 Adjustable Arm Straps

Figure 1-44 Removing/Replacing the Armband Straps

Figure 1-45 Armband Straps

1	Hook Fabric
2	Loop Fabric
3	Connection tabs.
4	Strap side for inside.
5	Strap side for outside.

1. Slip each end of the arm strap through the arm strap brackets ensuring the hook and loop fastening sections are on the outside of the armband.
2. The shorter strap is used for the wrist area and the longer strap is used for the forearm area.
3. Press the straps hook end against the straps loop fastener to secure each end of the strap to the armband. After both straps are loosely fastened in this manner, snap the HX2 onto the armband bracket.

4. Slip your hand through the armband straps until the armband is in the desired location. Grasp the tab at one end of the strap to loosen and then tighten each strap until the armband is comfortably snug.
5. Ensure the HX2 on the armband is stable and does not slide or slip around your arm.
6. Periodically check the straps, strap brackets and hook and loop fabric areas for damage. The damaged parts should be replaced before the straps or strap brackets are used on an armband again.

Note: The armband is washable, but only the mesh arm cover and straps are machine washable.

Getting Help

All LXE manuals are now available on one CD and they can also be viewed/downloaded from the LXE ServicePass website. Contact your LXE representative to obtain the LXE Manuals CD.

You can also get help from LXE by calling the telephone numbers listed on the LXE Manuals CD, in the file titled *Contacting LXE*. This information is also available on the LXE website's ServicePass page.

Explanations of terms and acronyms used in this manual are located in the file titled *LXE Technical Glossary* on the LXE Manuals CD.

Manuals

- HX2 User's Guide - English
- HX2 Cradle Reference Guide
- HX2 Reference Guide
- HX2 Multi-Charger User's Guide
- LXEbook – HX2 User's Guide (download to mobile device)
- RFTerm Reference Guide
- LXE Security Primer
- CE API Programmers Guide
- Ring Scanner Programming Guide

Contact your LXE representative for user and reference guide availability and subsequent updates.

Accessories

Note: *Items with a Green letter R in the second column are ROHS-compliant. Please contact your LXE representative when ordering ROHS-compliant items as the part number may have changed. Items without the letter R may have received ROHS-compliance after this guide was published. E designator means the accessory is RoHS Exempt.*

Power		
HX2 Standard Battery, Lithium Ion	E	HX2A301BATTSTD
HX2 Extended Battery, Lithium Ion	E	HX2A302BATTEXT
6 slot battery charger with universal power supply. Includes analyzing capabilities on one slot. US power cord included.	R	HX2A310CHRG6US
6 slot battery charger with universal power supply. Includes analyzing capabilities on one slot. Power cord not included.	R	HX2A311CHRG6WW
Cradle		
HX2 Desk cradle with spare charging slot. Includes universal power supply. US power cord included.	R	HX2A312DESKCRADLEUS
HX2 Desk cradle with spare charging slot. Includes universal power supply. Power cord not included.	R	HX2A313DESKCRADLEWW
Mobility		
Armband with standard wrist straps	R	HX2A201ARMBAND
Replacement Mesh Arm Cover for armband	R	HX2A204UNDERPAD
Strap kit for armband (includes different length straps to fit all arm sizes).	R	HX2A205STRAPKIT
Hip Flip (for belt mounting)	R	HX2A221HIPFLIP
Voice case (for belt mounting)	R	HX2A222VOICECASE
Belt for hip flip or voice case	R	9200L67
Ring Scanners		
SR laser for armband (short cable)	R	8610A101SRSLASER
2D Imager for armband (short cable)	R	8620A101SRSIMAGER
Mobile Bluetooth Barcode Readers		
PowerScan 7000BT Scanner RS-232 with pointer	R	8700A301SCNRBTSRI
PowerScan 7000BT Base Station, RS232, without universal power supply.	R	8700A501BASERS232
PowerScan 7000BT Base Station Power Supply, Std US, 120V	R	8700A502PSACUS
PowerScan 7000BT, RS232 Cable for Base Station, DB9S, Coil, 8'	R	8700A001CBL8DA9F

PowerScan 7000BT Battery Charger with Power Supply, Four Station, US Std	R	8700A503CHGR4US
PowerScan 7000BT Battery Pack	R	8700A504BATT
Bluetooth Standard Range Fuzzy Logic laser	R	8810A326SCNRBTFZ
Bluetooth Auto Range LORAX laser	R	8820A327SCNRBTER
Spare battery	R	8800A376BATTERY
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	R	8800A051POWERCORD
Single Slot Universal Battery Charger adapter cup for 8800 Battery	R	8800A377CHGRADPTRCUP
Single slot battery charger with International power supply	R	8800A378CHGR1SLOT
Universal Battery charger 4-Slot Base. Power Supply included, no AC power cord.	R	8800A379CHGRBASE
LS3408 Scanner Holster for Belt	R	8200A501HOLSTRBELT
Mounted Take Up Reel (Mounted applications)	R	8000A501INDREEL
Auto Sense Intellistand, Hands Free Scanning	R	8500A505STANDSMT
CBL ASSY, DA9F, 9ft (cradle to terminal)	R	8500A051CBL9DA9F
Desk Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	R	8800A001CRADLERCMI
Desk Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	R	8800A002CRADLECMI
Forklift Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	R	8800A003CRADLEVRCMI
Forklift Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	R	8800A004CRADLEVCMI
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	R	8800A051POWERCORD
Universal Desktop Power Supply 90-264VAC, 9VDC, 2A, EPS	R	8800A301ACPS
9-60VDC Forklift Power Supply (For Use with Forklift Cradles)	R	8800A302DCPS
Power Cable: Connects DC Power Supply to Forklift Cradle	R	8800A052DCPWRCABLE
Forklift Rugged Scanner Holder with RAM mount (all metal with cloth padding)	R	8800A005STAND
Cables		
USB ActiveSync Cable (Type A to HX2 cradle connector)	R	HX2A001CBLACTVSYNC
Battery Cable	R	HX2A002CBLBATT
Battery Cable with Audio	R	HX2A003CBLBATTAUDIO
Battery Extension Cable	R	HX2A004CBLBATTEXT
Cable Connector Plug	R	HX2A008CBLCONPLUG
Miscellaneous		
Rubber protective boot, gray	R	HX2A232BOOTGRAY

Replacement Stylus , 10-pack	R	9000A507STYLUS
Ring Scanner Trigger Assembly, 20 pack	R	8600A403TRIGGERKIT
Ring Scanner Replacement Strap Kit, 20 pack	R	8600A401RINGSTRAP
CD with CE 5.0 API's and LXE API's with documentation for custom application development	R	HX2A501CE50SDK
Touchscreen anti-glare anti-reflective protective film, 10 pack	R	HX2A502PROTFILM
Audio		
Single ear, single headband, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A501SNGBHEADSET
Single ear, dual headband, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A502DUALBHEADSET
Dual ear, behind the head, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A503BTHHEADSET
Replacement foam block for 502 dual band headsets, qty 1	R	HX1A504AHSBLOCKFOAM
Replacement head yoke for dual band 502 headset, qty 1	R	HX1A505DUALYOKE
Replacement head yoke for single band 501 headset, qty 1	R	HX1A506SINGLEYOKE
Replacement windscreen for all headset microphones, 10 Pack	R	HX1A508WINDSCREEN10
Replacement windscreen for all headset microphones, 50 Pack	R	HX1A509WINDSCREEN50
Replacement foam ear piece cover for 501 and 502 headsets, 10 pack	R	HX1A510FOAMEAR10
Replacement foam ear piece cover for 501 and 502 headsets, 50 pack	R	HX1A511FOAMEAR50

Chapter 2 Physical Description and Layout

Hardware Configuration

System Hardware

The HX2 hardware configuration is shown in the following figure.
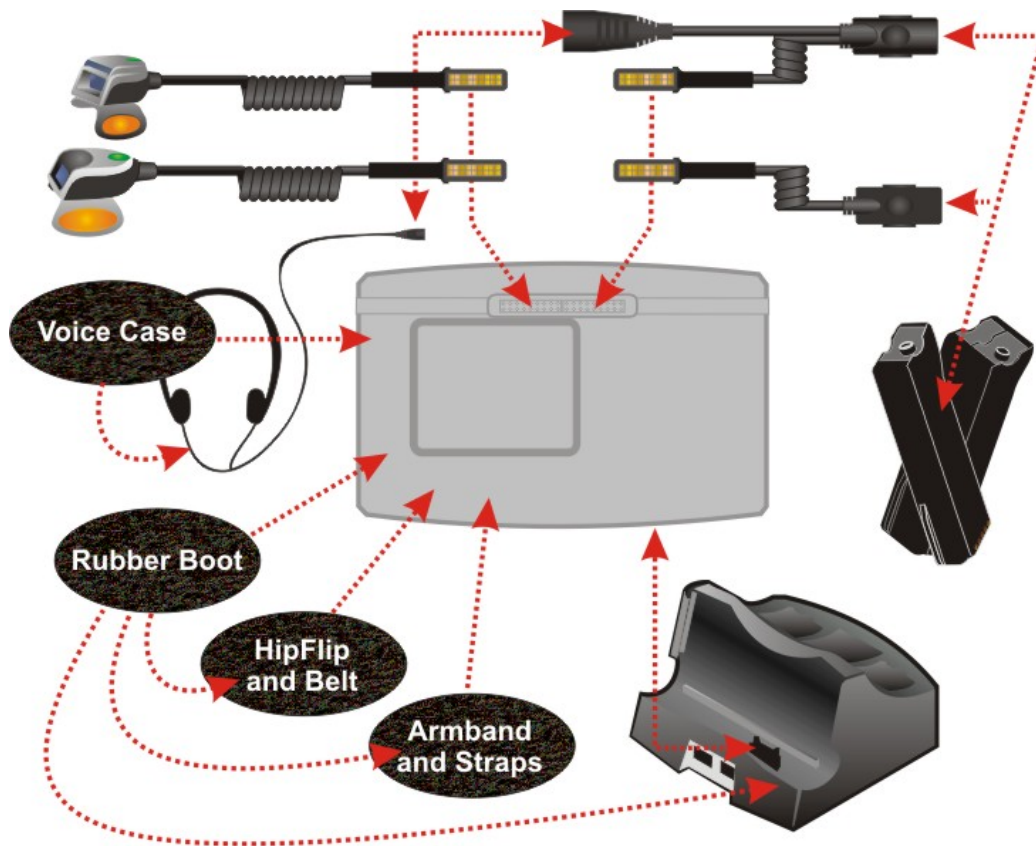
Figure 2-1 System Hardware

802.11b/g Wireless Client

The HX2 has an LXE 802.11b/g network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Adjusting power management on the network card is set to static dynamic control.

WEP, WPA and LEAP are supported. See *Chapter 5 – Wireless Network Configuration*.

Central Processing Unit

The CPU is a 400MHz Intel Xscale PXA255 CPU. The operating system is Microsoft Windows CE 5.0. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

Xscale turbo mode switching is supported and turned on by default.

The HX2 supports the following I/O components of the core logic:

- One SD card slot, inaccessible to the end-user.
- One TTL serial port designed to interface with LXE ring scanner only.
- One RS-232 serial port accessible via the cradle.
- USB master accessible via the cradle.
- USB client accessible via the cradle.
- One Digitizer Input port (Touch screen).

System Memory

The 400MHz CPU configuration supports 128MB SDRAM, 128MB SD card. SD card location is inaccessible to the end user.

The system optimizes for the amount of SDRAM available. The operating system executes out of RAM.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID required by CE 5.0 is stored in the boot flash. A second copy of the bootloader code is stored on the internal SD Flash drive, so that if a damaged bootloader is detected, it may be re-flashed correctly.

Internal SD Memory Card

The HX2 has one SD card interface for storage of operating system and program code, as well as persistent storage. The SD slot is inaccessible and ships with an LXE-qualified 128MB (optional 512MB) SD Flash card.

The internal SD flash card supports a FAT file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface. Operating system files are hidden on this drive with a terminal unique identifier in the internal flash, to prevent them being accidentally erased by a user. In addition, the registry hive files are stored on this device. The amount of Flash memory available for customer use is the original SD flash card size less 40MB.

Video Subsystem

The QVGA touchscreen is a 2.5" (6.3 cm) diagonal viewing area, 320 by 240 pixel Transflective Active Color LCD. The turn-off timing is configured through the | **Settings | Control Panel | Display | Backlight** icon. The display controller supports Microsoft CE 5.0 graphics modes.

A touchscreen allows mouse functions (tapping on the display or signature capture) using an LXE approved stylus. The touchscreen has an actuation force with finger less than 100 grams.

The color display has an LED backlight and is optimized for indoor use. The display appears black when the mobile device is in Suspend Mode.

Power Supply

The LXE HX2 uses two batteries for operation. A Lithium-Ion (Li-Ion) battery supplies power to the HX2 only when tethered to the HX2. The main battery is either the 2000 mAh (Standard) or the 4000 mAh (Extended) battery. Only one main battery can be tethered to the HX2 at a time. The batteries can be hot-swapped after the HX2 is placed in Suspend mode.

The internal backup battery is a 50 mAh Nickel Cadmium (NiCad) battery. The backup battery is recharged indirectly by the HX2 with a tethered battery. Recharging maintains the backup battery near full charge at all times. When the backup battery is fully drained, it may take up to 5 hours to recharge. The capability to discharge the backup battery is provided (see the HX2 Battery Control Panel applet) to allow the user to condition the backup battery in order to recover full battery capacity. The backup battery must be replaced by qualified service personnel. The backup battery has a minimum 2 year service life.

When the HX2 is docked in a powered cradle, the HX2 receives USB/serial signals through the cradle connector on the bottom of the HX2 and the cradle connector in the HX2 docking bay. The HX2 must be firmly seated in the docking bay before USB/serial communication can occur. An extra standard or extended Li-Ion battery pack can be recharged in the powered cradle while one of the batteries is tethered to, and powering, the HX2. The standard battery is fully recharged in a powered cradle in 4 hours. The extended battery is fully recharged in 8 hours.

Note: *Docked HX2 -- An uninterrupted external power source (wall AC/DC adapter connected to the HX2 cradle) transfers signals from the USB ports in the front of the cradle and the serial port on the back of the cradle, to the HX2. HX2 frequent connection to a fully charged tethered battery, is recommended to maintain backup battery charge status, as the backup battery cannot be recharged by a dead or missing tethered battery.*

The LXE HX2 Multi-Charger is designed to simultaneously charge up to six standard HX2 Rechargeable Lithium Ion Battery Packs in less than four hours, depending upon battery pack temperature and ambient conditions. The Extended battery packs require less than 8 hours. The HX2 Multi-Charger can charge up to five Standard and Extended batteries when they are not tethered to the HX2. See section titled *HX2 Multi-Charger*.

Bluetooth LXEZ Pairing

The HX2 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains wireless connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to from the HX2. However, the HX2 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the HX2 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

Bluetooth will simultaneously support one printer as a slave Bluetooth device and one scanner, either as a slave or as a master Bluetooth device.

Blue LED	Blinking slowly	Bluetooth is active but not connected to a device.
Blue LED	Blinking medium	Bluetooth is paired and connected to a device.
Blue LED	Blinking fast	Bluetooth is discovering other Bluetooth devices.
Blue LED	Unlit	Bluetooth hardware has been turned off or does not exist in the HX2.

See *Chapter 3 System Configuration*, control panel section titled *Bluetooth*.

Barcode data captured by the Bluetooth scanner is manipulated by the settings in the **HX2 Scanner Properties** control panel applet**.**

Multiple beeps may be heard during a barcode scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the HX2 during final barcode data manipulation.

Input/Output Connectors

The HX2 has three I/O connectors. Two connectors are located next to each other on the back of the mobile device. Each of the two connectors (one for left-handed users and the other for right-handed users) interfaces with peripherals such as a Laser Ring Scanner, an Imager Ring Scanner, an audio headset and a tethered battery.

Connector 1	Located on the back of HX2 and can accommodate a: • Tethered Laser or Imager Scanner • Tethered Headset/Microphone and HX2 Battery • Tethered Battery
Connector 2	Located on the back of HX2 and can accommodate a: • Tethered Laser or Imager Scanner • Tethered Headset/Microphone and HX2 Battery • Tethered Battery
Connector 3	Located on the bottom of HX2 and can accommodate: • Cradle • Cradle Power Input • USB Keyboard and mouse through cradle

Figure 2-2 COM Ports

The third I/O connector is used when docking the HX2 in a cradle. The cradle has RS-232, USB Client, unpowered USB Host and Power connections. The power connection on the cradle supplies power to the battery charging bays. All communication is managed by the cradle.

Audio Support

Speaker

The internal speaker supplies audible verification signals normally used by the Window's CE operating system. The speaker is located on the front of the HX2, above the [2] key. The mobile device emits a Sound Pressure Level (loudness) of at least 102 dB measured as follows:

- Frequency: 2650 ± 100 Hz
- Distance: 10 cm on axis in front of Speaker opening in front of unit.
- Duration : Continuous 2650 Hz tone.

The default is 1 beep for a good scan and 2 beeps for a bad scan.

Volume Control

Volume control is managed by a Windows CE control panel applet, an API and key sequences.

To adjust speaker volume use the:

- **Blue+Up Arrow** and **Blue+Down Arrow** keys on the Alpha Mode 3 Tap keypad
- **Orange+Diamond 1+Up Arrow** and **Orange+Diamond 1+Down Arrow** keys on the Dual Alpha and Triple Tap keypads.

Volume control is covered in greater detail later in this guide.

Voice

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the "Tethered Headset/Microphone and HX2 Battery" accessory cable.

Power Modes

1. **On**

2. Tap Power key or Suspend timer has timed out

3. Power key, any key, scan button tap, or touch screen tap

4. **Suspend**

5. Tethered battery and backup battery depleted

6. **Off**

7. Power Restored and On key pressed
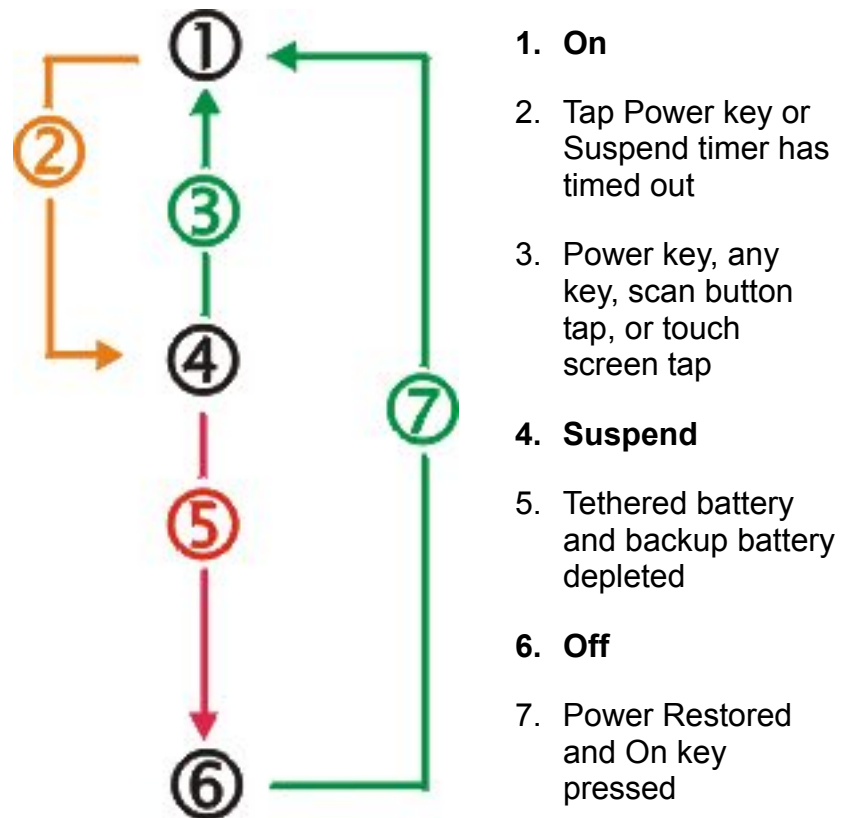
Figure 2-3 Power Modes – On, Suspend and Off

Primary Events Listing

Any key on the keypad	COM1 activity
Stylus touch on the touch screen	Docked in powered cradle
Power button tap	Bluetooth device reconnect / disconnect message
Ring scanner activity	

On Mode

The Display

When the display is On:

- the keypad, touchscreen and all peripherals function normally
- the display backlight is on until the Backlight timer expires

The HX2

After a new HX2 has been received, a charged battery tethered, and the Power key tapped, the HX2 is always On until both batteries are drained completely of power.

When the tethered battery and backup battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged battery is attached to the tether or external power is applied (for example, by docking the HX2 in a powered cradle) and the HX2 Power key is pressed.

Suspend Mode

The HX2

The Suspend mode is entered when the unit is inactive for a predetermined period of time or the user taps the Power key.

HX2 Suspend timers are set using ⊞ | **Settings** | **Control Panel** | **Power** | **Schemes tab**.

Any of the following primary events will wake the unit and reset the display / display backlight timers:

Any key on the keypad
Stylus touch on the touchscreen
Scan button on ring scanner pressed
Docked in a powered cradle
Power button tap

When the unit wakes up, the Display Backlight and the Power Off timers begin the countdown again. When any one of the above events occurs prior to the Power Off timer expiring, the timer starts the countdown again.

The HX2 should be placed in Suspend Mode before hotswapping the main battery.

Hotswapping the Ring Scanner does not require placing the HX2 in Suspend Mode.

Off Mode

The unit is in Off Mode when the tethered battery and the backup battery are depleted. Connect a fully charged main battery and press the Power key to turn the HX2 On.

Keypads

The HX2 has three keypad options for the 23-key keypad:

Alpha Mode 3 Tap	The HX2 default keypad on all HX2s shipped prior to September 2007. Setup requires no user interaction.
Dual Alpha	Set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped. Setup requires no user interaction with the My Device / Windows / Dual_Alpha.reg file.
Triple Tap	Requires file activation to setup the Triple Tap keypad for daily use. Setup requires the My Device / Windows / Triple_Tap.reg file be tapped and the HX2 warmbooted. Warmboot the HX2 by tapping Start	Run and, **using the SIP (virtual keyboard),** type WARMBOOT. Tap OK.

The Alpha Mode 3 Tap Keypad

The Alpha and Blue keys do not auto-repeat. Default timeout for any pressed key in any mode is 0.15 second.

Figure 2-4 Alpha Mode 3 Tap Keypad (Original)

See also: *Appendix A - Key Maps*.

Alpha Modifier Key

Tap | **Settings** | **Control Panel** | **KeyPad Control Panel** icon.

Persistent – By default, the Alpha key is persistent. Disable the radio button to disable Alpha key persistence. The Alpha mode LED is turned on when the Alpha mode is on.

When Persistent is enabled, the behavior of the Alpha modifier key is as follows:

- Pressing the Alpha key once toggles the Alpha mode and the orange LED illuminates.
- Pressing the Alpha key twice quickly (roughly twice in half a second) sets the Alpha mode and enables upper case (regardless of the previous state of the Alpha key). The orange LED illuminates.

If Alpha persistence is set to Off, the orange LED is off and Alpha mode is exited when a different key is pressed.

Pressing the Blue key modifier On or Off does not change the state of the Alpha mode.

The Alpha key does not need to be held down when another key is pressed.

When the Alpha key is kept pressed down while another key is pressed, then the Alpha mode is considered On (therefore the Alpha LED will turn on when the button is pressed, not when it is released). In this case, the Alpha mode is exited when the user releases the Alpha key, no matter if persistence is set to On or Off.

On the fourth (or fifth for the 7 and 9 keys) keyclick using a number key, in Alpha mode, the result is the specific number.

Blue Modifier Key

Pressing the Blue key once toggles the Blue mode. The Blue mode is exited when a key is pressed (including the Alpha key).

The Blue key does not need to be held down when another key is pressed.

When the Blue key is kept pressed down while another key is pressed, then the Blue mode is considered On. In this case, the Blue mode is exited when the user releases the Blue key.

See also: *Appendix A - Key Maps*.

Mappable Keys

Tap ⊞ | **Settings** | **Control Panel** | **KeyPad Control Panel** icon.

There are 29 key combinations that can be mapped using the KeyPad Control applet.

Key functions shown in the table below (available on most 101-key keyboards) can be mapped to any of the 29 key combinations.

CTRL	ALT	DELete
Function Keys F9 and F20	Insert	Shift
Print Screen	SysRq	Scroll Lock
Pause	NumLock	Home
PageUp	PageDown	End

Use the Input Panel to insert the following characters:

< >	{ }	[ ]	( )	_	+
: ;	" '	? /	~ `	!	@
#	$	%	^	&	|

See *Appendix A – Key Maps* for instruction on the specific keypresses to access all keypad functions.

The mappable keys can be mapped by the user to generate any key code defined by Windows CE.

The Dual Alpha Keypad

Set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped.

Setup requires no user interaction with the My Device / Windows / Dual_Alpha.reg file.

Features

- The Dual Alpha keypad modifier keys are the Green, Orange, Blue, Shift and Control (CTRL) keys.
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Alpha keys are accessed by two taps: a modifier key and a number key.
- Orange Alpha LED near the Backspace key has no function on this keypad.
- Any key press exits volume control mode. Any key press exits backlight control mode.
- F1 through F10 function keys are available using the keypad. Function keys F11 through F24 require multiple keypresses.
- Keys can be mapped by the user to generate any key code defined by Windows CE.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Figure 2-5 Dual Alpha Keypad

See *Appendix A – Key Maps* for instruction on the specific keypresses to access all keypad functions.

Note: The keypad is installed and activated by LXE prior to shipment. Contact LXE Customer Support for assistance.

The Triple Tap Keypad

Requires file activation to setup the Triple Tap keypad for daily use.

Setup requires the My Device / Windows / Triple_Tap.reg file be tapped and the HX2 warmbooted. Warmboot the HX2 by tapping Start | Run and, using the Soft Input Panel (SIP), type WARMBOOT. Tap OK.

Features

- The modifier keys are the Green, Orange, Blue, Shift and Control (CTRL) keys.
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Alpha keys are accessed by several taps: the blue modifier key and one to four taps of a number key. Capital keys also require a Shift key tap.
- The orange Alpha LED has no function on this keypad and is off.
- The default timeout for any Alpha key is 0.15 second.
- Any key press exits volume control mode. Any key press exits backlight control mode.
- F1 through F10 function keys are available using the keypad. Function keys F11 through F24 require multiple keypresses.
- Keys can be mapped by the user to generate any key code defined by Windows CE.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Figure 2-6 Triple Tap Keypad

The alphabet characters wrap for keys 2 – 9, for example:

- Blue + 2 produces a lower case a
- Blue + 22 produces a lower case b
- Blue + 222 produces a lower case c
- Blue + 2222 produces the number 2

See *Appendix A – Key Maps* for instruction on the specific keypresses to access all keypad functions.

Touchscreen

Figure 2-7 Touchscreen

The VGA display with touchscreen is an active TFT color unit capable of supporting VGA graphics modes at 50 dpi or greater. Display size is 320 x 240 pixels in landscape orientation; the diagonal viewing area is 2.5 inches (6.3 cm). The covering is designed to resist stains and has an anti-glare and anti-reflective coating. The touchscreen allows signature capture and touch input. The touchscreen responds to an actuation force (touch) of 4 oz. of pressure (or less).

The color display is optimized for indoor lighting. The LED backlight can be adjusted using the arrow keys. The display is black when the device is in suspend mode or when both batteries have expired and the unit is Off.

Touchscreen protective film is available from LXE. See *Accessories*.

Batteries

The HX2 is designed to work with a Lithium-Ion (Li-ion) tethered battery from LXE. Under normal conditions it should last approximately eight to ten hours before requiring a recharge. The more you use the ring scanner or the wireless transmitter, the shorter the time required between battery recharges.

A suspended HX2 maintains the date and time for a minimum of two days while tethered to a battery that has reached the Low Warning point and a fully charged backup battery. The HX2 retains data, during a battery hot swap, for at least 5 minutes.

Note: ***New battery packs must be charged prior to use***. *The Standard batteries require less than four hours and the Extended batteries require less than 8 hours.*

Checking Battery Status

Tap the | **Settings** | **Control Panel** | **Power** | **Battery** tab. Battery level, power status and charge remaining is displayed. Turbo setting is enabled/disabled using this applet.

Note: Battery power drain increases substantially in Turbo mode.

HX2 Status LED and the Batteries

When the LED is . . .	The Status is . . .	Comment
Blinking Red	Main Battery Power Fail	Replace the main battery with a fully charged main battery.
Steady Red	Main Battery Low	Low Battery Warning. If the main battery is not replaced with a fully charged battery before the main battery fails, the HX2 is turned Off.
No Color	Good	No user intervention required.

Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the HX2 Multi-Charger, HX2 Cradle or the HX2 unit.

Whenever possible, protect the battery charging terminals (five small round circles) by keeping them covered by the battery sleeve fabric. The battery pack is resistant to impact damage.

Under normal conditions a properly tethered Standard battery should last a minimum of approximately eight hours before requiring a recharge, the Extended battery a minimum of approximately 16 hours.

Battery Hotswapping

Important: When the backup battery power is Low or Very Low (⊞ | **Settings** | **Control Panel** | **Power** | **Battery** tab) dock the HX2 in a powered docking cradle *before* replacing the battery pack.

When the main battery power level is low, the HX2 will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the HX2 using a powered cradle.

You can replace the main battery by first placing the device in Suspend Mode then removing the discharged main battery and tethering a charged main battery within a five minute time limit (or before the backup battery depletes).

When the main battery is disconnected the device enters Critical Suspend state, the HX2 remains in Suspend mode, the display is turned off and the backup battery continues to power the unit for at least five minutes. Though data is retained, the HX2 cannot be used until a charged main battery pack is connected. After tethering the full battery, press the Power key.

Full operational recovery from Suspend can take several seconds while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the HX2 startup completes, and Bluetooth relationships establish or re-establish.

If the backup battery depletes before a fully charged main battery can be inserted, the HX2 will turn Off.

Low Battery Warning

It is recommended that the main battery pack be removed and replaced when its energy depletes. When the main battery Low Battery Warning appears (the Status LED remains a steady red) perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be saved.

Note: Once you receive the main battery Low Battery Warning, you have approximately 5 minutes to perform an orderly shutdown and replace the main battery pack before the device powers off. The Low Battery Warning will transition the mobile device to Suspend before the device powers off.

Backup Battery

The HX2 has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times comes from the HX2 main battery.

It takes several hours of operation before the backup battery is capable of supporting the operation of the mobile device. The duration of backup battery life is dependent upon operation of the HX2, its features and any operating applications.

The backup battery has a minimum service life of two years. The backup battery is replaced by LXE.

The backup battery can be discharged, recharged and conditioned using a CE Control Panel applet. Tap ⊞ | **Settings** | **Control Panel** | **Battery** then tap the Discharge button.

Handling Batteries Safely

- Never dispose of a battery in a fire. This may cause an explosion.
- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.

Caution ⚠️	Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention. NiCd and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

HX2 Multi-Charger (Optional)

The LXE HX2 Multi-Charger is designed to simultaneously charge up to six HX2 Rechargeable Lithium Ion Batteries at a time, in any combination of Standard or Extended batteries. The Standard batteries require less than four hours and the Extended batteries require less than 8 hours. Total charging time required depends upon battery pack temperature and conditions. There is one bay that is used for Charging only when the Analyze button is not pressed.
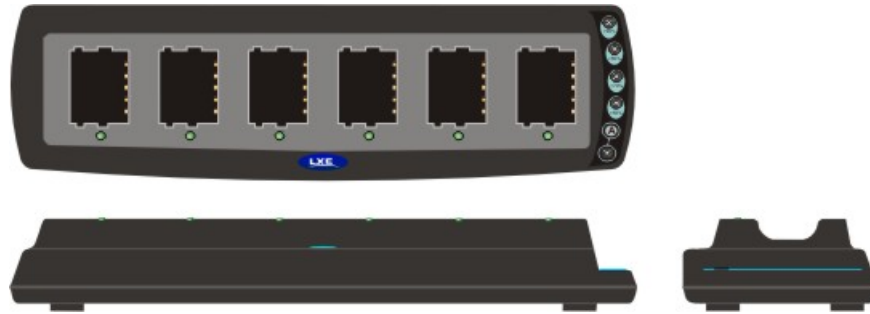
Figure 2-8 HX2 Multi-Charger

Charging Pocket LEDs

LED 🟢	Indication	Description
Off	No Battery/power	Battery pack not plugged in or no power applied.
Green	Charged	Battery pack fully charged.
Red	Charging	Battery pack charging.
Yellow	Standby	Battery pack temperature out of range.
Flashing Red on any station	Fault	Battery pack fault or failure.
Flashing Red on any station	Timeout	Battery analyzer's 4.5 hour timeout period expired.
Flashing Red on all stations.	Charger/Analyzer Failure	Battery analyzer fault or failure.

Charger/Analyzer LEDs

Percentage of Battery Capacity		Between 90% and 100%	Between 80% and 90 %	Between 70% and 80%	Between 50% and 70%
Analyze Progress LED Status		● On	● Off	● Off	● Off
		● On	● On	● Off	● Off
		● On	● On	● On	● Off
		● On	● On	● On	● On
		When all LEDs are off, the battery capacity is less than 50%.			

Figure 2-9 Multi-Charger Control Panel

Refer to the *HX2 Multi-Charger User's Guide* for instruction in setting up the charger, inserting the battery packs into the charging bays, interpreting the LEDs and using the Charge/Analyze Pocket.

HX2 Docking/Charging Cradle

The HX2 desktop cradle secures the HX2 with or without a protective rubber boot, recharges the tethered HX2 battery and a spare battery (Standard and Extended), has a protected storage bay for the tethered Ring Scanner when the HX2 is docked, and enables serial communication with USB devices (host, client, and other USB cabled devices).

HX2 keypad data entries can be mixed with ring scanner barcode data entries while the HX2 is docked in a cradle.

Using an external power supply the HX2 cradle recharges Standard batteries in approximately 4 hours (8 hours for the Extended battery). The HX2 does not need to be docked during a spare battery charging process. See *Accessories*.

Remove the voice case before placing the HX2 in the cradle. The HX2 cannot be docked in a cradle while it is mounted in a hip flip or arm band.

Figure 2-10 Powered Cradle LEDs

The cradle LEDs are on the front of the cradle.

1	B1 LED – Back left battery charging bay	Normal State – Off. With battery and AC power, normal state may be any state listed in *Cradle LED*s.
2	PWR LED - HX2 docked / on / receiving power bay	Normal State – Off. With HX2 in, turned On and AC power, normal state is On.
3	B2 LED – Back right battery charging bay	Normal State – Off. With battery and AC power, normal state may be any state listed in *Cradle LED*s.

IMPORTANT –

- Do not put the HX2 into Suspend Mode (using Start | Suspend or by tapping the Power key) while the HX2 is connected to peripheral devices (or ActiveSync) through the connectors on the cradle. The HX2 is unable to maintain the connection during Suspend Mode.
- If the USB connections are interrupted due to a Suspend operation – then when the HX2 resumes, disconnect the cables and then reconnect the cables again to initiate USB and/or ActiveSync connection again.

Cradle LEDs

Cradle PWR LED

When PWR LED is …	It means ….
Off	No AC/DC power supplied to the cradle and/or No HX2 in the charging bay and/or HX2 is not properly seated in charging bay and/or if this is the first time the HX2 has been inserted, the HX2 is properly seated and has not been powered On.
Green	HX2 is On, is properly seated in the charging bay and is receiving external power through the cradle.

B1 and B2 LED

When B1 and/or B2 LED is …		It means ….
Off	No battery or no AC power	No spare battery in the battery bay(s) or no AC/DC power is being applied to the cradle.
Green	**Charged**	Spare battery pack fully charged.
Red	**Charging**	Spare battery pack charging.
Amber	**Standby**	Spare battery pack temperature out of range.
Flashing Red	**Fault**	Spare battery pack fault or failure.

Refer to the *HX2 Cradle Reference Guide* for instruction in setting up the cradle, inserting the battery packs, interpreting the LEDs, connecting cables and using the cradle for powering the HX2 and communication.

Chapter 3 System Configuration

Introduction

There are several different aspects to the setup and configuration of the HX2. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this chapter are to be used *as examples only*, the configuration of your specific mobile device may vary. The following sections provide a general reference for the configuration of the HX2 and some of it's optional features.

Note: LXE recommends frequently charging the HX2 tethered battery using an external power source (a powered cradle) to ensure continuous charging of the backup battery.

Windows CE 5.0

For general use instruction, please refer to commercially available Windows CE guides or the Windows CE on-line Help application installed with the HX2 operating system.

This chapter's contents assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows XP (or later) desktop computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the HX2 and its Windows CE environment.

> **Note**:
>
> The HX2 reloads the operating system upon every warm boot or cold boot. Anything not saved or preserved to the registry is lost.
>
> In *warm boot*, the OS and the CAB files are reloaded from the internal SD card and the preserved registry is also reloaded.
>
> During *cold boot*, the system behavior is identical to warm boot with the addition that the registry is erased, forcing the HX2 to reboot with factory defaults. The registry is recreated when 20 minutes of uptime elapses or upon the first save or suspend function. It is also recreated every 10 registry changes and at every warm boot.

Installed Software

Note: Some standard Windows options require an external modem connection. Modems are not available from LXE nor supported by LXE.

When you order an HX2 you receive the software files required by the separate programs needed for operation and wireless communication. The files are loaded by LXE and stored in folders in the HX2.

This section lists the contents of the folders and the general function of the files. Files installed in each HX2 are specific to the intended function of the HX2.

Software Load

The software supported by the HX2 is summarized below.

Operating System	Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer for Windows CE browser and utilities.
Wireless Client Drivers	The 2.4GHz Summit wireless client driver is pre-loaded by LXE.
Bluetooth Client Driver	Optional.
Wavelink Avalanche	Optional.
Java	Optional. Java executables and browser components are handled by the Java option (when installed).
Terminal Emulation	Optional: RFTerm (VT220, TN5250, TN3270).
LXE API Routines	See *Accessories* for the LXE SDK Kit part number

Note: Please contact your LXE representative to get access to CAB files as they are released by LXE.

Software Applications

The following applications are included:

- WordPad
- Pocket Inbox
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer
- Scanner Wedge (LXE developed)
- AppLock (LXE developed)
- Media Player
- ActiveSync
- Internet Explorer

Note that the Viewer applications allow viewing documents, but not editing them.

Software Backup

Application programs and data that are normally RAM resident are backed up via ActiveSync, as well as being stored on the internal SD card. The operating system is on internal SD card and does not need backup. Registry configuration is backed up to internal SD card automatically using the hive registry setup from CE 5.0. Registry backup occurs on every Suspend, WARMBOOT.EXE, every 20 minutes and every 10 registry changes.

Version Control

Version numbers are applied to the boot loader and the OS image independently. The version information stored consists of the LXE build number, plus the date and time of compile (in lieu of a build number). These version numbers are stored in non-volatile storage, where the user cannot inadvertently modify them. A control panel and API is provided so the user can reference the version numbers for support purposes.

The HX2 has a unique 128-bit ID code as required by the CE 5.0 specification. This ID number is generated by the boot loader. This ID code is available in the control panel, and via a Win32 standard API.

In addition, an API is provided to return a standard LXE copyright string, so that applications may reference this to be sure they are running on an LXE mobile device for licensing purposes.

See *Accessories* for the LXE HX2 SDK Kit part number.

Boot Loader

The HX2 supports a proprietary boot loader. It is the responsibility of the boot loader to:

- Initialize all system hardware
- Load code into internal FPGA device(s)
- Load the OS image from SD card to DRAM
- Initiate OS startup
- Handle wakeup from system suspend, loading saved state
- Handle copying a new boot loader from SD card to internal flash

The HX2 reloads the OS every time during warm boot or cold boot. In Warm Boot (i.e., the user executes a Warm Boot) the OS and the CAB files are reloaded from the internal SD card and the preserved registry is also reloaded. Anything else (user data), which was not preserved in the registry, is lost. During Cold Boot (i.e., user executes a Cold Boot utility) the system behavior is identical to Warm Boot with the addition that the registry is reloaded with factory defaults.

The SD card holds user applications and CAB files. The SD card is mapped to the System folder in the Windows CE file system.

Folders Copied at Startup

The following folders are copied on startup:

System\Desktop	copied to	Windows\Desktop
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs

Copying these folders at startup saves any changes made by the user. For example, saving user-installed fonts and help files and tailoring the desktop and programs menus to meet the user's needs.

This function copies only the directory contents, no sub-folders.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by the launch process.

Optional Software

Bluetooth

Only installed on a Bluetooth equipped HX2. The System Administrator can Discover and Pair targeted Bluetooth devices for each HX2. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly Name for each HX2. The Bluetooth control panel can be accessed by tapping **Start | Settings | Control Panel | Bluetooth**, the desktop icon, or by double-tapping the Bluetooth icon in the taskbar.

JAVA

Installed by LXE. Files can be accessed by tapping **Start | Programs | JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of JAVA examples and Plug-ins is also installed with the JAVA option. LXE does not support all JAVA applications running on the mobile device.

LXE RFTerm

Installed by LXE. The application can be accessed by tapping **Start | Programs | RFTerm**. Please refer to *Terminal Emulation Setup* earlier in this guide for RFTerm quick start instruction. Refer to the *RFTerm Reference Guide* on the LXE Manuals CD for complete information and instruction. WAV files added by the user should be stored in System\LXE\RFTerm\Sounds.

Wavelink Avalanche Enabler

Related Manual: *Using Wavelink Avalanche on LXE Windows Computers*.

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager. After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

The HX2 has the Avalanche Enabler installation files loaded, *but not installed,* on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. The designation of the mobile device to the Avalanche CE Manager is LXE_HX2.

See *Wavelink Avalanche Enabler Configuration* at the end of this chapter for instruction.

If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

Desktop

For general use instruction, please refer to commercially available CE user's guides or the CE on-line Help application installed in the HX2.

Note: Whenever possible, dock the HX2 in a powered cradle to conserve the main battery and to ensure the backup battery is charged.

The HX2 Desktop appearance is similar to that of a desktop PC running Windows XP.

At a minimum, it has named icons that can be tapped with the stylus to access My Computer, Internet Explorer, and the Recycle Bin.

At the bottom of the screen is the Start button. Tapping the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

The Start Menu Shutdown option found on most desktop PC's has been replaced with a single command: **Suspend** because the HX2 is always powered On (when a fully charged tethered battery and backup battery are present).

Tap the Suspend button, or tap the red Power button, to turn the screen off and place the HX2 into Suspend mode.

Tap the Power button to Resume all paused functions and wake the unit up.

Note: There may be more or fewer icons on your desktop than those listed below in the LXE default Desktop table.

Desktop Icon	Function
My Device	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Internet Explorer	Connect to the Internet/intranet (requires a wireless transmitter and Internet Service Provider – please note that ISP enrollment is not available from LXE).
Summit Client	Used for configuring Summit client for network security settings.
My Documents	Storage for downloaded files / applications.
Start	Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help, run programs or place the unit into Suspend mode.

My Device Folders

Folder	Description	Preserved upon Coldboot?
Application Data	Data entered by the end-user and saved by the running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Profiles	Network user profiles	No
Program Files	Applications	No
System	Internal SD Flash Card	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	Yes

Start Menu Program Options

The following options represent the factory default program installation. Your system may be different based on the software and hardware options purchased.

Access: ⊞ **| Programs**

Communication	Stores Network communication options
ActiveSync	Begin ActiveSync connection
Get Connected	Run this command after setting up a connection
Remote Control	Manage HX2 files using ActiveSync
Start FTP Server	Begin connection to FTP server
Stop FTP Server	Stop connection with FTP server
VOIP Demo	Voice over IP demo
Microsoft File Viewers	View downloaded files (see Note)
Excel Viewer	View Excel documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word and RTF files
Command Prompt	The command line interface in a separate window
Inbox	Microsoft Outlook mail inbox.
Internet Explorer	Access web pages on the world wide internet
Java	Option.
LXE RFTerm	Option. Terminal emulation application. RFTerm automatically opens as soon as a reboot is completed.
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Radio Config Utility	Radio management program. WZC icon in toolbar.
Remote Desktop	Microsoft Remote Desktop Connection program.
Summit Client	RF client management program.
Transcriber	Handwriting recognition program using an integrated dictionary.
Wavelink Avalanche	Option. Remote management for networked devices.
Windows Explorer	File management program

Note: The Microsoft File Viewers cannot display files that have been password protected or encrypted.

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to paired devices automatically at the conclusion of each reboot.
- If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

Communication

Access: 🟦 **| Programs | Communication**

Note: *Some communication menu options require an external modem connection to the HX2.*
          Modems are not available from LXE nor supported by LXE.

ActiveSync

Once a relationship (partnership) has been established between the HX2 and a desktop computer, ActiveSync can synchronize using the network link or USB port on the HX2.

Refer to *ActiveSync / Get Connected Process* later in this chapter for more information and instruction.

To initiate synchronization (or network link) from the mobile device that already has a relationship with the desktop computer, tap 🟦 **| Programs | Communication | ActiveSync** to begin the process.

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

Connect

Connect is used to initiate a hardwired connection to a host and to create the initial partnership for synchronizing wirelessly.

The default connect setup is USB direct connect.

After a Connect setup is selected, 🟦 **| Programs | Communication | Connect** will start to connect to a host.

See Also: *Cold Boot and Loss of Host Re-connection*

Remote Display

Access: 🟦 **| Programs | Communication | Remote Display**

Equipment Required: *HX2 USB ActiveSync Cable. Desktop/laptop computer.*

Remote Display is used with ActiveSync to display the contents of the HX2 file structure on a desktop/laptop computer screen. Once connected, the desktop keyboard and mouse can be used to manipulate files, data or settings on the HX2.

Before using Remote Display, refer to the following processes outlined in *ActiveSync / Get Connected Process* for information and instruction:

- "Initial Install | USB Connection"
- "Initial Install | Connect – Initial Install Process"
- "Explore"
- "Disconnect"

Note: *Initial ActiveSync connection requires a USB connection, subsequent connections can be*
          either USB or RS-232 serial. When the HX2 enters Suspend, an established ActiveSync
          connection is maintained. Refer to "ActiveSync / Get Connected Process" for full details.

1.   Run ActiveSync on the desktop/laptop.

2. Connect the HX2 to the desktop computer using the USB cable. Follow the instructions on the desktop to set up a partnership (LXE recommends choosing the *No* option to set up the HX2 as a guest).
3. Select the ActiveSync menu option Explore and the file structure of the HX2 is displayed in the HX2 window on the desktop monitor.
4. Files on the desktop computer can be dragged to a folder in the HX2 window on the desktop monitor and dropped to add them to the HX2.
5. ActiveSync converts the file to run on a CE device automatically during the transfer.
6. To close or disconnect the ActiveSync connection with the HX2, disconnect the USB connector first. ActiveSync on the desktop closes. Remote (Display) Control on the HX2 closes.

Refer to "ActiveSync / Get Connected Process" for full details.

Start / Stop FTP Server

Access: | **Programs | Communication |**
Start FTP Server *or*
Stop FTP Server

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

VoIP Demo

LXE proof of concept unsupported demo application. Contact your LXE representative for availability / assistance.

Command Prompt

Access: ⊞ **| Programs | Command Prompt**
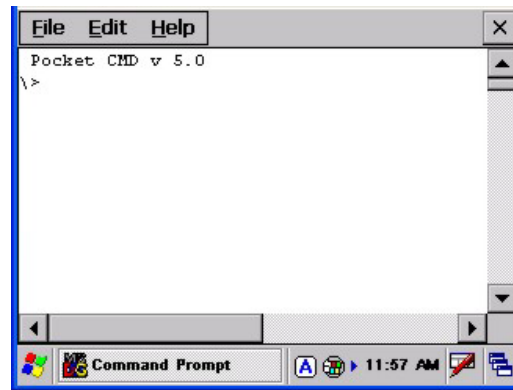
Figure 3-1 Pocket CMD Prompt Screen

Type help at the command prompt for a list of available commands. Exit the Command Prompt by typing exit at the command prompt or select File | Close.

Inbox

Access: ⊞ **| Programs | Inbox**

This option requires a connection to a mail server. There are a few changes in the CE version of Inbox as it relates to the general desktop Windows PC Microsoft Outlook Inbox options. Tap the ? button to access Inbox Help.

ActiveSync can be used to transfer messages between the HX2 inbox and a PC's desktop inbox. Refer to *ActiveSync Processes* in this guide.

Internet Explorer

Access: ⊞ **| Programs | Internet Explorer**

The default start page is www.lxe.com and the default search page is www.google.com.

See section titled *Internet Options* later in this chapter for Internet Explorer settings.

Internet Explorer requires a network card and an Internet Service Provider to access the Internet. There are a few changes in the CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options.

Select View | Options to setup General, Connection, Security, Privacy, Advanced, and Popup options when connecting to the Internet.

Tap the ? button to access Internet Explorer Help.

Media Player

Access: | Programs | Media Player

There are few changes in the CE version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options.

Select View | Options to setup Buffering, Playback and Media Network Share options when connecting to the Internet. This option requires a network card and an Internet Service Provider.

Tap the ? button to access Media Player Help.

Microsoft WordPad

Access: | Programs | Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad. By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g. .RTF or .DOC.

Tap the ? button to access WordPad Help.

Summit Client

Access: [win] **| Programs | Summit**

Summit automatically installs and runs after every cold and warm boot.

Disable Summit	**Start	Programs	Summit	SCU**
Tap the Disable Radio button. The wireless device is enabled by default after every cold reset.	
Enable Summit	**Start	Programs	Summit	SCU	Enable Radio**
When the wireless device is disabled, tap the Enable Radio button. The wireless device is enabled by default after every cold reset.	

See *Chapter 5 - Wireless Network Configuration* for Summit Client Utility setup information and instruction.

Certs

Access: [win] **| Programs | Summit | Certs**

Contents of README.TXT file located in Start | Programs | Summit | Certs menu option:

CA Certificate files, user certificate files and PAC files are accessed only from this location. When entering the certificate filenames in the Summit Client Utility (SCU), only the filename and extension are entered. Only PEM, DER and PFX extensions are allowed for certificate files.

See *Chapter 5 - Wireless Network Configuration* for directions for acquiring CA and user certificate files.

Wireless Zero Config Utility and the Summit Client

This utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the application is enabled and the HX2 is not connected to a network.

If you will be using the Wireless Zero Config Utility to configure the network card, or connect to a network, perform the following steps:

1. Tap the Summit Client Utility icon on the desktop, or tap **Start | Programs | Summit | SCU**.
2. Select **ThirdPartyConfig** in the Active Config drop down box.
3. A message appears that a Power Cycle is required to make settings activate properly. Tap **OK** to close the message window.
4. Tap the **Power** button to place the HX2 in **Suspend**, then tap the Power button to **wake the HX2** from Suspend mode.

The Wireless Zero Config utility begins.

Transcriber

Access: **| Programs | Transcriber**

Select Transcriber on the **Start | Programs** menu or tap the Input Panel icon in the toolbar and tap Transcriber. When active, a "hand with a pen" icon is displayed in the taskbar. Make changes to the Transcriber application, enable or disable the current Transcriber session by tapping the "hand with a pen" icon in the toolbar. When Transcriber is enabled, all touchscreen activity is captured/read by the Transcriber program.

Tap the ? button or the Help button to access Transcriber Help.

Windows Explorer

Access: **| Programs | Windows Explorer**

There are a few changes in the CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the ? button to access Windows Explorer Help.

Taskbar

Access: **| Settings | Taskbar …**

The Taskbar can be used to determine how the taskbar appears on the display. Use the Advanced tab to clear the contents of the Documents menu.

Factory Default Settings	
General	
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled
Advanced	
Expand Control Panel	Disabled

There are a few changes in the CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

Figure 3-2 Taskbar General Tab

Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the **Settings | Control Panel** menu option. When it is unchecked, the Control Panel Properties screen is displayed.

Figure 3-3 Advanced Tab

Clear Contents of Document Folder
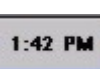
Tap the Clear button to remove the contents of the *Recently Opened* Document folder.

Taskbar Icons

As HX2 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to | **Help** for an explanation of standard Windows CE taskbar icons.

Following are **a few** of the HX2 and LXE unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

	Wireless Client Connected / Not Connected
	Bluetooth
	ActiveSync Connection
1:42 PM	Current Time
	Summit Client signal strength.

Settings | Control Panel Options

Access: *[icon]* **| Settings | Control Panel** or **My Device | Control Panel link**

Getting Help

Please tap the ? button to get Help when changing Settings options.

Option	Function
About	Software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility. See Chapter 6 for details.
Battery	View voltage and status of the main and backup batteries. Battery charge and discharge is performed using this option.
Bluetooth	Set the parameters for Bluetooth device connections.
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Dialing	Set dialup properties for internal modems (Modems are not supplied or supported by LXE).
Display	Set background graphic and scheme. Set backlight properties and timers.
Input Panel	Select the current key / data input method. Select custom key maps.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
Keypad	Configure Alpha key, Mappable keys, RunCmd and LaunchApp.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.

Option	Function
Password	Set HX2 access password properties for signon and/or screen saver.
PC Connection	Control the connection between the HX2 and a local desktop/laptop computer.
Power	Set Power scheme properties. Review device status and properties..
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Select to remove specific user installed programs in their entirety. *Note: Programs listed in this location are deleted upon warm and cold boot processes.*
Scanner	Set scanner key wedge, scanner port, and imager LED illumination options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign scanned data manipulation parameters.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound wav files to CE events.

Note: Change the font displayed on the screen by choosing ⊞ | Settings | Control Panel | Keyboard and then the Key map dropdown list.

About

Access: 🏁 **| Settings | Control Panel | About**
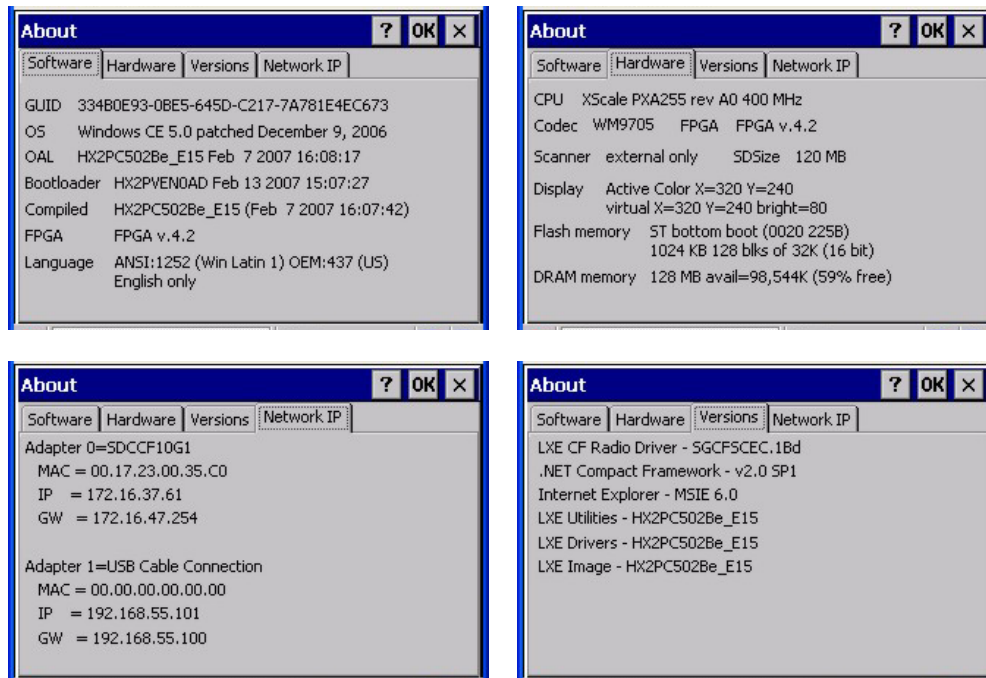
Figure 3-4 Control Panel – About

The About panels display hardware and software details. The data cannot be edited by the user.

The Software tab Language parameter indicates any pre-installed Asian fonts.

User application version information can be shown in the Version window. Version window information is retrieved from the registry.

Modify the Registry using the Registry Editor (see section titled *Utilities*). LXE recommends caution when editing the Registry and also recommends making a backup copy of the registry before changes are made.

The registry settings for the Version window are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

Create a new string value under this key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Accessibility

Access: ⊞ **| Settings | Control Panel | Accessibility**

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general desktop Accessibility options. Adjust the settings and tap the OK button to save the changes. The changes take effect immediately.
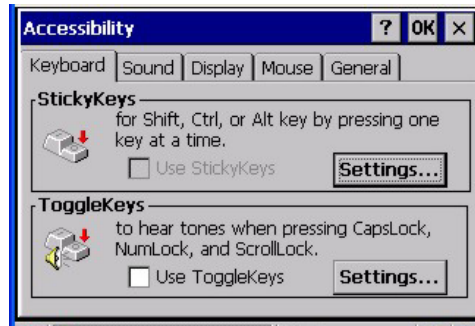
Figure 3-5 Control Panel – Accessibility

The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, please note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selection, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Administration – For AppLock

Access: ⊞ **| Settings | Control Panel | Administration**

Use this option to set parameters for mobile devices that are intended to be used as dedicated, single or multiple application devices. In other words, only the application or feature specified in the AppLock configuration by the Administrator are available to the end-user.

LXE devices with the AppLock feature are shipped to start up in Administration mode with no default password, and when the device is started for the first time, the user has full access to the mobile device and no password prompt is displayed. After the Administrator specifies an application or applications to lock, assigns a password and the device is rebooted (or the AppLock hotkey is pressed), the mobile device is then in end-user mode.

AppLock also contains a component which sets configuration parameters as specified by the Administrator.

See *Chapter 6 - AppLock* for further information and instruction.

Battery

Access: ⊞ **| Settings | Control Panel | Battery**

View the status of the Main and Backup batteries.
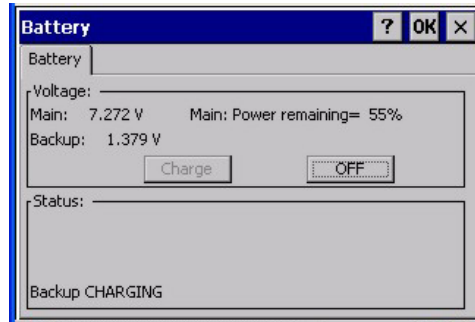
Figure 3-6 Control Panel – Battery

The Battery tab shows the status and the percentage of power left in the main battery. It also shows the status of the backup battery. The listed values cannot be changed by the user.

LXE recommends Discharging and Recharging the *backup battery* twice a year. Use the Charge or Discharge buttons to charge and discharge the backup battery:

To Charge Backup Battery   Tap the Charge button. The Discharge button text changes to "Off". When the backup battery is Charging, tap the Off button to stop the Charge process.

To Discharge Backup Battery   Tap the Discharge button. The Charge button text changes to "Off". When the backup battery is discharging, tap the Off button to stop the Discharge process.

The Main Battery is charged/recharged when the HX2 is docked in a powered cradle and the battery is inserted in a cradle charging bay. It is also charged/recharged when the battery is disconnected from the HX2 and then placed in a charged HX2 Multi-charger.

Bluetooth

Access: ![Windows icon] **| Settings | Control Panel | Bluetooth**

Discover and manage pairing with nearby Bluetooth devices. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored. Your Bluetooth panel setups may be different than those shown on the following pages.

Factory Default Settings	
Discovered Devices	None
Settings	
Turn Off Bluetooth	Enabled
Report when connection lost	Enabled
Report when connected	Disabled
Report failure to reconnect	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Disabled
Continuous search	Disabled

Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the HX2.

- The HX2 default Bluetooth setting is On.
- The HX2 cannot be discovered by other Bluetooth devices when the *Computer is discoverable* option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- The HX2 can pair with one Bluetooth scanner and one Bluetooth printer.
- Paired scanners and printers connections must be deleted before a different scanner or printer can be paired with the HX2.
- The Bluetooth remote device should be as close as possible, and in direct line of sight, with the HX2 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the HX2.
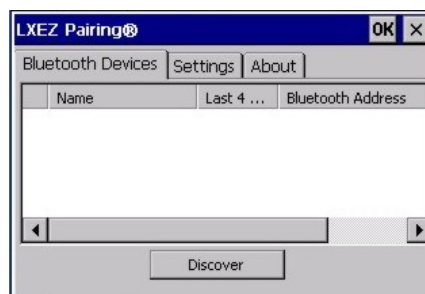
Figure 3-7 Control Panel - Bluetooth

Tap the Discover button to locate all discoverable nearby Bluetooth devices. The Discovery process also queries for the unique identifier for each device discovered.
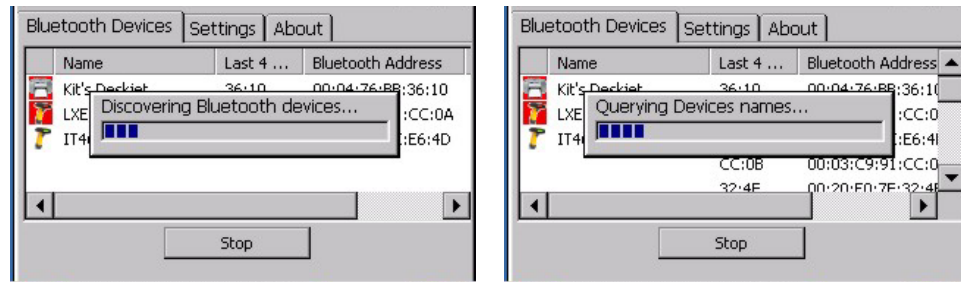
Figure 3-8 Discover Bluetooth Devices and Query Device Data

Bluetooth Devices

A device previously discovered and paired with the HX2 is shown in the Bluetooth Devices panel. Previously paired device data is persistent through warmboot and Suspend/Resume functions.

Figure 3-9 Bluetooth Devices Panel

Note: *When an active paired device, besides the HX2, enters Suspend Mode, is turned Off or leaves the HX2 Bluetooth scanning range, the Bluetooth connection between the linked device and the HX2 is lost. There may be audible or visual signals as paired devices disconnect from the HX2. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.*

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as printers or scanners; the Bluetooth panel will assign an icon to the device name once paired.

An icon with a red background indicates the devices Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the HX2 and the devices Bluetooth connection is active.

Inactive devices can be deleted from the list. Active devices can be disconnected from the HX2 and remain on the list.

Doubletap a device in the list to open the device properties menu.
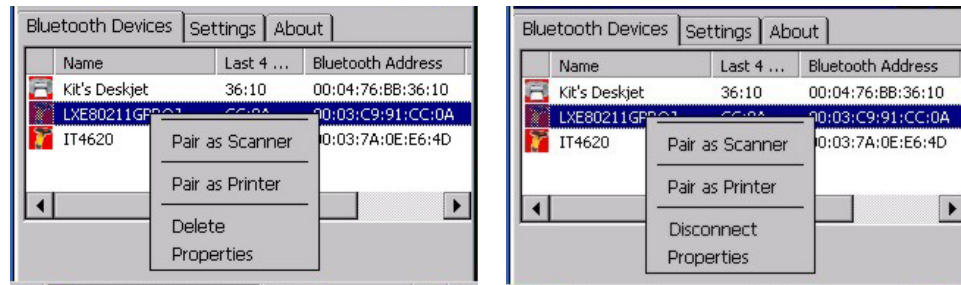
Figure 3-10 Bluetooth Device Pair / Delete / Disconnect Menu

Tap **Pair as Scanner** to set up the HX2 to receive scanner data.

Tap **Pair as Printer** to set up the HX2 to send data to the printer.

Tap **Delete** to delete an inactive device (icon with red background) from the HX2 paired device database. Close the LXEZ Pairing control panel to erase the device from the list after deleting.

Tap **Disconnect** to disconnect an active device (icon with white background) from the HX2 paired device database. The icon background turns red and the device remains in the list.
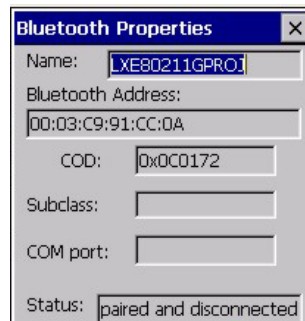
Figure 3-11 Bluetooth Device Properties Menu

Tap **Properties** to view the status of a device. The data displayed is the result of the device Query performed during the Discovery process.

Data on the Bluetooth Properties panel cannot be changed by the HX2 user.

Settings

Figure 3-12 Bluetooth Settings Panel

Turn Off Bluetooth Button

Tap the button to toggle Bluetooth hardware On or Off. When Off, the Bluetooth LED is turned off. The default value is Bluetooth On.

Options

Option	Default	Information
Report when connection lost	Enabled	There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box. When disabled, lost connections are invisible to the user.
Report when connected	Disabled	When enabled, there may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.
Report failure to reconnect	Enabled	The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box. When disabled, failure to reconnect is invisible to the user.
		Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.
Computer is connectable	Enabled	Disable this option to inhibit HX2 connection with all nearby Bluetooth devices.

Option	Default	Information
Computer is discoverable	Disabled	When enabled, other Bluetooth devices can discover the HX2 when it is nearby. Disable this option to ensure other devices cannot discover the HX2.
Prompt if devices request to pair	Disabled	When enabled (checked), a dialog box is placed on the display when devices request to pair. Tap the X button, OK button or No button to close the dialog box.
Continuous search	Disabled	When enabled, the Bluetooth connection never stops searching for a device it has paired with if the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the HX2 stops searching after 30 minutes. This option draws power from the Main Battery.
Computer Friendly Name	OS Version	The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

*Note: The Device Name listed in **Start | Settings | Control Panel | System | Device Name** is not used during Bluetooth operation. Owner Identification name listed in **Start | Settings | Control Panel | Owner | Identification** is not used during Bluetooth operation.*

About

Figure 3-13 Bluetooth About Panel

This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Pairing and Auto-Reconnect

The HX2 *Bluetooth*® module can establish relationships with new devices after the end-user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of and then returned within range. Pairing supports SPP devices only.

Up to two Bluetooth devices can be connected to the HX2 at a time; LXE supports one scanner and one printer (see *Accessories*).

Taskbar Icon	Legend
	Bluetooth® module is connected to one or more of the targeted Bluetooth device(s).
	HX2 is not connected to any Bluetooth device. HX2 is ready to connect with any Bluetooth device. HX2 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: Configuration elements are persistent and stored in the registry.

Setup the *Bluetooth*® module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the HX2 while AppLock is in control. See *Chapter 6 – AppLock* for more information.

Certificates

Access: | **Settings | Control Panel | Certificates**

Manage digital certificates used for secure client communication. Lists the Stored certificates trusted by the HX2 user. These values may change based on the type of network security resident in the client, access point or the host system.

Figure 3-14 Control Panel – Stored Certificates

Tap the **Import** button to import a digital certificate file. Tap the **View** button to view a highlighted digital certificate. Tap the **Remove** button to remove highlighted certificate files. Tap the ? button and follow the instructions in the Help file when working with trusted authorities and digital certificates.

See Also: *Chapter 5 - Wireless Network Configuration* for instruction.

Date/Time

Access: ⊞ **| Settings | Control Panel | Date/Time Icon**

Set Date, Time, Time Zone, and assign a Daylight Savings location after a warm boot or a cold boot or at anytime.

Factory Default Settings	
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled
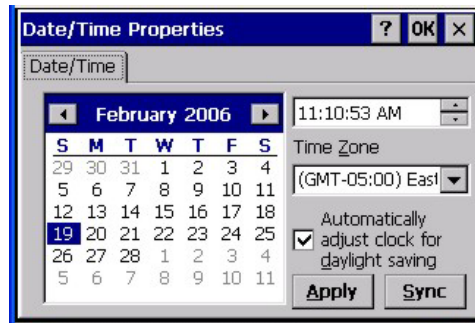
Figure 3-15 Control Panel – Date/Time Properties

There is very little functional change from general desktop PC Date/Time Properties options. Adjust the settings and tap the OK button or the Apply button to save the changes. The changes are saved to the Registry and take effect immediately.

Tap the Sync button to synchronize HX2 date and time with a time server. By default, the HX2 OS first searches for a time server on the local intranet. If not found, it then searches the internet for a time server. A connection to the internet is required for the last option.

Double-tapping the time displayed in the Taskbar causes the Date/Time Properties screen to appear.

GrabTime Utility

The HX2 includes a GrabTime utility which can be configured to synchronize the time with a local server during each reboot function. Please see *Configuring GrabTime* in the *Utilities* section for details.

Dialing

Access: [logo] **| Settings | Control Panel | Dialing**

Set dialup properties for internal modems. Modems are not supplied or supported by LXE.

Factory Default Settings	
Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled
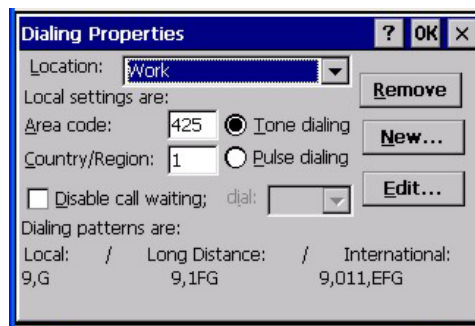
Figure 3-16 Control Panel – Dialing

Tap the Edit button to make changes to Dialing properties. Tap the ? button and follow the instructions in Help.

Display

Access: ⊞ **| Settings | Control Panel | Display Icon**

Select the Desktop image and set the display backlight timer when on battery or external power.

Factory Default Settings	
Background	Windows CE
Tile	Disabled
Appearance	
Default	Windows Standard
Backlight	
Battery Auto Turn Off	Enabled
Idle Timer	3 seconds
External Auto Turn Off	Enabled
Idle Timer	2 minutes

Background
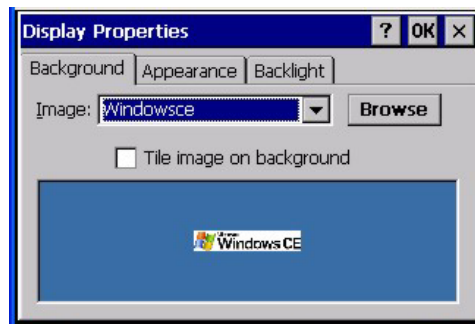
Figure 3-17 Control Panel – Display | Background

There is very little change from general desktop PC Display Properties / Background options. Select an image from the dropdown list (or tap the Browse button to select an image from a different folder) to display on the Desktop, then tap the OK button to save the change. The change is saved to the Registry and take effect immediately.

Appearance
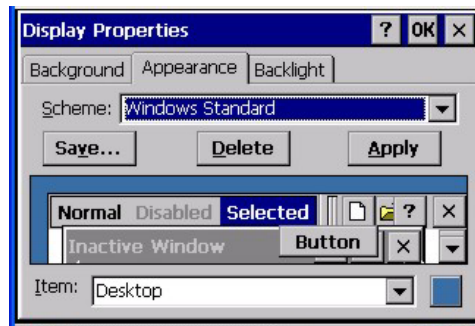
Figure 3-18 Control Panel – Display | Appearance

There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the HX2. Tap the OK button to exit, or the X button to escape without making any changes. Changes are saved to the registry and take effect immediately.

Backlight

Figure 3-19 Control Panel – Display | Backlight

When the backlight timer expires, the screen backlight is dimmed but not turned off. Default values are 3 seconds for Battery power and 2 minutes for External power.

Adjust the settings and tap the OK button to save the changes or the X button to escape without making any changes. Tap the ? button for Help. The changes are saved to the Registry and take effect immediately.

Input Panel

Access: ![Windows icon] **| Settings | Control Panel | Input Panel**

Select the current key / data input method. The Input Panel is also known as the virtual keypad or Soft Input Panel.

Factory Default Settings	
Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options	
Keys	Small keys
Use gestures (Transcriber)	Disabled
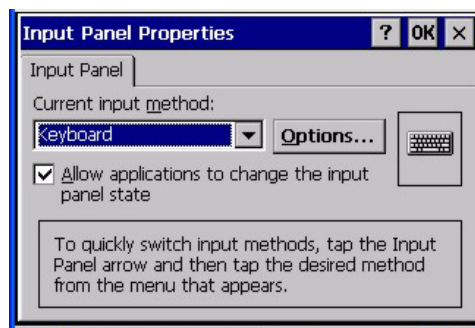
Figure 3-20 Control Panel – Input Panel

Use this screen to make the Input Panel or the physical keypad primarily available when entering data. Selecting Keyboard enables both.

Tap the Options button to set the size of the keys displayed on-screen and whether transcriber gestures are enabled or disabled.

Tap the OK button to save any changes and exit, or tap the X button to exit without saving any changes. Tap the ? button for Help.

Note: Check with your LXE representative for language packs as they become available.

Internet Options

Access: ⊞ **| Settings | Control Panel | Internet Options**

Set options for internet connectivity.
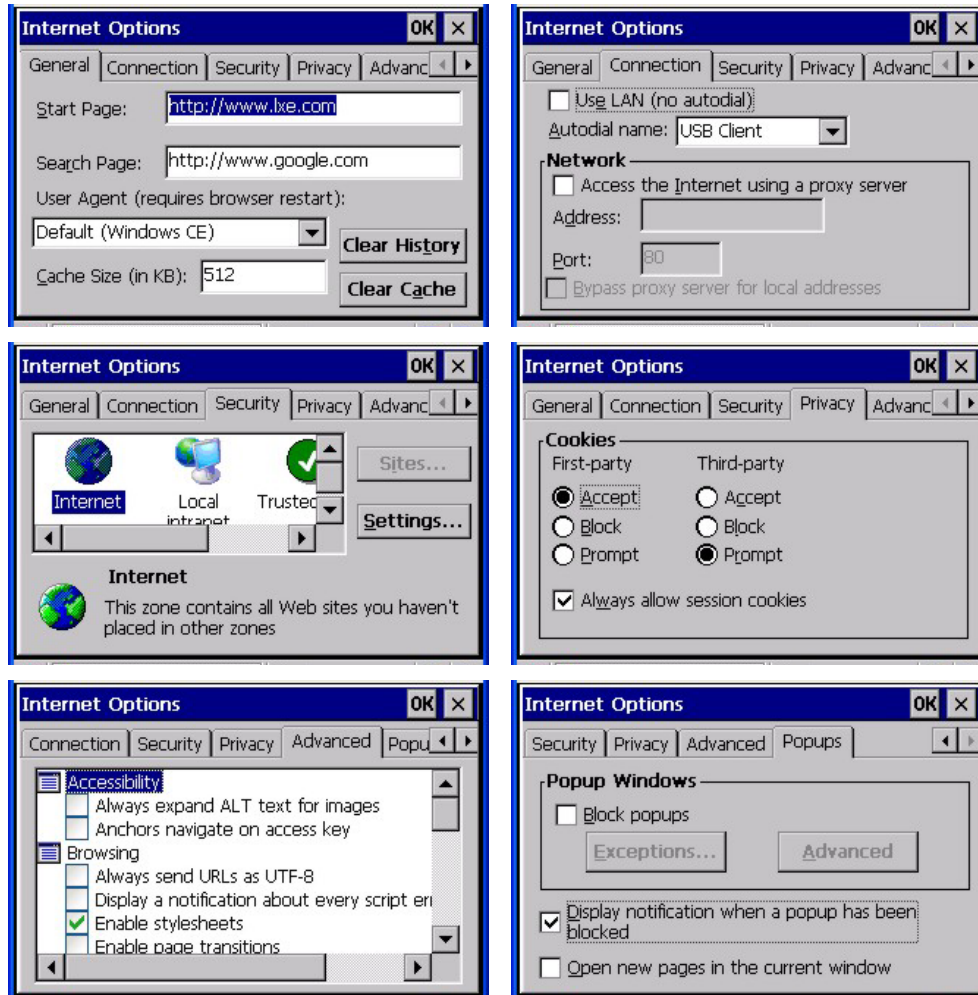
Figure 3-21 Control Panel – Internet Options

Select a tab. Adjust the settings and tap the OK button to save the changes. Changes are saved from tab to tab. Tap the X button to ignore all changes. The changes take effect immediately. Tap the ? button for Help.

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
User Agent	Default (Windows CE)
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	USB Client
Proxy Server	Disabled

Factory Default Settings	
Security – Internet	
Script Safe ActiveX	Enable
Script Unsafe ActiveX	Disable
Run ActiveX	Enable
Scripting allow paste	Prompt
Active scripting	Enable
Display mixed content	Prompt
Allow Meta Refresh	Enable
Sub frames across domains	Prompt
Data Source across domains	Disable
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enable
Theming Support	Enable
Underline links	Never
Multimedia	All options enabled
Security	All options enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Keyboard

Access: 🏁 **| Settings | Control Panel | Keyboard Icon**

Set keypad key map and keypad key repeat delay and key repeat rate.

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key map	Default HX2
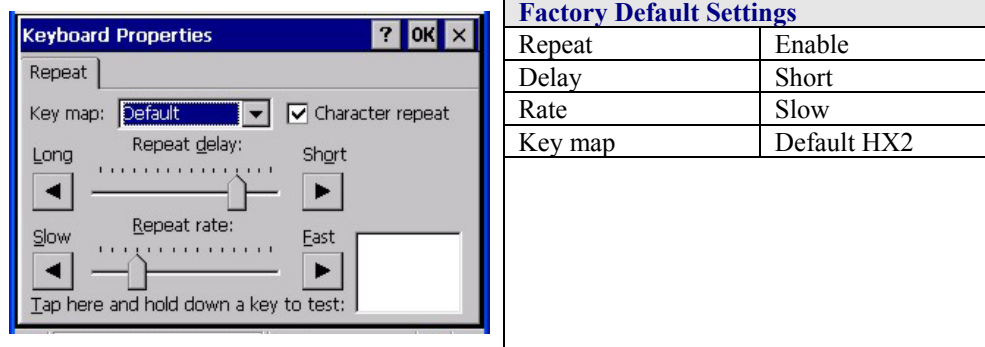
Figure 3-22 Control Panel – Keyboard

Select a key map using the drop-down list. Adjust the character repeat settings and tap the OK button to save the changes. Tap the X button to ignore changes. Tap the ? button for Help. The changes take effect immediately.

When new key maps, or fonts, are added to the registry, they appear in the Key map dropdown list on the Keyboard Properties panel. Only one font at a time can be selected. The fonts affect the screen display.

These values do not affect virtual (onscreen) key taps.

Keymaps and Fonts

Please contact your LXE representative about the availability of the following fonts for your HX2.

Descriptive name	Font filename	Notes
Simplified Chinese	simsun.ttc	These Asian fonts are ordered separately and built-in to the HX2 OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the default (extended) fonts. See About | Software | Language for the name of any installed fonts.
Traditional Chinese	mingliu.ttc	
Japanese	msgothic.ttc	
Korean	gulim.ttc	

When an Asian font is copied into the fonts folder on the card/System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in Regional Control Panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party .NET applications, and the font does not work for some third-party MFC applications.

Keypad

Access: ⊞ **| Settings | Control Panel | Keypad Icon**

Use this option to assign key functions to mappable keys, determine application launch sequences and program command Run sequences.

Note: *Keypad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option .*

Factory Default Settings		
Alpha (Alpha is not available with Dual Alpha or Triple Tap keypads)		
Persistence	On	
Configure 0, 1	0 – 1 click	Configure to – Space
Keypad Backlight	On	
KeyMap		
Modifier Mode	None	
Key	Backspace	Remap to – Backspace
Edit String	Shift	String – Null
LaunchApp		
App1	Null	
App2	Null	
App3	Null	
App4	Null	
App/Opt	EXE	
RunCmd		
Cmd1	Null	
Cmd2	Null	
Cmd3	Null	
Cmd4	Null	
File/Parm	FILE	
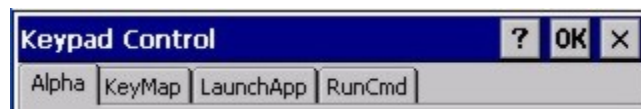
Figure 3-23 Control Panel Tabs for Alpha Mode 3 Tap Keypad

Figure 3-24 Control Panel Tabs for the Dual Alpha and Triple Tap Keypads

Assign settings by selecting keys from the drop down boxes. Tap the OK button to save the changes. Tap the X button to ignore changes and return to the Control Panel. Tap the ? button for Help. The changes take effect immediately.

Alpha Tab

Note: Alpha tab is not available when the HX2 has a Dual Alpha or Triple Tap keypad.
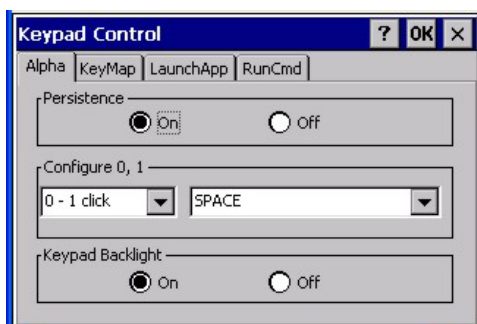
Figure 3-25 Control Panel – Keypad – Alpha Tab

Tap the OK button to save the changes. Tap the X button to ignore changes and return to the Control Panel. Tap the ? button for Help. The changes take effect immediately.

Persistence	Select the Off radio button (disable) when the Alpha key is to be tapped every time an alpha character is desired. The default value is On (enabled).
Configure 0, 1	Use the drop down boxes to assign a specific number of keyclicks, of either the 0 or 1 key, to map another key command to the 0 or 1 key sequence. The same key command can be assigned to more than one 0 or 1 keyclick sequence.
Keypad Backlight	Select the Off radio button (disable) when the keypad backlight is to remain Off regardless of the OS event in process. The default value is On (enabled). When On the keypad backlight responds to OS events as designed. When On, keypad backlight behavior is based on the settings of the Display Backlight Timer.

KeyMap Tab
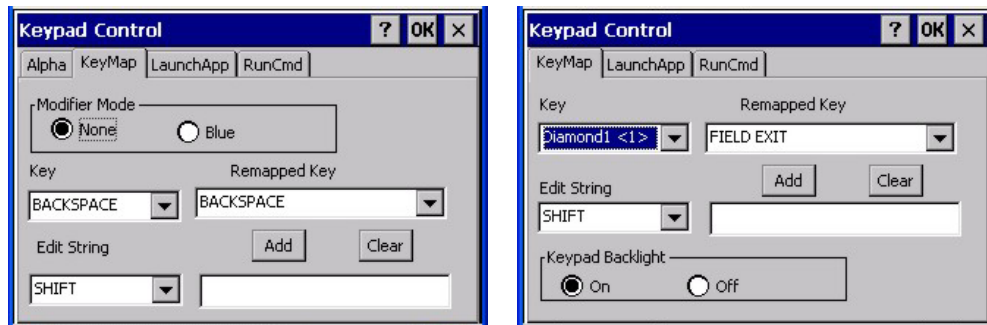
Alpha Mode 3 Tap Keypad   Dual Alpha or Triple Tap Keypad

Figure 3-26 Keypad – KeyMap Tab

Tap the OK button to save the changes. Tap the X button to ignore changes and return to the Control Panel. Tap the ? button for Help. The changes take effect immediately.

Modifier Mode	The default value is No modifier. Select the Blue radio button (enable) when the Blue key is to be tapped before the Remapped key is tapped.
Remapped Key	Keyboard keys and some CE functions can be remapped to any of the keys listed in the Key dropdown list. Select an HX2 keyboard key in the Key dropdown list to remap. Select the desired result key in the Remapped key dropdown list. Buttons available for remapping using the Key dropdown list are the Backspace, Left Arrow, Right Arrow, Up Arrow, Down Arrow, F1, F2, F3 and F4. The default keys mapped to each of the keys in the Key dropdown list are the original key value. For example, the default remapped key value for the Down Arrow key is the Down Arrow.
Edit String	Select a keyboard key from the Edit String dropdown list. Move the cursor to the text entry box. Remap a key to *Key String*, then you can edit the string using Keyboard or the Input Panel or by selecting the desired key from the Edit String dropdown list. Then tap Add. Tap Clear to clear all contents of the String text box. String can contain up to 64 characters.

LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the mobile device emits a single beep, if the launch is successful, the mobile device is silent.
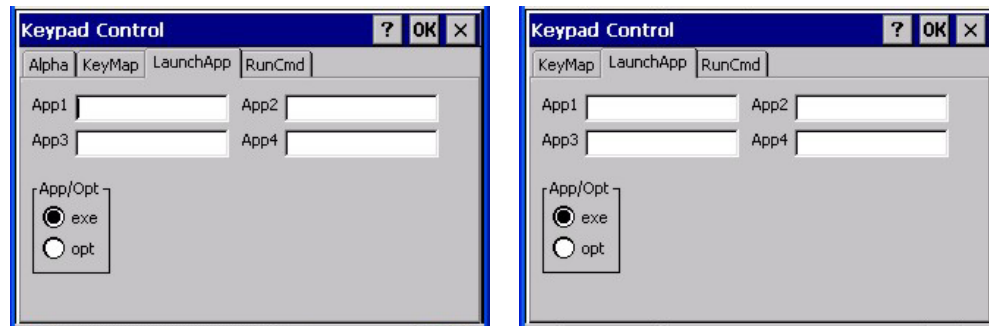
Alpha Mode 3 Tap Keypad   **Dual Alpha or Triple Tap Keypad**

Figure 3-27 Keypad – LaunchApp Tab

The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g. App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box, allowing parameter entry.

Tap the OK button to save the changes. Tap the X button to ignore changes and return to the Control Panel. Tap the ? button for Help. The changes take effect immediately.

See Also: Appendix A – Key Maps, *Creating Custom Key Maps* for more information.

RunCmd Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the mobile device emits a single beep, if the launch is successful, the mobile device is silent.
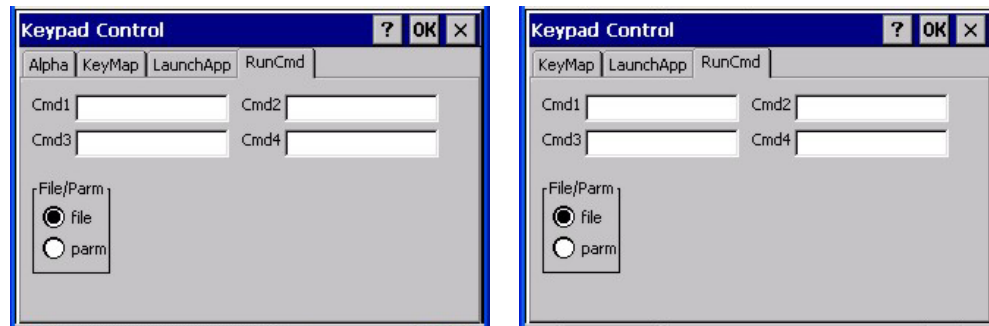
Alpha Mode 3 Tap Keypad   **Dual Alpha or Triple Tap Keypad**

Figure 3-28 Keypad – RunCmd Tab

The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g. Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.

Tap the OK button to save the changes. Tap the X button to ignore changes and return to the Control Panel. Tap the ? button for Help. The changes take effect immediately.

See Also: Appendix A – Key Maps, *Creating Custom Key Maps* for more information.

Mixer

Access: 🏁 **| Settings | Control Panel | Mixer Icon**

The microphone aperture is located immediately below the Up Arrow key. The speaker aperture is located immediately above the 2 key. Use these settings to adjust the volume, record gain, and sidetone for microphone input and speaker output.

Factory Default Settings	
Output	
Master Volume	-6.0 dB
Sidetone	12.0 dB
Input	
Input	Disabled
Internal Mic	Enabled
Bluetooth	Dimmed
Enable Headset	Enabled
Input Boost	Disabled
Record Gain	22.5dB
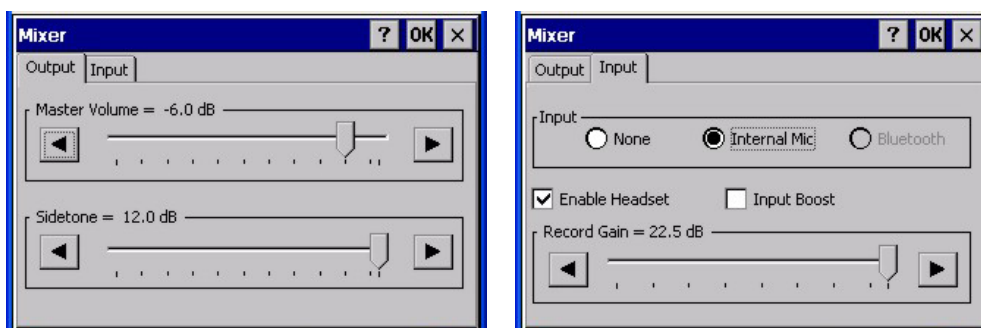
Figure 3-29 Mixer

Tap OK to save the settings or tap the X button to ignore changes.

Output tab

Tap and hold the **Output** sliders, moving them left and right to adjust the output decibel level. Or tap the left and right arrows to adjust the sliders.

Input tab

Option	Function
None	When enabled, the internal microphone is turned off. The default is unchecked (disabled).

Option	Function
Internal Mic	When enabled, the internal microphone is turned on. The default is checked (enabled). Enable the **Input Boost** checkbox to boost Record Gain by 20 dB. For example, if Record Gain is set to 40 dB and Input Boost is enabled, the dB for microphone output is boosted by 20 dB. The resulting microphone output would be approximately 60 dB.
Bluetooth	Future use.
Enable Headset	When Enable Headset is unchecked (disabled), the internal speaker and microphone are enabled. When Enable Headset is checked (enabled), the internal speaker and microphone are disabled. The default is checked (enabled). *When you will be using a tethered battery/audio cable without a headset, disable the Enable Headset parameter*.
Input Boost	When checked (enabled) increases the sensitivity of the microphone (internal or headset) by 20 dB.
Record Gain	Tap and hold the slider and move it left and right to adjust. Or tap the left and right arrow keys to adjust the slider. The default is 22.5 dB.

Mouse

Access: [Windows icon] **| Settings | Control Panel | Mouse**
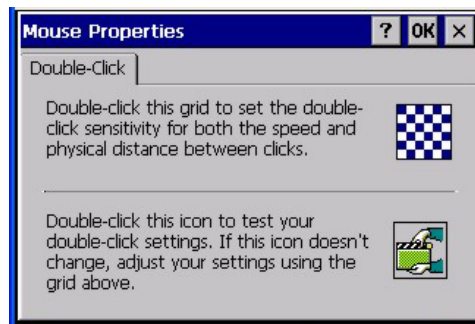
Figure 3-30 Mouse

Set the double-click sensitivity for stylus taps on the touchscreen. Tap OK to save the settings or tap the X button to ignore changes. Tap the ? button for Help.

See the section titled *Stylus* for touch screen calibration.

Network and Dialup Connections

Access: 🏁 **| Settings | Control Panel | Network and Dialup Connections**

Set network driver properties and network access properties. Select a connection to use, or create a new connection on the HX2.
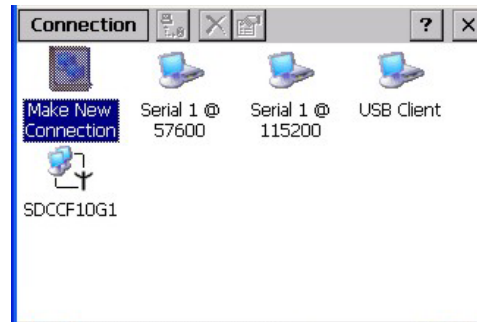
Figure 3-31 Network and Dialup Connections

Tap OK to save the settings or tap the X button to ignore changes. Tap the ? button for Help.

Create a Connection Option

1. On the mobile device, select 🏁 **| Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the one you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the Next button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the **Port Settings** tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off **Wait for dial tone**, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap OK.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select 🏁 | Settings | Control Panel | PC Connection and tap the Change Connection… button.
11. Select the new connection. Tap OK twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Click the desktop **Connect** icon to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Owner

Access: ⊞ **| Settings | Control Panel | Owner Icon**

Set the mobile device owner details.

Factory Default Settings	
Identification	
Name, Company, Address, Telephones	Blank
Display at power-on	Disabled
Notes	
Notes	Blank
Display at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank
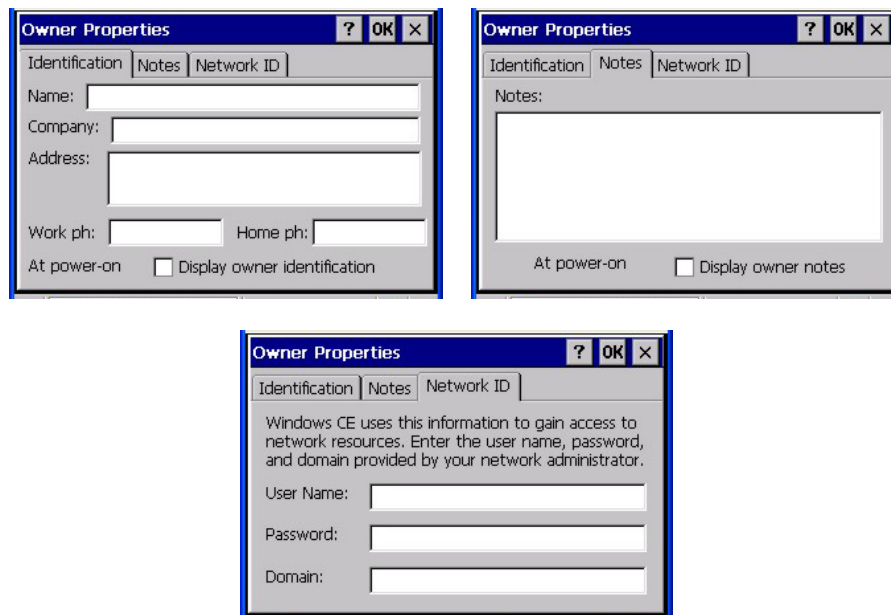
Figure 3-32 Owner Properties

Enter the information and tap the OK button to save the changes.

The changes take effect immediately.

Password

Access: ⊞ **| Settings | Control Panel | Password Icon**

Set HX2 user access/power up password properties. Password and password settings are saved during a warm boot and a cold boot. The screensaver password affects the Remote Desktop screensaver only.

Factory Default Settings	
Password	Blank
Enter at Power On	Disabled
Enter at Screen Saver	Disabled

Note: Once a password is assigned, each Settings option requires the password be entered before each Settings option can be accessed.
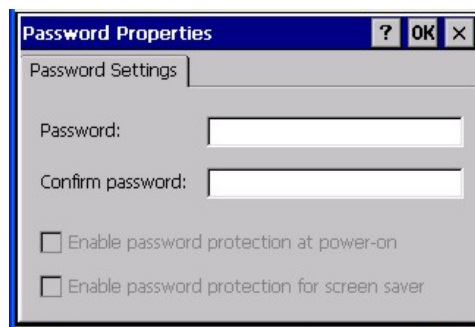
Figure 3-33 Password

Enter the password in the Password textbox, then type it again to confirm it.

Enable the power-on checkbox and, if desired, the screensaver checkbox. Tap the OK button to save the changes. The password is in effect immediately.

The screensaver password is the same as the power-on password. They are not set independently. A screensaver password cannot be created without first enabling the **Enable password protection at power-on** checkbox. The screensaver password is not automatically enabled when the **Enable password protection at power-on** checkbox is enabled.

Troubleshooting – Passwords

The password must be entered before performing a cold boot or cold reset. If entering a power-on or screensaver password will not allow you to disable password protection or run COLDBOOT, contact LXE Technical Support.

PC Connection

Access: ⊞ **| Settings | Control Panel | PC Connection**

Control the connection between the HX2 and a nearby desktop/laptop computer.

Factory Default Settings	
Enable direct connection	Enabled
Connect Using	'USB Client'

Tap the **Change Connection ..** button to adjust the settings. Then tap the OK button to save the changes. The changes take effect immediately.

Unchecking the **Enable direct connections …..** disables ActiveSync.

Change Connection ….

Selecting Change Connection displays a list of configured ActiveSync connections.
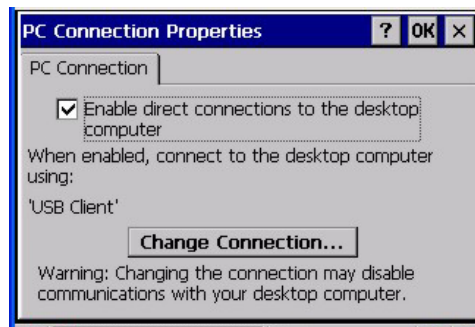
Figure 3-34 PC Connection

Please refer to the *Backup HX2 Files* section later in this chapter for parameter setting recommendations.

Power

Access: 🏁 **| Settings | Control Panel | Power**

Please refer to *Chapter 2 - Physical Description and Layout* section titled *Power Modes*.

Factory Default Settings		
Battery		
Turbo	Enabled	
Schemes		
AC Power	User Idle	2 minutes
AC Power	System Idle	2 minutes
AC Power	Suspend	5 minutes
Battery Power	User Idle	3 seconds
Battery Power	System Idle	15 seconds
Battery Power	Suspend	5 minutes

The mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to "Never", the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

Because of the cumulative effect, and using the Battery Power Scheme Defaults listed above:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15sec + 3sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.
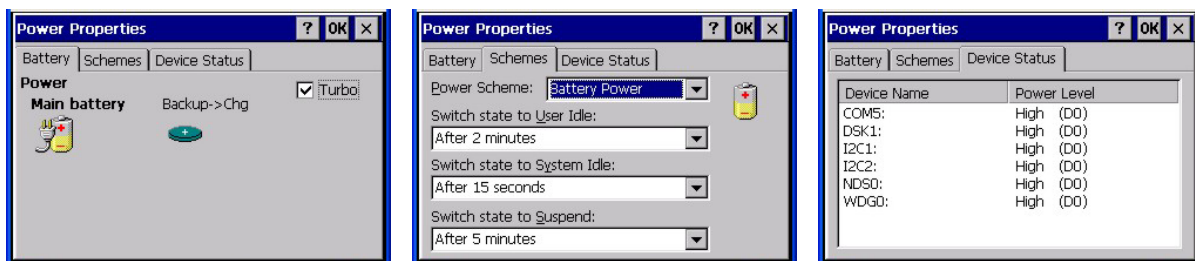
Figure 3-35 Power

Adjust the settings and tap the OK button to save the changes. Changes are saved across tabs. Tap the X button to discard any changes. Tap the ? for Help. The changes take effect immediately.

Regional Settings

Access: ![Windows] **| Settings | Control Panel | Regional Settings**

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the user interface language and the default input language.

Factory Default Settings	
Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 *pos* / ($123,456,789.00) *neg*
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy *short* / dddd,MMMM,dd,yyyy *long*
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US

Figure 3-36 Regional Settings

Tap the Customize button to assign a different format for dates, times, numbers and currency. Adjust the settings and tap the OK button to save the changes. Changes are saved across tabs. Tap the X button to discard any changes. Tap the ? for Help. The changes take effect immediately.

Remove Programs

Access: ![Windows] **| Settings | Control Panel | Remove Programs**

Note: Programs listed in this location are deleted upon warm and cold boot processes.

Highlight a program in the list and tap the Remove button. Follow the prompts on the screen to uninstall **user-installed only** programs.

Files stored in the **My Documents** folder are not removed using this option.

Note: Do not remove LXE-installed programs using this option.

Scanner

Access: 🏁 **| Settings | Control Panel | Scanner**

Set HX2 scanner keyboard wedge, scanner sound, scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Scanner parameters apply to the HX2 tethered scanner/imager *only*.

Barcode manipulation parameters are applied to the data resulting from successful barcode scans.

Tethered scanner configuration can be changed using the Scanner Control Panel or via the LXE API functions. While the changed configuration is being read, the Scanner LED is solid amber. The scanner is not operational during the configuration update.

After hotswapping tethered scanners, the HX2 auto-detects the tethered scanner type.

Factory Default Settings	
Main	
Port 1	Disabled until auto-detect
Port 2	Disabled until auto-detect
Port 3	Disabled until auto-detect
Send key messages (WEDGE)	Enabled
Enable Scanner Sound	Enabled
Imager LED Illumination	Internal
COM1 Port (external serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Barcode	
Enable Code ID	Disabled

Port 1 defaults to Bluetooth and Port 2 defaults to Ring when a Bluetooth enabled HX2 with ring scanner is powered On by the user. See the figure below for an example.
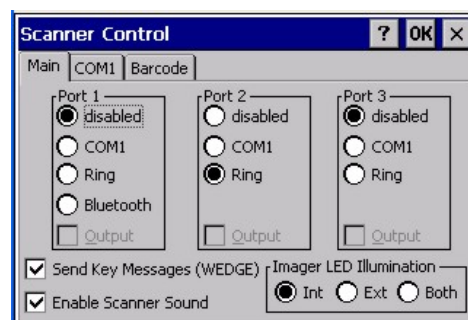
Figure 3-37 Scanner Control Panel

See *Chapter 4 – Scanner* for explanation and instruction when settings parameters on the Scanner Control Panels.

Stylus

Access: ⊞ **| Settings | Control Panel | Stylus**

Set double-tap sensitivity properties and/or calibrate the touch panel. The stylus is not shipped automatically with the HX2. The stylus is an accessory.

Double Tap
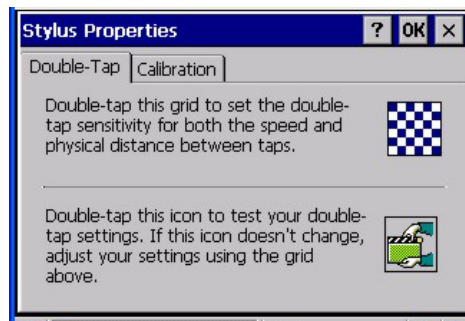
Figure 3-38 Stylus – Double-Tap

Follow the instructions on the screen and tap the OK button to save the changes. The double-tap changes take effect immediately.

Calibration
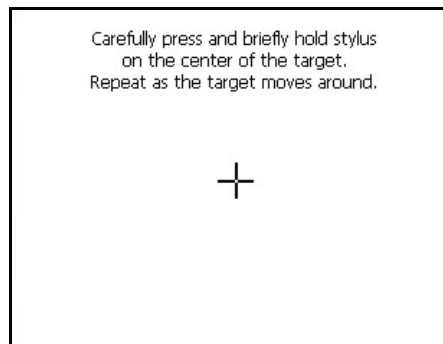
Figure 3-39 Stylus – Calibrate

Press and hold the stylus on the center of the target as it moves around the screen. Press Enter to keep the new calibration settings or Esc to cancel.

System

Access: ⊞ **| Settings | Control Panel | System Icon**

Review System and mobile device data and revision levels. Adjust Storage and Program memory settings.

Factory Default Settings	
General	N/A
Memory	1/3 storage, 2/3 program memory
Device Name	HX2001
Device Description	LXE_HX2

General

Figure 3-40 System – General

System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. Hence, a system with 128 MB may only report 99 MB memory, since 29 MB is used up by the Windows CE operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory
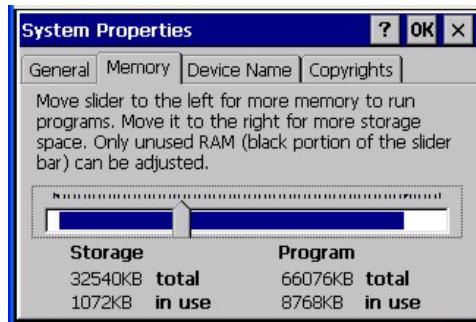
Figure 3-41 System – Memory

Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the HX2 is running slowly, try increasing the amount of program memory. Adjust the settings and tap the OK button to save the changes. The changes take effect immediately.

Device Name
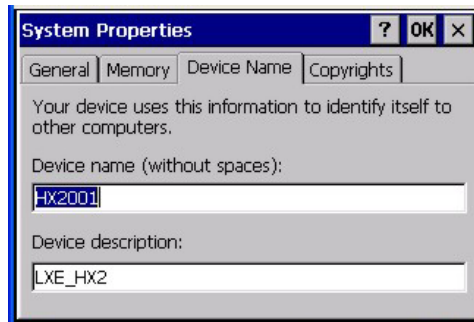
Figure 3-42 System – Device Name

The device name and description can be changed. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. The changes take effect immediately.

Copyrights
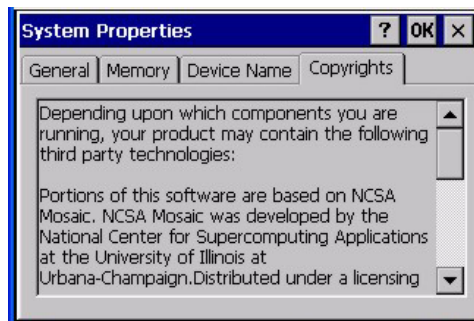
Figure 3-43 System – Copyrights

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Volume and Sounds

Access: ![Windows icon] **| Settings | Control Panel | Volume & Sounds**

Set volume parameters and assign sound wav files to CE events.

Factory Default Settings	
Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!
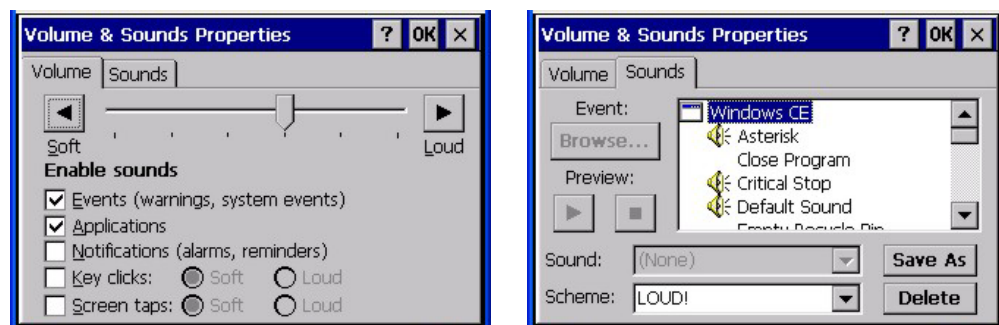
Figure 3-44 Volume & Sounds

Follow the instructions on the screen and tap the OK button to save the changes. The changes take effect immediately.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice. By default a good scan sound on the mobile device is a single 2700 Hz beep, and a bad scan sound is a double beep.

SD Flash Cards, CAB Files and Programs

The Flash card, located inside the HX2, is intended to protect the user from losing the LXE drivers and configuration information in the event of a cold boot. Also, on any boot, the contents of any registered CAB files are automatically unpacked. The flash card cannot be removed/exchanged by the user.

Access Files on the Flash Card

Tap the **My Device** icon on the Desktop then tap the **System** icon.

Files

A flash card is used for permanent storage of the LXE driver and utility files. It is also used for registry content back up. The flash card cannot be removed/exchanged by the user.

CAB files, when executed, are not deleted.

SUMMIT.CAB	Summit Client files needed for radio operation.
APPLOCK.CAB	AppLock program. See *Chapter 6 - AppLock*.
The following CAB files are optional and may or may not be present:	
LXE_HX2_ENABLER.CAB	Wavelink Avalanche Enabler.
RFTERM.CAB	RFTerm terminal emulation application.
JAVA.CAB	Java application.
BLUETOOTH.CAB	Bluetooth Client files needed for pairing operation.

Note: *APPLOCK.CAB can be removed if not used. The Wavelink Avalanche Enabler CAB file should not be executed if the HX2 will not be managed using Wavelink Avalanche Manager. See section titled <u>Wavelink Avalanche Enabler Configuration</u> later in this chapter.*

ActiveSync / Get Connected Process

Introduction

Requirement: ActiveSync version 3.8 (or higher) must be on the host (desktop/laptop, PC) computer.
HX2 USB ActiveSync Cable (Type A to HX2 cradle connector [HX2A001CBLACTVSYNC])

A partnership between a PC and the HX2 must be established using a USB connection. When more than one PC will be synchronizing with the HX2, each PC will need its own partnership with the HX2 established. See section titled *Initial Install* for the procedure.

After the partnership has been established with the HX2 and the host computer, ActiveSync can be performed over USB, or wireless (RF). HX2 serial connection is not supported in this release.

Using Microsoft ActiveSync you can synchronize information on your PC with the HX2 and vice versa. Synchronization compares the data on the HX2 with the PC and updates both with the most recent data. For example, you can:

- Synchronize Microsoft Word and Microsoft Excel files between the HX2 and PC. Files are automatically converted to the correct format.
- Back up and restore mobile device data.
- Copy (rather than synchronize) files between the mobile device and PC e.g. the HX2 LXEbook (the user's guide in CE compatible format).
- Control when synchronization occurs by selecting a synchronization mode. For example, synchronize continually while connected to a PC or only when the synchronize command is chosen.
- Select which information types are synchronized and control how much data is synchronized.

Note: By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information to synchronize. The synchronization process makes the data (in the information types selected) identical on both the PC and the mobile device. If an information type is selected that does not exist on the HX2, the data appears to transfer, but it is ignored by the HX2 and not loaded.

When installation of ActiveSync is complete on a PC, the ActiveSync Setup Wizard begins and starts the following processes:

- connect the mobile device to the PC,
- set up a partnership so you can synchronize information between your mobile device and your PC, and
- customize synchronization settings.

For more information about using ActiveSync on a PC, open ActiveSync, then open ActiveSync Help .

Initial Install

Initial installation / relationship must be established using a USB cable connection between the HX2 and the desktop/laptop (PC). Once a relationship has been established, tap 🏁 | **Help** | **ActiveSync** for help.

Install ActiveSync on Desktop/Laptop

Go to the Microsoft Windows website ActiveSync Download | Install file location:

www.microsoft.com/downloads

and type ActiveSync in the Keywords text box. This process should locate the latest version of ActiveSync.

Install ActiveSync on the PC before using ActiveSync to connect the PC to the mobile device.

Follow the instructions in the ActiveSync Wizard.

Check that 🏁 | **Programs** | **Communication** | **ActiveSync** | **Tools** | **Options** has the correct connection selected. Refer to *USB Connection*.

When installation of ActiveSync is complete on your PC, the ActiveSync Setup Wizard on the PC begins and it begins searching for a connected device.

Because ActiveSync is already installed on your mobile device, your first synchronization process begins automatically when you finish setting up your PC in the ActiveSync wizard and, using the HX2 ActiveSync cable, connect your mobile device to the PC.

Figure 3-45 Connect ActiveSync Cable to HX2 Cradle Connector

Insert the HX2 cable end into the cradle connector on the bottom of the HX2 until a click is heard.

Insert the USB-A end in a USB port on the desktop/laptop computer.

Note: The ActiveSync cable for the HX2 does not appear to fit tightly with the cradle connector (see Figure). This is normal.

USB Connection

Tap the ⊞ | **Settings** | **Control Panel** | **PC Connection** on the HX2. Tap the Change Connection button. From the popup list, choose

USB Client

This will set up the HX2 to use the USB configuration (Default). Tap OK and ensure the check box for **Enable direct connections to the desktop computer** is checked.

Tap OK to return to Settings.

Connect – Initial Install Process

Connect the correct cable to the PC (the host) and the HX2 (the client) cradle (HX2A001CBLACTVSYNC). Tap the ⊞ | **Programs** | **Communication** | **Connect** icon on the HX2.

The HX2 connection is made using ⊞ | **Programs** | **Communication** | **ActiveSync.**

When the desktop/laptop computer and the HX2 in the powered cradle successfully connect, the initial ActiveSync process is complete.

Change Connection Parameters

Tap the ⊞ | **Settings** | **Control Panel** | **PC Connection**. Tap the **Change Connection** button. From the popup list, choose

Option	Description
USB Client	This will set up the HX2 to use the USB port direct (Default).

- Tap OK and ensure the check box for Enable direct connections to the desktop computer is checked.
- Tap OK to return to Settings.
- Select Scanner and ensure the ring scanner is set to a port that is different than the "Connect" port (COM 1).

Backup HX2 Files

Use the following to backup data files from the HX2 to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

Initial ActiveSync partnership between the HX2 and the target PC has been completed. After the partnership has been established with the mobile device and the host computer, ActiveSync can be performed over USB, or wireless (RF).
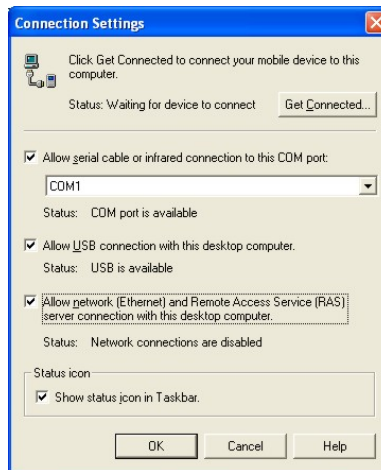
Figure 3-46 ActiveSync Connection Settings on a Windows PC

HX2 and PC Partnership

An ActiveSync partnership between the PC and HX2 has been established. See section **Initial Setup**.

USB Transfer

- A PC with an available USB port and an HX2 in a cradle with a USB cable. The desktop or laptop PC must be running Windows 98 SR2, Windows 2000 or Windows XP.
- LXE-specific USB cable as listed in the following section *Connect*.
- **Allow USB connection with this desktop computer** is checked.

Wireless Client Transfer

- A PC or laptop with a radio card or wireless connection.
- The **Allow network (Ethernet) and Remote Access Service (RAS) server connection with this desktop computer** is checked.

Connect

Connect the correct cable to the PC (the host) and the HX2 (the client).

Select "Connect" from [Windows] | **Programs** | **Communications** | **Connect**.

Note: ActiveSync over USB will start automatically when the cable is connected.

Explore

From the ActiveSync Dialog on the Desktop PC, click on the Explore button, which allows you to explore the HX2 from the PC side, with some limitations.

You can copy files to or from the HX2 using drag-and-drop.

You will not be allowed to delete files or copy files out of the \Windows directory on the HX2. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows OS image. This, however, includes most of the files in the \Windows directory).

For example, you can drag the *LXEbook – HX2 User's Guide* from your desktop computer to the My Documents folder on the HX2.

Disconnect

USB Connection

- Disconnect the cable from the HX2 cradle.
- Click the ActiveSync status bar icon in the lower right hand corner of the PC's status bar. Then click the Disconnect button.

  IMPORTANT – Do not put the HX2 into Suspend Mode while connected via USB. The HX2 will be unable to connect to the host PC when it resumes operation.

Wireless Client Connection

- Put the HX2 into Suspend Mode by tapping the red Power button.
- Click the status bar icon in the lower right hand corner of the PC's status bar. Then click the Disconnect button.

ActiveSync Troubleshooting

> **ActiveSync on the host returns to the Get Connected screen without connecting to the cabled device.**

If the HX2 is connected to a PC by a cable, disconnect the cable from the HX2 and reconnect it again.

Check that the correct connection is selected, **USB Client**.

See Also: *Cold Boot and Loss of Host Reconnection*.

> **ActiveSync indicator on the host remains grey**

The host doesn't know you are trying to connect. It may mean a bad cable. Try the connection again with a known-good cable.

> **Drop down list is blank in the ActiveSync dialog box**

The wireless link is broken. Make sure that the wireless client in the HX2 has a valid IP address.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a mobile device and a PC. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership for a unique client can be established to two hosts.

If the HX2 is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (| **Settings** | **Control Panel** | **System** | **Device Name**)

If the cold booted HX2 tries to reestablish the partnership with the same host PC, a new random number is generated for the HX2 and ActiveSync will insist the unique name of the HX2 be changed. If the HX2 is associated with a second host, changing the name will destroy *that* partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

Utilities

These utilities are pre-loaded by LXE.

LAUNCH.EXE

All applications to be installed into memory are normally in the form of Windows CE CAB files. The CAB files exist as separate files from the main installation image, and need to be copied to the mobile device using an internal Flash card or from a PC using ActiveSync. The CAB files are loaded into the folder **System**, which is the internal Flash drive.

Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup. The CAB file can update the registry as desired and cause the unpacked file(s) to be placed in the appropriate location.

The registry information needed is under the key *HKEY_LOCAL_MACHINE \ SOFTWARE \ LXE \ Persist*, as follows. The main subkey is any text, and is a description of the file. Then 3 values are added:

> **FileName** is the name of the CAB file, with the path (usually \System)
> **Installed** is a DWORD value of 0, which changes to 1 once auto-launch installs the file
> **FileCheck** is the name of a file to look for to determine if the CAB file is installed.

The value in FileCheck is the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

Three optional fields are also added: **Order**, **Delay**, and **PCMCIA**. These are all DWORD fields, described below.

The auto-launch process goes as follows. The launch utility opens the registry database and reads the list of CAB files to auto-launch. First it looks for **FileName** to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the **Installed** flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it. If the **Installed** flag is set, auto-launch looks for the **FileCheck** file. If it is present, the CAB file is installed, and that registry entry is complete. If the **FileCheck** file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file. Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.

To force execution every time (for example, for **AUTOEXEC.BAT**), use a **FileCheck** of **dummy**, which will never be found, forcing the item to execute.

For persist keys specifying **.EXE** or **.BAT** files, the executing process will be started, and then **Launch** will continue, leaving the loading process to run independently. For other persist keys (including **.CAB** files), **Launch** will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.

The **Order** field is used to force a sequence of events; **Order=0** is first, and **Order=99** is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence. Note: If the order of loading is not critical, it may be easier to use the \System\Startup folder instead; see below.

The **Delay** field is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to **0** if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA

slots are off on powerup, to prevent the **Unidentified PCMCIA Slot** dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default radio drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.

Note that the auto-launch process can also launch batch files (***.BAT**), executable files (***.EXE**), registry setting files (***.REG**), or sound files (***.WAV**). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Registry information is already in the default image for the following [5]:

```
;; ------- autoexec batch file – for users convenience
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AUTOEXEC]
          "FileName"="\\System\\Autoexec.bat"
          "Installed"=dword:0
          "FileCheck"="ALWAYSEXEC"
          "Order"=dword:50
;; The file name "ALWAYSEXEC" or "dummy" does not really matter as long as there is
;;  no file of that name in the directory. You can use any name that you want for this entry
;;  as long as it is a non existent file name. The purpose of this value is that if someone
;;  wants to only execute this file one time then you would replace the value of FileCheck
;;  with the name of a file that would exist the next time a warm boot occurs.


;; special function – makes Launch copy system folders from ATA drive
;; we put it in here so that we control when it happens (esp. for Applock)
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
          "FileName"="COPYFOLDERS"
          "Installed"=dword:0
          "FileCheck"=""
          "Order"=dword:10


;; ------- Summit radio support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Summit Radio]
          "FileName"="\\System\\SUMMIT.CAB"
          "Installed"=dword:0
          "FileCheck"="\\WINDOWS\\SDCCF10G.DLL"
          "Order"=dword:2
          "PCMCIA"=dword:1


;; ------- RFTerm support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
          "FileName"="\\System\\RFTERM.CAB"
          "Installed"=dword:0
          "FileCheck"="\\WINDOWS\\LXE\\RFTERM.EXE"
          "Order"=dword:11
```

---

[5] CAB files for options not purchased are not loaded e.g. JAVA or RFID. If a CAB file is missing, please contact your LXE Representative.

```
;; ------- Voxware support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Voxware]
        "FileName"="\\System\\MX7BSTRP.CAB"
        "Installed"=dword:0
        "FileCheck"="ALWAYSEXEC"
        "Order"=dword:60


;; ------- Bluetooth support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Bluetooth]
        "FileName"="\\System\\BLUETOOTH.CAB"
        "Installed"=dword:0
        "FileCheck"="\\WINDOWS\\BTUI.EXE"
        "Order"=dword:30


;; run the app after it has loaded and radio is ready
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
        "FileName"="\\WINDOWS\\LXE\\RFTERM.EXE"
        "Installed"=dword:0
        "FileCheck"="ALWAYSEXEC"
        "Order"=dword:40
        "Delay"=dword:1


;; ------- Avalanche support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
        "FileCheck"="\\System\\avalanche\\model.dat"
        "Installed"=dword:0
        "Order"=dword:4
        "FileName"="\\System\\LXEAVA.CAB"


[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
        "Order"=dword:5
        "FileName"="\\System\\Avalanche\\Avainit.exe"
        "FileCheck"="ALWAYSEXEC"
        "Installed"=dword:0


;; ------- Applock support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockInstall]
        "FileName"="\\System\\AppLock.CAB"
        "Installed"=dword:0
        "FileCheck"="\\WINDOWS\\APPLOCK.EXE"
        "Order"=dword:0


[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockPrep]
        "FileName"="\\windows\\AppLockPrep.exe"
        "Installed"=dword:0
        "FileCheck"="ALWAYSEXEC"
        "Order"=dword:1
        "Delay"=dword:2


[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLock]
        "FileName"="\\windows\\AppLock.exe"
        "Installed"=dword:0
        "FileCheck"="ALWAYSEXEC"
        "Order"=dword:63
```

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\KbdLocks]
     "FileName"="\\windows\\KbdLocks.exe"
     "Installed"=dword:0
     "FileCheck"="ALWAYSEXEC"
     "Order"=dword:62

When you are installing your custom CAB file to the mobile device's operating system, refer to the default image segments that are commented with "… RFTERM …" to see the expected Registry format.

One special key is included to force the system folders (Desktop, Fonts, Programs, etc.) to copy from the internal ATA card (**\System**) to the **\Windows** directory. This is implemented as a persist key so the sequence of startup events can be controlled (especially for AppLock). The filename is a special internal trigger for the Launch utility, to activate the **CopyFolders** function. *DO NOT EDIT OR ALTER THIS KEY, OR IT MAY NO LONGER FUNCTION.* You may however change the **Order** or **Delay** values if necessary for a particular startup sequence.

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
     "FileName"="COPYFOLDERS"
     "FileCheck"=""
     "Order"=dword:0F

To have files (CAB, EXE, REG, or WAV files) loaded on startup, when sequence of execution is not important, you can put these files in the \System\Startup folder (on the internal Flash card). This is parsed by the Launch utility, and these programs are started or executed.

REGEDIT.EXE

Before using REGEDIT.EXE, please refer to commercially available Microsoft Power Tools for Windows manuals . For example Microsoft Windows Registry Guide, Second edition.

The Registry Editor allows viewing, searching for items and changing settings in the registry. The registry contains information about how the mobile device runs. LXE recommends **caution** when inspecting and editing the Registry as making incorrect changes can damage the mobile device operating system. LXE recommends making a backup copy of the registry before viewing or c a r e f u l l y making changes to the registry.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

WARMBOOT.EXE

Double tap this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double-tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

Configuring GrabTime

Note: This utility affects the behavior of GrabTime at warmboot. After a coldboot, GrabTime is disabled.

The HX2 has a GrabTime utility which can automatically synchronize the HX2 with a worldwide time server (via an Internet connection) at boot up. By default, GrabTime for time synchronization at boot up is Off.

To enable GrabTime to run automatically at boot up, run **\Windows\grabtime.reg** and perform a warmboot. For more detail, see *LAUNCH.EXE*, earlier in this chapter.

Synchronize with a local time server

1. Use ActiveSync to copy **GrabTime.ini** from the **My Device | Windows** folder on the HX2 to the host PC.
2. Edit GrabTime.ini (on the host PC) to add the local time server's domain name to the beginning of the list of servers. You can then optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini to the **My Device | System** folder on the HX2.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. Each time the mobile device is cold booted, the Windows/GrabTime.ini file is replaced with the default version and the System/GrabTime.ini file is not.

Configuring CapsLock Behavior

To set CapsLock status to On after a warmboot, run \Windows\CapsLockOn.reg and perform a warmboot.

To set CapsLock status to Off after a warmboot, run \Windows\CapsLockOff.reg and perform a warmboot.

Note: Setting CapsLock to On using this method does not display the CapsLock icon in the Windows CE taskbar. The current status of CapsLock can be changed with the CAPS key sequence [2 Alpha clicks], however this method does not change CapsLock behavior upon reboot.

Note: These utilities affect the behavior of the CapsLock on warmboot. After a coldboot, CapsLock is disabled.

Command-line Utility

Command line utilities can be executed by Start | Run | [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all data in RAM is erased). The command is not case-sensitive.

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap Start | Run | then type prtscrn and tap OK, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and the captured screen file (scr*nnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Wavelink Avalanche Enabler Configuration

If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device.

Terminology may appear different, based on your installed version:

- Avalanche Manager may be shown as the Avalanche Mobility Center Console
- Avalanche Agent may be shown as the Avalanche Mobile Device Server
- Avalanche Management Console may be shown as the Avalanche Mobility Center or the Avalanche Mobility Center Console

Note that actual operation of the Enabler on the mobile device does not change.

Briefly . . .

The Wavelink Avalanche Enabler installation file is loaded on the mobile device by LXE; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. Related manual: *Using Wavelink Avalanche on LXE Windows Computers*.

Note: On LXE mobile devices with integrated scanners, the Scanner Wedge has primary control of the serial ports and must be configured properly to allow the Enabler to access the serial ports.

Enabler Install Process

- Doubletap the Avalanche Enabler CAB file in the System folder. The filename is LXE_HX2_ENABLER.CAB.
- Warm boot the mobile device.

Enabler Uninstall Process

To remove the LXE Avalanche Enabler from a Windows CE mobile device:

- Delete the Avalanche folder located in the System folder.
- Warm boot the mobile device.

The Avalanche folder cannot be deleted while the Enabler is running. See *Stop the Enabler Service*. If sharing errors occur while attempting to delete the Avalanche folder, warm boot the mobile device, immediately delete the Avalanche folder, and then perform another warm boot.

Orphaned Packages

To prevent the enabler from restoring parameters, delete orphaned packages through the Avalanche Mobility Center (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details and instruction).

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Avalanche MC Console:

1. Open the Enabler Settings Panels by tapping the **Avalanche** icon on the desktop.
2. Select File | Settings. Enter the password.
3. Select the **Startup/Shutdown** tab.
4. Select the **Do not monitor or launch Enabler** parameter to prevent automatic monitoring upon startup.
5. Select **Stop Monitoring** for an immediate shutdown of all enabler update functionality upon exiting the user interface.
6. Tap the **OK** button to save the changes.
7. Reboot the device if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on an LXE device can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server and the LXE device.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server and the mobile device.
- Wirelessly via the 2.4GHz network card and an access point

After installing the Enabler on the mobile unit, a reboot is required for the Enabler to begin normal functionality. Following a mobile device reboot, the Enabler searches for an Mobile Device Server, first by polling all available serial ports and then over the wireless network. The designation of the mobile device to the Avalanche Mobility Center Manager is LXE_HX2.

The Enabler running on LXE Windows CE devices will attempt to access COM1, COM2, and COM3. "Agent not found" will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the LXE scanner applet in the Control Panel).

The wireless connection is made using the default client interface on the mobile device therefore the device must be actively communicating with the network for this method to succeed. If a Mobile Device Server is found the Enabler will automatically attempt to apply all wireless and network settings from the active profile. When configured to download available packages, the Enabler will also automatically download and process all available packages.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the Enabler will attempt to apply all network and wireless settings contained in the active profile. The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler. These local parameters cannot be overridden from the Avalanche Mobility Center Console.

The default Enabler adapter control setting are:

- Manage network settings – enabled
- Manage wireless settings – disabled for Windows CE Units
- Use Avalanche network profile – enabled

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the **Enabler Settings Panels** by tapping the **Avalanche icon** on the desktop.
2. Select File | Settings. Enter the password.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for Manage Network Settings, Manage Wireless Settings and Use Avalanche Network Profile.
6. Tap the **OK** button to save the changes.
7. Reboot the device.

Related Manual: *Using Wavelink Avalanche on LXE Windows Computers*.

Enabler Configuration

Avalanche Icon

The Enabler user interface application is launched by clicking:

either the Avalanche icon on the desktop or Taskbar

or

selecting Avalanche from the Programs menu.

The opening screen presents the user with the connection status and a navigation menu.

Figure 3-47 Avalanche Enabler Opening Screen

File	View	Help
Connect	Updates	Adapter Info
Abort	Programs	About
Settings	Icons	
Scan Config	List	
Exit	Details	
	Launchable	
	All Packages	
	Time on Taskbar	
	Device Status	

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the mobile device immediately upon a successful connection.
Abort	Stop transmission.
Settings	The Settings option under the File menu allows the user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected. The default password is **system** The password is not case-sensitive.
Scan Config	*Note: LXE does not support the Scan Configuration feature on Windows CE devices.* The Scan Config option under the File menu allows the user to configure Enabler settings using a special barcode that can be created using the Avalanche Management Console utilities. Refer to the *Wavelink Avalanche Mobility Center User's Guide* for details.
Exit	The Exit option is password protected. The default password is **leave** The password is not case-sensitive. If changes were made on the Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed: Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Avalanche Update using File | Settings

Access: Start | Avalanche | File | Settings

Use these menu options to setup the Avalanche Enabler on the mobile device. LXE recommends changing and then saving the changes (reboot) before connecting to the network.

Alternatively, the Mobile Device Server can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details – available on the Wavelink Avalanche website).

Menu Options

Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF are used to check for the presence of the Mobile Device Server.
Execution	*Unavailable in this release.* LXE recommends using AppLock, which is resident on each Windows CE mobile device. See Chapter 6 - AppLock.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Startup/Shutdown	Set options for Enabler program startup or shutdown.
Scan Config	This option allows the user to configure Enabler settings using a special barcode that is created by the Avalanche Mobility Center. *Not currently supported by LXE.*
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection Tab

Figure 3-48 Avalanche Enabler Connection Options

Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the mobile device.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.

Execution Tab

Note the dimmed options on this panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.

Unavailable in this release. LXE recommends using AppLock. See *Chapter 6 – AppLock.*

Figure 3-49 Avalanche Enabler Execution Options (Dimmed)

Auto-Execute Selection	An application that has been installed with the Avalanche Mobility Center Console can be run automatically following each reboot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Mobility Center Console.
Delay before execution	Time delay before launching Auto-Execute application.

Server Contact Tab

Figure 3-50 Avalanche Enabler Server Contact Options

Sync Clock	Reset the time on mobile computer based on the time on the Mobile Device Server.
Contact at startup	Connect to the Mobile Device Server when the Enabler is accessed.
Contact when cradled	Initiate connection to the Mobile Device Server based on a docking event. *Not available on the HX2.*
Contact Periodically	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can 'wakeup' and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.

<u>Startup/Shutdown Tab</u>

> **LXE recommends using AppLock for this function.** AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in *Chapter 6 AppLock*.
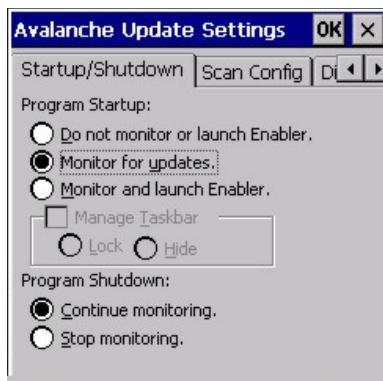
Figure 3-51 Avalanche Enabler Startup / Shutdown Options

Do not monitor or launch Enabler	When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
Monitor for updates	Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Manage Taskbar (Lock or Hide)	Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.
Program Shutdown (Continue or Stop monitoring)	The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

LXE recommends using AppLock for this function. See *Chapter 6 AppLock* for instruction.

Scan Config Tab
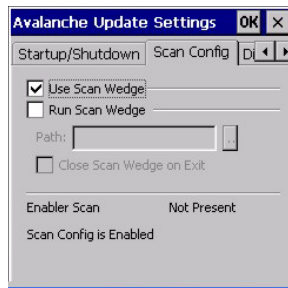
Note: Scan Config functionality is a standard option of the Wavelink Avalanche System but is not currently supported by LXE on Windows CE devices.

Figure 3-52 Avalanche Enabler Scan Config Option

Display Tab
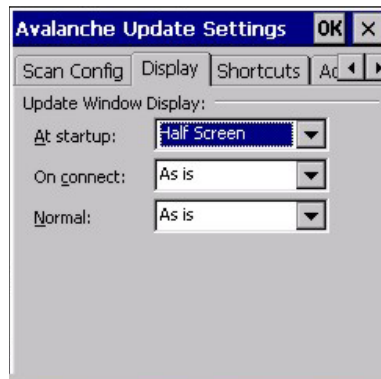
Figure 3-53 Avalanche Enabler Window Display Options

The user interface (Update Window Display) for the Enabler can be configured to dynamically change based on the status of the connection with the Mobile Device Server.

At startup   Half screen, Hidden or Full screen. Default is Half screen.

On connect   As is, Half screen, full screen, Locked full screen. Default is As is.

Normal   Half screen, Hidden or As is. Default is As is.

Shortcuts Tab

LXE recommends using AppLock for this function. AppLock is resident on each mobile device with a Windows OS.
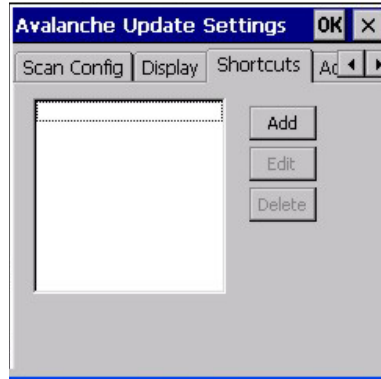
Figure 3-54 Avalanche Enabler Application Shortcuts

Configure shortcuts to other applications on the mobile device. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

LXE recommends using LXE AppLock for this function. See *Chapter 6 - AppLock* for instruction.

Adapters Tab

> *Note:*   *LXE recommends the user review the network settings configuration utilities and the default values in <u>Chapter 5 – Wireless Network Configuration</u> before setting All Adapters to Enable in the Adapters applet.*
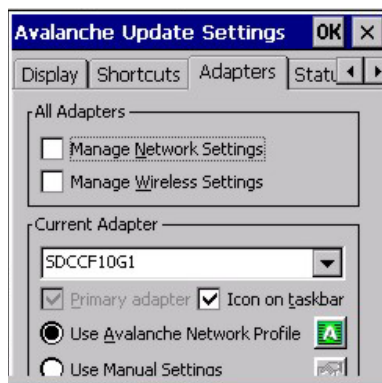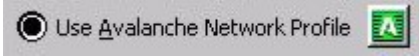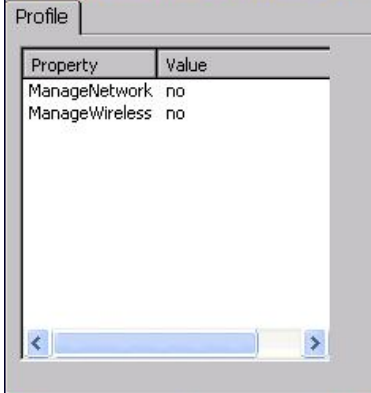
Figure 3-55 Avalanche Enabler Adapters Options – Network

Manage Network Setting	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Management Console and is disabled by default. This parameter setting **does not apply to Summit Clients** *only*.
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.

Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Avalanche Mobility Center Console.
Avalanche Icon	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings. **Figure 3-56 Avalanche Network Profile Displayed**

Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche Management Console and use only the network settings on the mobile device.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.

Network   **DNS**   **Wireless**
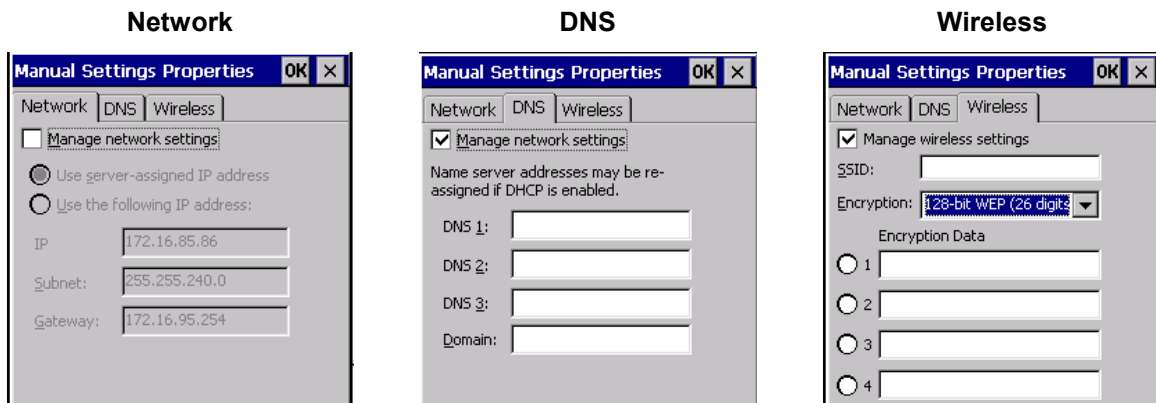
For device-specific descriptions of these Enabler parameters, refer to *Chapter 5 – Wireless Network Configuration*.

LXE does **not** recommend enabling **Manage Wireless Settings**.

Figure 3-57 Manual Settings Properties Panels

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global **Manage wireless settings** and **Manage network settings** options are enabled on the Adapters panel (see Figure titled *Avalanche Enabler Adapters Options – Network*). Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status Tab

The Status panel displays the current status of the mobile device network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button. When tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.
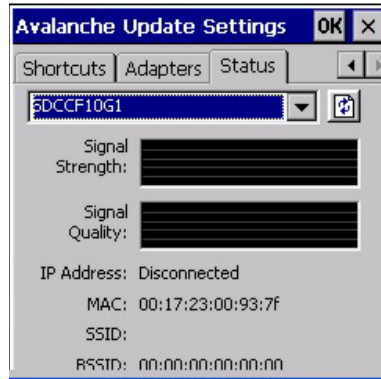
Figure 3-58 Status Display

Link speed indicates the speed at which the signal is being sent from the adapter to the mobile device. Speed is dependent on signal strength.

Troubleshooting

Coldboot / Warmboot

If a device managed by Avalanche is cold-booted, a warmboot MUST be performed following the coldboot. Failure to perform the warmboot will leave the device in an undetermined configuration and it may not perform as expected. If the intention is to stop using Avalanche to manage the device configuration, please see *Enabler Uninstall Process* earlier in this section.

Chapter 4 Scanner

Introduction

> *Note:* *For the purposes of this chapter, the term "scanner" represents the HX2 ring scanner, ring imager, mobile Bluetooth scanner and/or 2D imager, unless specifically stated otherwise.*

Access: ⊞ | Settings | Control Panel | Scanner

Set HX2 scanner keyboard wedge, scanner sound, and scanner port. Assign baud rate, parity, stop bits and data bits for COM1. Scanner parameters apply to the HX2 tethered ring scanner/imager or the mobile Bluetooth barcode reader *only*.

Barcode manipulation parameters in this chapter are applied to the data resulting from successful barcode scans sent to the HX2 for processing.

Tethered scanner configuration can be changed using the Scanner Control Panel or via the LXE API functions. While the changed configuration is being read, the ring scanner's Scan LED is solid amber. The ring scanner is not operational during the configuration update.

After hotswapping the HX2 tethered scanners the HX2 auto-detects the tethered scanner type.

The HX2 may be using any of the following ring scanners:

- Symbol SE4400 Imager
- Symbol SE955 Scanner

or one of two mobile Bluetooth scanners:

- PSC 7700BT
- PL4407

The scanner/imager activates when the Scan button or Scan trigger is pressed.

📖 Please refer to the *Ring Scanner Programming Guide* for instruction when configuring specific scanner parameters by using the ring barcode reader to scan the engine-specific setup barcodes in the guide.

📖 *Ring Scanner Programming Guide* and the *Reset All barcode*. After scanning the Reset All (to factory defaults) barcode for the specific scan engine, the next step is **Start | Control Panel | Scanner**. Tap the OK button and close the scanner applet. This action will synchronize all scanner formats.

> *Note:* *Scanner control panel options are based on the installed software version levels, driver and OS versions in HX2 devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device. To identify the software version, tap the **About** icon in the Control Panel.*

Barcode Processing Overview

Note: Steps 1-7 describe the barcode manipulation. Steps 8-12 describe how the manipulated data is built. Step 13 describes how the manipulated data is output.

The complete sequence of barcode processing is as follows:

1. Scanned barcode is tested for a **code ID**. If one is found, it is stripped from the data, and the settings for the symbology specified are used. Otherwise, the **All** symbology settings are used.
2. If symbology is **disabled**, the scan is rejected.
3. If the **length** of data (minus the code ID) is out of specified **Min/Max** range, the scan is rejected.
4. Strip **leading** data bytes unconditionally.
5. Strip **trailing** data bytes unconditionally.
6. Parse for, and strip if found, **Barcode Data** strings.
7. Replace any **control characters** with string, as configured.
8. Add **prefix** string to output buffer.
9. If **Code ID** is *not* stripped, add saved **code ID** from above to output buffer.
10. Add processed **barcode** string from above to output buffer.
11. Add **suffix** string to output buffer.
12. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
13. If key output is enabled, start the process to output keys. If control characters are encountered:

    *   If Translate All is set, key is translated to CTRL + char, and output.
    *   If Translate All is not set, and key has a valid VK code, key is output.
    *   Otherwise, key is ignored (not output).

The data is ready to be read by applications.

See *Barcode Processing Examples* at the end of the *Barcode Tab* section.

Factory Default Settings

Factory Default Settings	
Main	
Port 1	Disabled until auto-detect
Port 2	Disabled until auto-detect
Port 3	Disabled until auto-detect
Send key messages (WEDGE)	Enabled
Enable Scanner Sound	Enabled
Imager LED Illumination	Internal
COM1 Port (cradle serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Barcode	
Enable Code ID	None

Port 1 defaults to Bluetooth and Port 2 defaults to Ring when a Bluetooth enabled HX2 with ring scanner/imager is powered On by the user. See the figure below for an example.
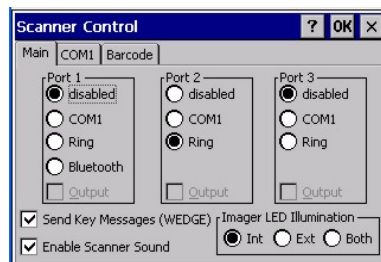
Figure 4-1 Scanner Control Panels

If **Send Key Messages …** is checked any data scan is converted to keystrokes and sent to the active window. When this box is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using **Wedge**.

Disable *Enable Internal Scanner Sound* when you want an application, not the Bluetooth scan engine or the CE operating system, to control scanner audible notifications. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Main Tab

Access: 🏁 **| Settings | Control Panel | Scanner | Main tab**

Factory Default Settings	
Main	
Port 1	Disabled until auto-detect
Port 2	Disabled until auto-detect
Port 3	Disabled until auto-detect
Send key messages (WEDGE)	Enabled
Enable Scanner Sound	Enabled
Imager LED Illumination	Internal
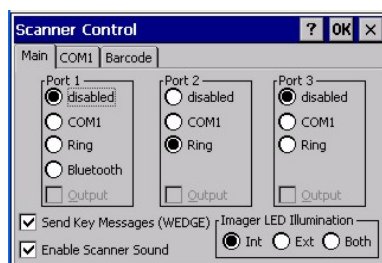
Figure 4-2 Scanner Control / Main

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Parameter	Function
Port	The ports are disabled until the HX2 auto-detects a device tethered to the port. Port 1 defaults to Bluetooth and Port 2 defaults to Ring when a Bluetooth enabled HX2 with ring scanner/imager is powered On.
Send Key Messages (WEDGE)	When Send Key Messages (WEDGE) is checked any data scan is converted to keystrokes and sent to the active window. When this checkbox is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using **Wedge**.
Enable Scanner Sound	The default is Enabled. Functionality of the tethered scanner driver engine includes audible tones on good scan (at the maximum db supported by the speaker) and failed scan.
	Disable this parameter when good scan/bad scan sounds are to be handled by alternate means e.g. application-controlled sound files.
	Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned barcode data by the processing causes a bad scan beep from the HX2 on the same data.

Parameter	Function
Imager LED Illumination	The default setting is Internal illumination. The imager has a bank of three LEDs above the imager aperture that illuminate when External or Both radio buttons are enabled. The illumination turns off when the scan is complete.

COM1 Tab

Access: ⊞ **| Settings | Control Panel | Scanner | COM1 tab**

Factory Default Settings	
COM1 Port (cradle serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
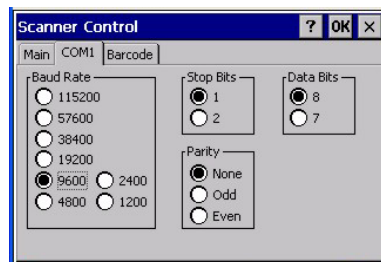
Figure 4-3 Scanner Control / COM1

If these values are changed, the default values are restored after a cold boot or reflashing.

Barcode Tab

Access: ⊞ **| Settings | Control Panel | Scanner | Barcode tab**

The Scanner application (Wedge) can only enable or disable the processing of a barcode inside the Wedge software.

The Scanner application enables or disables the Code ID that may be scanned.

Enabling or disabling a specific barcode symbology is done manually using the configuration barcode in the *Ring Scanner Programming Guide* (available on the LXE Manuals CD and the LXE ServicePass website).

Choose an option in the Enable Code ID drop-down box: None, AIM ID, Symbol ID, or Custom ID.
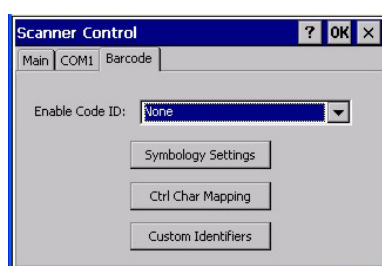
Figure 4-4 Scanner Control / Barcode tab

Buttons

Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

See Also: *Barcode Processing Overview* earlier in this chapter.

Enable Code ID

This parameter programs the ring scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

Options

None	Programs the scanner to disable transmission of a Code ID. The only entry in the Symbology popup list is All.
AIM	Programs the scanner to transmit the AIM ID with each barcode. The combo box in the Symbology control panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.
Symbol	Programs the scanner to transmit the Symbol ID with each barcode. The combo box in the Symbology control panel is loaded with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.
Custom	Does not change the scanner's Code ID transmission setting. The combo box in the Symbology control panel is loaded with any configured Custom Code IDs.

Notes

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the barcode data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e. treated as a Code ID).
- UPC/EAN Codes only: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to AIM or Symbol, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 ']A1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- When using the parameters in the mobile device OS Scanner Control Panel to manage indicators for good read/bad read decoding, the number or patterns of beeps heard may be confusing. Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep, and then the rejection of scanned barcode data by the Scanner Control Panel processing causes a bad scan beep by the mobile device on the same data

Barcode – Symbology Settings

The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured. The features available on the Symbology Settings dialog include the ability to individually enable or disable a barcode from scanning, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode.

The Symbology drop-down box contains all symbologies **supported on the HX2**. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is tapped. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.
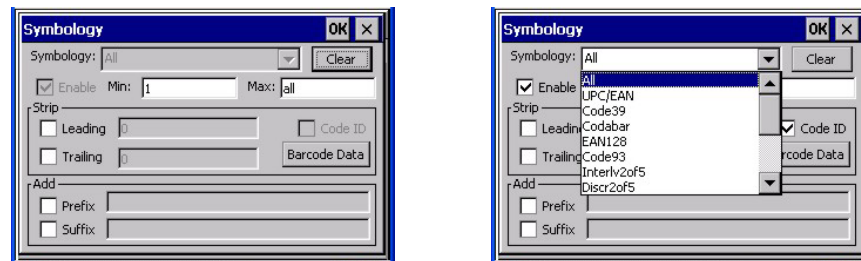
Figure 4-5 Barcode Tab / Symbology Settings

Clear   This button will erase any programmed overrides, returning to the default settings for the selected symbology. If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Barcode tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Barcode tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults. If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two. If a symbology has not been configured (does not have an * next to it) the settings for "All" are used which is not necessarily the default.

Parameters

Enable	This checkbox enables (checked) or disables (unchecked) the symbology field. The scanner driver searches the beginning of the barcode data for the type of ID specified in the Barcode tab – Enable Code ID field (AIM or Symbol) plus any custom identifiers. When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed. If the symbology is disabled, all other fields on this dialog are grayed. When there are **no** *customized settings*, and the Enable checkbox is unchecked (All is selected and no other settings are customized) a confirmation dialog is presented to the user "You are about to disable all scan input – Is this what you want to do?". Tap the Yes button or the No button. Tap the X button to close the dialog without making a decision. If there **are** *customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies except the customized ones.
Min	This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed. Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.
Max	This field specifies the maximum length that the barcode data (not including Code ID) can be to be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999). If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length will be used instead.

Strip Leading/Trailing Control

Figure 4-6 Symbology / Strip Leading / Trailing

This group of controls determines what data is removed from the barcode before the data is buffered for the application. If all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.

If the total number being stripped is greater than the number of characters in the barcode data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading	This strips the number of characters specified from the beginning of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default.
Trailing	This strips the number of characters specified from the end of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default.
Code ID	Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

Barcode Data	This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.
	To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.
	Tap the OK button to store any additions, deletions or changes.
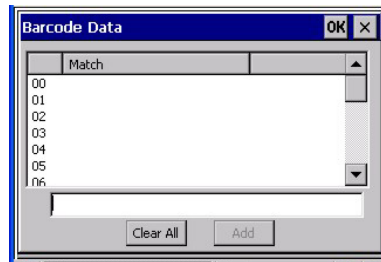
Figure 4-7 Symbology / Barcode Data Match List

Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Tap the **Add** button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The **Add** button changes to **Insert**. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The **Add** button changes to **Replace**. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The **Clear All** button changes to a **Remove** button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a 'good' beep will still be sounded, since barcode data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains *ABC* and *AB*, in that order, incoming data with *ABC* will match first, and the *AB* will have no effect.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard ***** is not specified, the string is assumed to strip from the beginning of the barcode data. The string *ABC** strips off the <u>prefix</u> *ABC*. The string ***XYZ** will strip off the <u>suffix</u> XYZ. The string *ABC*XYZ* will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard *?* may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The Barcode Data is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the barcode data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

See Also: *Barcode Processing Overview* earlier in this chapter.

Figure 4-8 Symbology / Prefix and Suffix Control

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see the *Hat Encoding* section in *Appendix B - Technical Specifications* for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix   To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pulldown list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.

Add Suffix   To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pulldown list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

See *Hat Encoding* and *Decimal-Hexadecimal Chart* in *Appendix B - Technical Specifications*.

Note: *Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. <F1>), arrow keys, Page up, Page down, Home, and End.*

Barcode – Ctrl Char Mapping

See Also: *Barcode Processing Overview* earlier in this chapter.

The Ctrl Char Mapping button activates a dialog to define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.
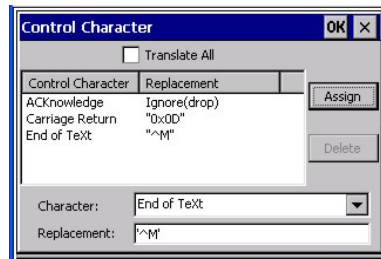
Figure 4-9 Barcode Tab / Ctrl Char Mapping

See *Hat Encoding* and *Decimal-Hexadecimal Chart* in *Appendix B - Technical Specifications*.

Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Translate All	This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a keystroke equivalent is dropped.
Character	This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default *Ignore (drop)* in the Replacement edit control.

Replacement	The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button. For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a. The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.
List Box	The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.
Delete	This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Barcode – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard AIM or Symbol IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

These are called "custom" Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data. The dialog below allows the custom Code IDs to be configured.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if **Enable Code ID** is set to **AIM** or **Symbol**), or to replace the list of standard code IDs (if **Enable Code ID** is set to **Custom).**

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*
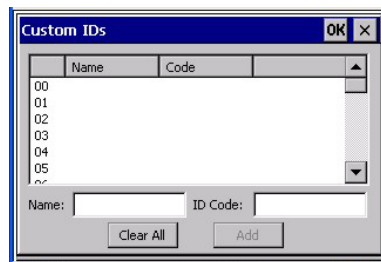
Figure 4-10 Barcode Tab / Custom Identifiers

After adding, changing and removing items from the Custom IDs list, tap the OK button to save changes and return to the Barcode panel.

Parameters

Name text box   Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the **Name** and **ID Code** may have the same value. **Name** is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box   ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add	Entering data into both the Name and ID Code fields enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The **Add** button changes to **Insert**. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The **Clear All** button changes to a **Remove** button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a barcode is converted to the text 'STX'.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	'^M'	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	'\^I'	Value 0x09 in a barcode is converted to the text '^I'.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	'0x0A'	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '0\x0A'	Value 0x0C is a barcode is converted to text '0x0A'

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	**EAN-128 (|C1)**	**EAN-13 (|E0)**	**Intrlv 2 of 5 (|IO)**	**Code93**
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	*< rejected >* *(too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	*< rejected >* *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	*< rejected >* *(disabled)*
Code-93	]G0444444	*< rejected >* *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	*< rejected >* *(too short)*

Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

Length Based Barcode Stripping

Use this procedure to create symbology rules for two barcodes with the same symbology but with different discrete lengths. This procedure is not applicable for barcodes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired barcode ID.
- Next, a custom barcode symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

For the purposes of this example, the following sample barcode parameters will be used – EAN128 and Code128 barcodes. Some of the barcodes start with '00' and some start with '01'. The barcodes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character barcode is CODE128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN128 barcode and 0 for Code128 barcode.

- c1 = Code = ']C1'
- c2 = Code = ']C1'
- c3 = Code = ']C0' (24 character barcode is CODE128)
- c4 = Code = ']C1'
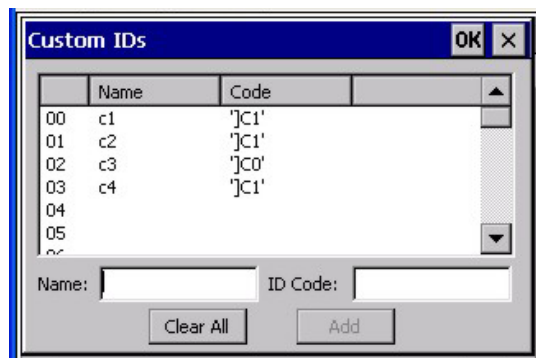
AIM Custom IDs

AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

Add the AIM custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.

AIM Custom Setup for C1

Click the Barcode Data button. Click the Add button.

Add the data for the match codes.
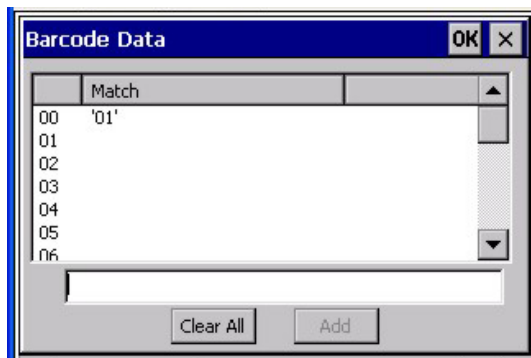
Barcode Match Data for C1

Refer to the previous section *BarcodeData Match List* for instruction.

Scan a barcode and examine the result.

Chapter 5 Wireless Network Configuration

Introduction

It may be necessary to upgrade client drivers in order to use certain Summit Client Utility (SCU) features and/or security options described in this chapter. Please contact your LXE representative for Summit driver update availability.

The HX2 mobile device has a wireless client that can be configured for no encryption, WEP encryption or WPA security, no authentication and all authentications listed below.

Certificates are necessary for many of the WPA authentications. Please refer to the *Certificates* section at the end of this chapter for more information on generating and installing certificates.

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys
- The Summit profile settings for Auth Type, EAP Type and Encryption depend on the security option chosen.

Wireless Security Options Supported
No Security
WEP
LEAP
EAP-FAST
PEAP-MSCHAP
WPA/LEAP
WPA-PSK
PEAP-GTC
EAP-TLS

Please refer to the *LXE Security Primer* to prepare the Authentication Server and Access Point for wireless communication. The document is available on the LXE Manuals CD and the LXE ServicePass website.

It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Summit Client Configuration

 Summit Client Utility Icon

Note: Terminology used on your screen displays may be different than those shown in the figures in this chapter. Contact your LXE representative for Summit driver updates as they become available.

Start the Summit Client configuration by tapping the Summit Client Utility icon on the desktop. You can also start the Summit Client utility by tapping **Start | Programs | Summit | SCU**.

Important: After adding a new profile or changing parameters of an existing profile, tap Start | Suspend. When the device Resumes, saved changes are applied.

Summit Client Utility

Access: **Start | Programs | Summit | SCU** *or* **SCU Icon on Desktop** *or* **SCU Icon in Taskbar**

or

Figure 5-1 Summit Client Utility (SCU)

The **Main** tab provides information, the Admin Login and active config (profile) selection.

Profile specific parameters are found on the **Config or Profile** tab. The parameters on this tab can be set to unique values for each profile.

The **Status** tab contains information on the current connection.

The **Diags** tab provides utilities to troubleshoot the client (network device).

Global parameters are found on the **Global Settings or Global** tab. The values for these parameters apply to all profiles.

Note: A password is required before making changes to Summit client profile parameters. A password is not required to switch from one profile to another.

Help

Help is available by clicking the **? button** in the title bar on most SCU screens.

SCU Help may also be accessed by selecting **Start | Help** and tapping the Summit Client Utility link. The SCU does not have to be open to view the help information using this option.

Summit Tray Icon

The Summit tray icon ▮▮▮ provides access to the SCU and is a visual indicator of link status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active.
- The Windows Zero Config utility is not active.
- The Tray Icon setting is On.

Tap the icon to launch the Summit Configuration Utility.

Use the tray icon to view the link status:

Summit client is not currently associated or authenticated to an Access Point.

The signal strength for the currently associated/authenticated Access Point is -80 dBm or weaker.

The signal strength for the currently associated/authenticated Access Point is stronger than -80dBm but not stronger than -60 dBm.

The signal strength for the currently associated/authenticated Access Point is stronger than -60 dBm but not stronger than -40 dBm.

The signal strength for the currently associated/authenticated Access Point is stronger than -40 dBm.

Main Tab

Factory Default Settings	
Main	
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI

or
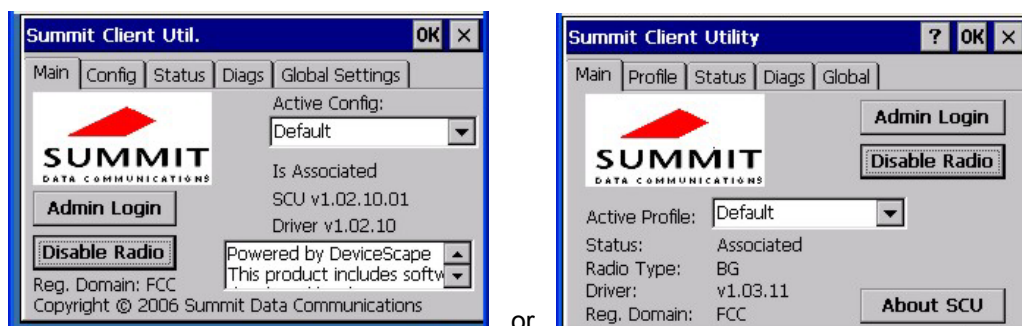
Figure 5-2 SCU – Main Tab

The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (the radio is an 802.11 b/g radio)
- Regulatory Domain
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc).

The **Active Config or Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named "ThirdPartyConfig" is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module. See *Wireless Zero Config Utility* later in this chapter for Wireless Zero Config instruction.

The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

The **Admin Login** button provides access to editing wireless parameters. Config / Profile and Global / Global Settings may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Admin Login

To login to Administrator mode, tap the **Admin login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the Admin Logout button, or a navigation button (X or OK), to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.

Figure 5-3 Main Tab – Enter Admin Password

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap OK. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global / Global Settings tab.

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Config / Active Profile on the Main tab.
- View the current parameter settings for the profiles on the Config / Profile tab.
- View the global parameter settings on the Global / Global Settings tab.
- The current connection details on the Status tab.
- Radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags tab.

After Admin login, the end-user can also:

- Create, edit, rename and delete profiles on the Config / Profile tab.
- Edit global parameters on the Global / Global Setting tabs.
- Enable/disable the Summit tray icon in the taskbar.

Config / Profile Tab

> *Note:*   *Tap the* **Commit** *button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!*

Factory Default Settings	
Config / Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	BG Optimized or BG Rates Full
Auth Type	Open
EAP type	None
Encryption	None

 or
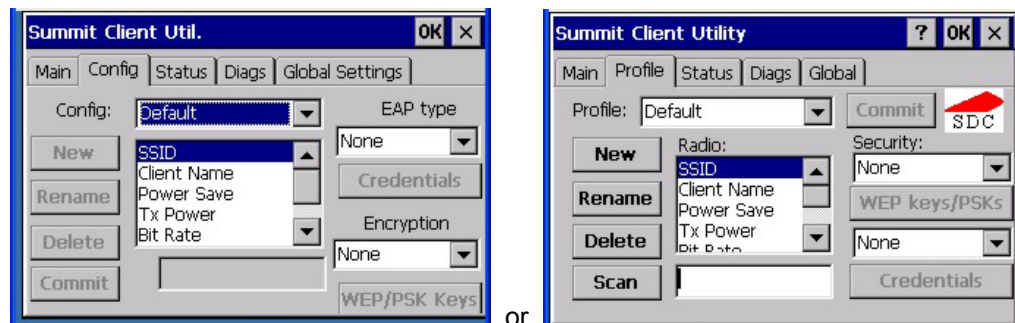
Figure 5-4 SCU – Config / ProfileTab

When logged in as an Admin (see *Admin Login*), use the Config / Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin.

Buttons

Button	Function
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see *Config/Profile Parameters*) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.

Button	Function
Scan	Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers.
	If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.
	Figure 5-5 SCU – Scan
	If you are logged in as an Admin, tap an SSID in the list and tap the Connect button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already).
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

Important – The settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security type chosen. Please refer to *Wireless Security* later in this Summit Client Utility section to determine the proper settings for the security type implemented on the wireless LAN.

Config / Profile Parameters

Parameter	Default	Explanation
Config or Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Config or Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 10mW or 1mW. *Depending on the version of the SCU, the options for Tx Power are between Maximum and 1mW.*
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Radio Mode	BG Optimized or BG Rates Full	Specify 802.11g and/or 802.11b when communicating with the Access Point. Options are: B rates only, BG Rates full, G rates only, BG optimized. *Note: Default value may vary depending on installed SCU driver version.*
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.

Parameter	Default	Explanation
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, or EAP-TLS. *Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.*
Encryption	None	Type of encryption to be used to protect transmitted data. Options are: None, Manual WEP, Auto WEP, WPA PSK, WPA TKIP, WPA2 PSK, WPA2 AES, CCKM TKIP, CKIP Manual, CKIP Auto, Manual WEP CKIP, or Auto WEP CKIP. *Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.*

Status Tab

This screen displays information on the current profile and wireless connection. Information cannot be edited or changed on the Status panel.
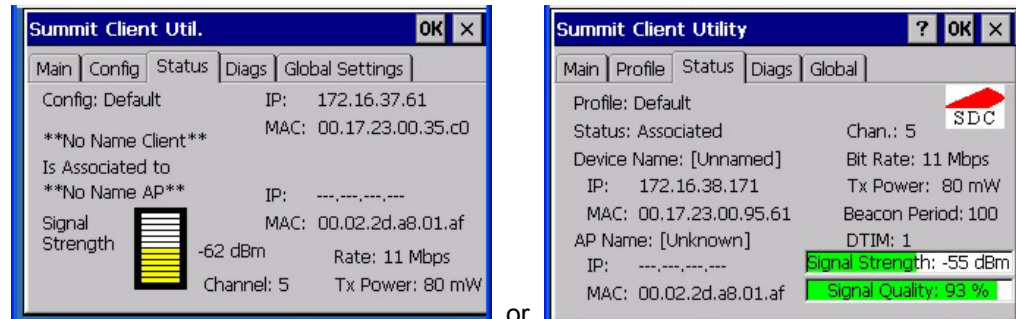
Figure 5-6 SCU – Status Tab

The panel displays:

- Config / Profile being used.
- The client name, IP address and MAC address.
- The status of the network connection (down, associated, authenticated, etc.).
- The name, IP address and MAC address of the Access Point maintaining the connection to the network.
- Channel currently being used for wireless traffic.
- Beacon period – The time between AP beacons in kilomicroseconds (1 kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Current transmit power in mW.
- Rate in Mbps.
- Signal strength (RSSI) and signal quality (changes with network activity). Signal quality is a measure of the clarity of the signal and is displayed as a percentage.

Note: After completing radio configuration, it is good practice to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab

The Diags panel can be used for troubleshooting network traffic and wireless connectivity issues for the IP address shown. Admin login is required for the (Re)connect button function.

Note: Site Survey functions are not available in this release. The Diagnostics function is not available in all versions.

or
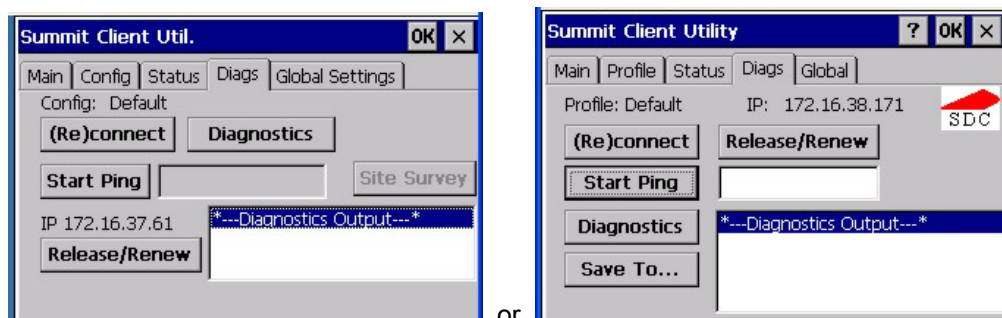
Figure 5-7 SCU – Diags Tab

Buttons

Button	Function
(Re)connect	Tap this button to apply, or reapply, the current config profile and attempt to associate or authenticate to the wireless LAN. Activity is logged in the Diagnostic Output text box on the lower part of the panel.
Release/Renew	Release the current IP address to obtain a new IP address. This option renews the IP address when applicable. Activity is logged in the Diagnostic Output text box. If a fixed IP address has been assigned to the wireless device, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed.
Start Ping	Tap the text box and type an IP address to Ping. Tap the Start Ping button to start pinging the IP address. The button name changes to Stop Ping. Tap Stop Ping to end the pinging process. The pinging process ends when any other button on this panel is tapped or a different menu tab is selected. Ping results are displayed in the Diagnostic Output text box.
Diagnostics	Tapping this button begins an attempt to (re)connect to the wireless LAN. This option provides more data in the Diagnostics Output text box than the (Re)connect option. The data dump includes client state, profile settings, global settings, and a list of access points by SSID broadcasting in the wireless device's immediate area. The text file created, _sdc_diag, is placed in the Windows folder. It is overwritten when Diagnostics is run again. Not available in all releases. Tap the **Save To .... button** to save the Diagnostics log to a TXT file in the My Device folder (the default folder).
Site Survey	Not available in this release.

Global / Global Settings Tab

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

*Note: Tap the **Commit** button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!*
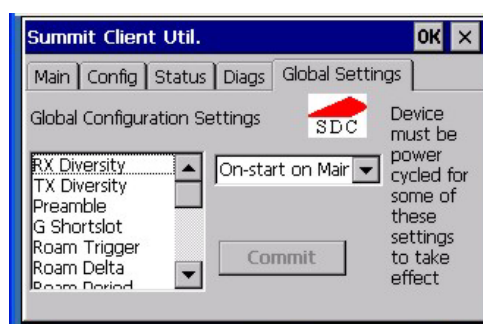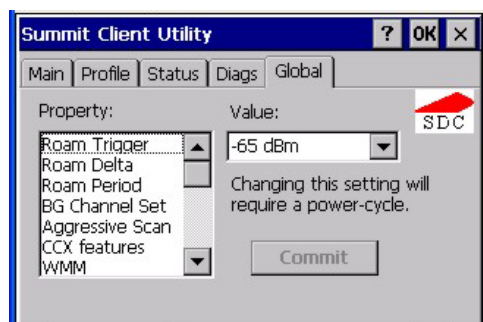
Factory Default Settings	
RX Diversity	On-Start on Main
TX Diversity	On
Preamble	Auto *
G Short Slot	Auto *
Roam Trigger	-65 dBm
Roam Delta	10 dBm
Roam Period	10 sec.
BG Channel Set	Full *
Aggressive Scan	On *
Frag Threshold	2346
RTS Threshold	2347
Ping Payload	32 bytes
Ping Timeout	5000
Ping Delay ms	1000
LED	Off
Hide Passwords	Off
Auth Timeout	8 seconds *
Admin Password	SUMMIT or blank
Certs Path	System
CCX	Off
WMM	Off
Tray Icon	On *

or

Figure 5-8 SCU – Global / Global Settings Tab

* Not available in all versions

Global / Global Settings Parameters

Custom Parameter Option

LXE does not support the parameter Custom option. The parameter value is displayed as "Custom" when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter's drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the "custom" value in the registry.

Parameter	Default	Function (* Not available in all versions)
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).
Preamble *	Auto	The type of network header, or preamble, for packets. Options are: Auto, Short, or Long.
G Short Slot *	Auto	802.1x short slot timing mode. Options are: Auto, On, or Off. *Note: The G Short Slot parameter has no effect on the Summit client device. This option is always set to On regardless of the parameter setting.*
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	10 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	10 sec	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.

Parameter	Default	Function (* Not available in all versions)
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Hide Password	Off	If On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT or blank	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.

Parameter	Default	Function (* **Not available in all versions**)
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the Windows folder path currently exists before assigning the path in this parameter. See sections titled *Root Certificates* and *User Certificates* later in this chapter for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out.
		Options are: none.
		For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
CCX or CCX Features	Off	Use of Cisco Compatible Extensions (CCX) radio management and Access Point specified maximum transmit power features.
		Options are: On, Off
WMM	Off	Use of Wi-Fi Multimedia extensions.
		Options are: On, Off
Tray Icon *	On	Determines if the Summit icon is displayed in the System tray.
		Options are: On, Off
Aggressive Scan *	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs.
		Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel.
		Options are: On, Off
Auth Timeout *	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail.
		If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed.
		If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials.
		Options are: An integer from 3 to 60.

Note: *Tap the* **Commit** *button to save changes. If this panel is closed before tapping the Commit button, changes are not saved!*

Summit Wireless Security

Use the instructions in this section to complete the entries on the Config or Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameter settings than are listed in these instructions. Please see your System Administrator for complete information about your network and its wireless security requirements.

Default profile	LXE recommends editing the Default profile instead of creating new profiles. **Important**: Perform a Warm Reset (using the Suspend/Resume key sequence) after changing parameters to save the changed parameters in the registry.
Switching profiles	Successfully connecting after switching from one profile to another may take up to 30 seconds from the moment the "Is not authenticated" or "Is not Associated" messages are displayed.
Adding, changing or renaming profiles	LXE recommends performing a Warm Reset function (using the Suspend/Resume key sequence) after tapping the Commit button.

Note: The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the Config tab. The reminder feature may not be present in all versions. Contact your LXE representative for version upgrades.

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers two choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the mobile device can access the network.
- The Username and Password are left blank on the Credentials screen. When the mobile device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

Note: It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

How to: Use Stored Credentials

1. After completing the other entries in the profile, tap the the **Credentials** button.
2. Enter the **Username** and **Password** on the Credentials screen and tap the **OK** button.
3. Tap the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
6. For EAP-TLS, also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the **CA Cert** (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the **User Cert** (User Certificate filename) on the credentials screen by using the **Browse** button.
10. If using EAP-FAST and manual PAC provisioning, input the PAC filename and password.

11. Tap the **OK** button then the **Commit** button.
12. Verify the device is authenticated by reviewing the Status tab. When the device is properly configured, the Status tab indicates the device is Authenticated and the method used.

Note: More details are provided in the appropriate Summit Wireless Security section following in this chapter. If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

> **How to: Use Sign On Screen**

1. After completing the other entries in the profile, tap the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or WPA/LEAP.
2. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
3. For EAP-TLS, also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the **CA Cert** (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the **User Cert** (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Tap the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the **Username** and **Password**. Tap the **OK** button.
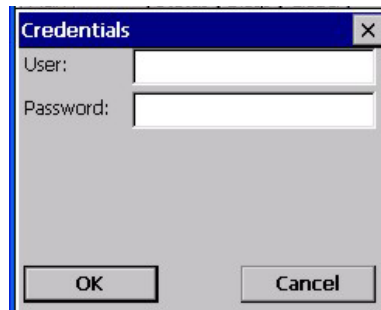

Figure 5-9 Sign-On Screen

Verify the device is authenticated by reviewing the **Status** tab. When the device is properly configured, the Status tab indicates the device is Authenticated and the method used.

The sign-on screen is displayed after a reboot for each of the listed protocols.

Note: *Complete details are provided in the appropriate Summit Wireless Security section following in this chapter.*

If a user enters invalid credentials and taps **OK***, the device associates but does not authenticate. The user is again prompted to enter credentials.*

If the user taps the **Cancel** *button, the device does not associate. The user is not prompted again for credentials until the device is rebooted, the radio is disabled then enabled, the* **Reconnect** *button on the Diags tag is tapped or the profile is modified and the* **Commit** *button is tapped.*

Windows Certificate Store vs. Certs Path

Note: *It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store. To generate the user certificate, follow the instructions in *Generating a User Certificate for the Mobile Device*, later in this chapter.

Import the user certificate into the Windows certificate store by following the instructions in *Installing a User Certificate on the Mobile Device*, later in this chapter. A Root CA certificate is also needed for EAP-TLS. Refer to the section below.

Root CA Certificates

Root CA certificates are required for PEAP/MSCHAP, PEAP/GTC, and EAP-TLS. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use Windows Certificate Store

1. Follow the instructions later in this chapter for *Downloading a Root CA Certificate to a PC.*
2. To import the certificate into the Windows store, follow the instructions for *Installing a Root CA Certificate on the Mobile Device* later in this chapter.
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to Step #8.
5. Otherwise, to select a specific certificate tap the **Browse** (…) button.

Figure 5-10 Choose Certificate

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and tap the **Select** button to return the selected certificate to the **CA Cert** textbox.
8. Tap **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use the Certs Path

1. Follow the instructions later in this chapter for *Downloading a Root CA Certificate to a PC*.
2. Copy the certificate to the specified Windows folder on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the **Certs Path** global variable. Please note the location chosen for certificate storage should persist after warmboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the **CA Cert** textbox.
5. Tap **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

No Security

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Config or Profile** tab.

 or

Figure 5-11 Configure a Summit Profile with No Security

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to None.

Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** function to connect using the new profile configuration.

Note: LXE recommends performing a Suspend/Resume function each time the Commit button is tapped.

WEP Keys

Please see your System Administrator for complete information about your network WEP key requirements.

To connect using WEP, use the following minimum required profile options..

- Auth Type = Open
- EAP Type = None
- Encryption = Manual WEP

Tap the **WEP keys/PSK Keys** button. The WEP Key Entry text entry box appears.

or
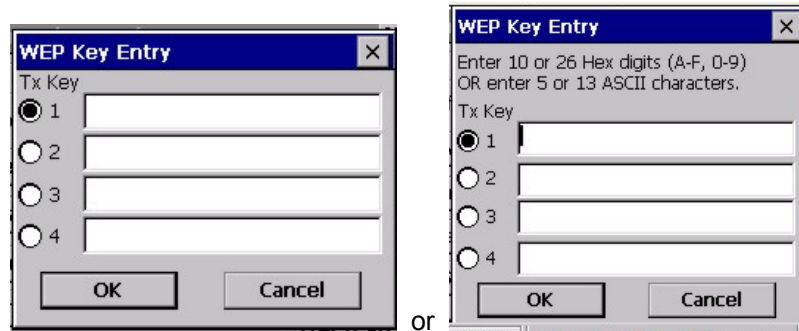
Figure 5-12 Summit WEP Keys

Enter the **WEP key**. If there are more than one set of keys, tap the radio button in front of the Key to be used.

WEP keys may be entered in Hex or ASCII format. For previous versions of the SCU, if the WEP key entry does not offer a choice between Hex and ASCII, the key must be in Hex (refer to the Hex Key Format segment that follows).

Once configured, tap **OK** then tap the **Commit** button. Ensure the correct Active Config is selected on the Main tab and warm boot. The SCU Main tab shows the device is associated after the radio connects to the network.

Hex Key Format

Valid keys are 10 (for 40 bit encryption) or 26 (for 128 bit encryption) hexadecimal characters (0-9, A-F). Enter the key(s) and tap **OK**.

ASCII Key Format

Valid keys are 5 (for 40 bit encryption) or 13 (for 128 bit encryption) alphanumeric characters. Enter the key(s) and tap **OK**.

LEAP w/o WPA Authentication

If the Cisco/CCX certified Access Point (AP) is configured for open authentication, set the Auth Type client parameter to **Open**.

If the AP is configured for network EAP only, set the Auth Type client parameter to **LEAP**.

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Admin Login **password** and tap OK. Tap the **Config or Profile** tab.

 or

Figure 5-13 Configure a Summit Profile for LEAP w/o WPA

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to LEAP.

Set **Encryption** to Auto WEP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

Figure 5-14 LEAP Credentials Dialog

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired.

Enter the **Password**, if desired. Tap **OK**.

Tap the **Commit** button to save the new profile configuration. Perform a **warm reset** to connect using the new profile configuration.

See Also: *WPA/LEAP Authentication* later in this section to configure the client for WPA LEAP.

See Also: *Sign-on vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

EAP-FAST Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.
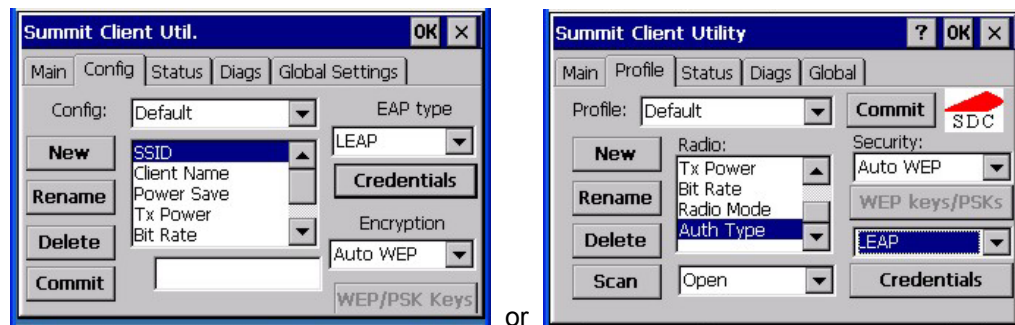
Tap the **Config or Profile** tab.

Figure 5-15 Configure a Summit Profile for EAP-FAST

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to EAP-FAST.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server.

The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the client device. Please refer to the *LXE Security Primer* for more information on the RADIUS server configuration.

To use Stored Credentials, tap the **Credentials** button.
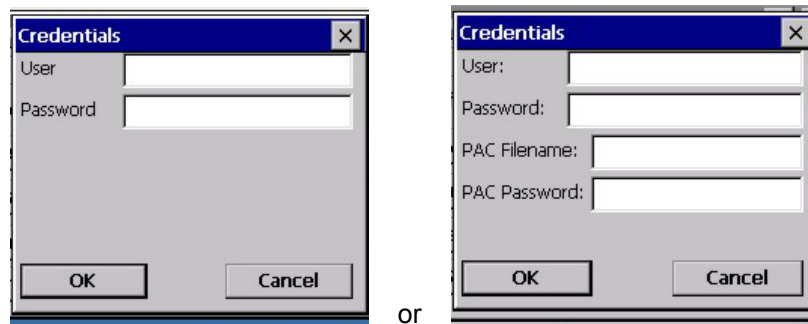
Figure 5-16 Summit EAP-FAST Credentials

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired.

Enter the **Password**, if desired. Tap **OK**.

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the mobile device. The same username/password must be used to authenticate each time. When using automatic PAC provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

For manual PAC provisioning, the PAC filename and password must be entered. The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be Read Only.

Tap OK then tap Commit to save the new profile configuration. Ensure the correct Active Profile is selected on the Main tab and perform a warmboot (or Suspend/Resume) function.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

PEAP/MSCHAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.
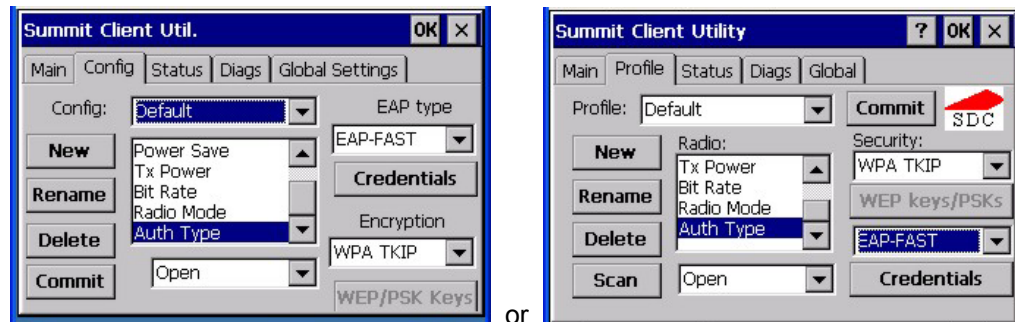
Tap the **Config or Profile** tab.

Figure 5-17 Configure a Summit Profile for PEAP/MSCHAP

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to PEAP-MSCHAP.

Set **Encryption** to Auto WEP (without WPA). To configure PEAP-MSCHAP for WPA set Encryption to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

Enter the **Username** or Domain\Username in the Credentials popup text entry box, if desired. Enter the **Password**, if desired. Leave the CA Certificate Filename blank for now. Tap **OK**. Tap **Commit**.

or
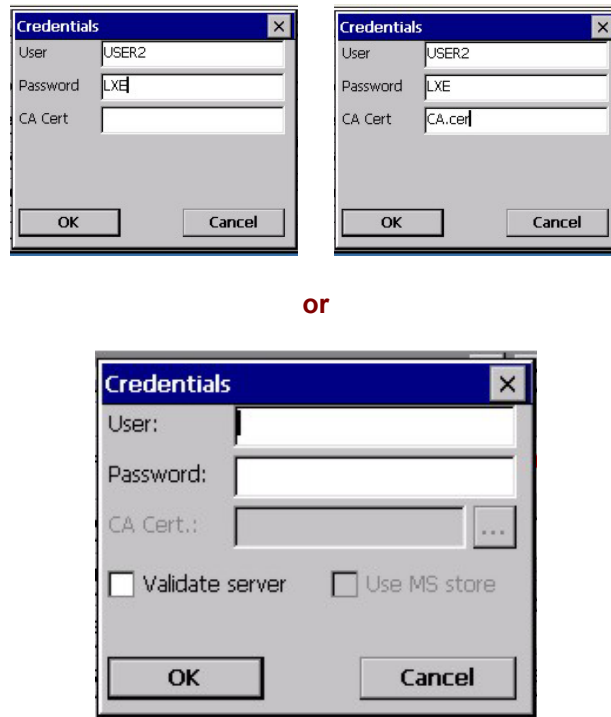
Figure 5-18 PEAP/MSCHAP Credentials

Note: The date must be properly set on the device to authenticate a certificate.

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [. . .] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit.**

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

WPA/LEAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.
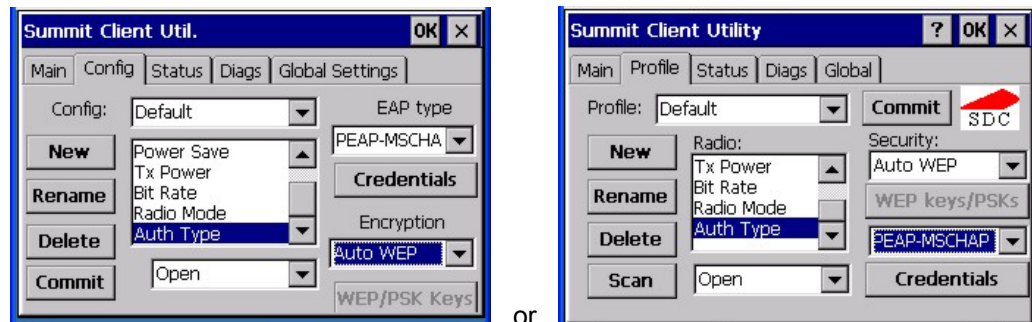
Tap the **Config or Profile** tab.

 or

Figure 5-19 Configure a Summit Profile with LEAP for WPA TKIP

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open. Set **EAP Type** to LEAP. Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

Figure 5-20 LEAP Credentials

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired. Enter the **Password,** if desired. Tap **OK**.

Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** (or Suspend/Resume) to connect using the new profile configuration.

See Also: *LEAP w/o WPA* earlier in this section to configure the client for LEAP without WPA.

See Also: *Sign-on vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.

Tap the **Config or Profile** tab.

 or

Figure 5-21 Configure a Summit Profile with WPA PSK Encryption

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to WPA PSK.

Tap the **WEP keys/PSK Keys** button.

Figure 5-22 Summit PSK Entry Dialog

Enter the Passphrase in the **PSK Entry** popup text entry box. This value can be a 64 hex character or an 8-63 byte ASCII value. Tap **OK**

Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** (or Suspend/Resume) to connect using the new profile configuration.

PEAP/GTC Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.
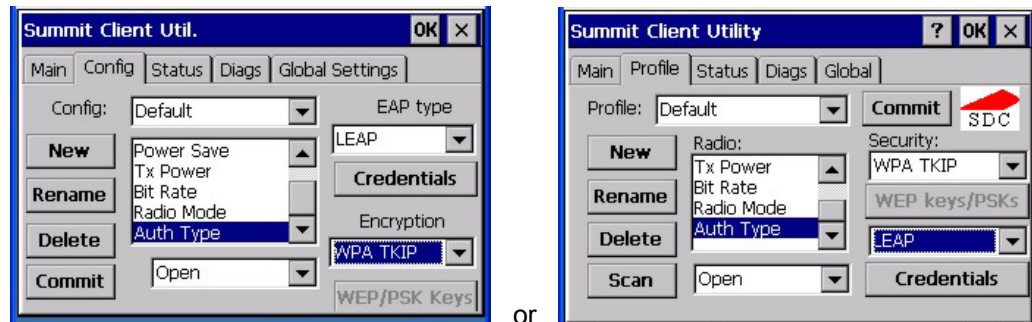
Tap the **Config or Profile** tab.

or
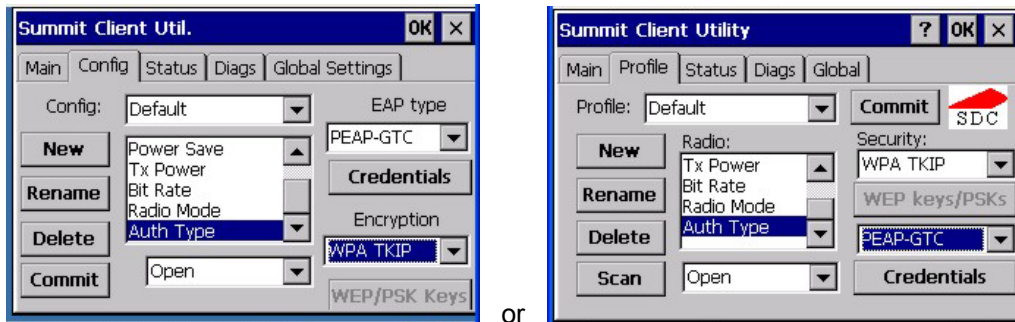
Figure 5-23 Configure a Summit Profile with PEAP/GTC

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to PEAP-GTC.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

or

Figure 5-24 PEAP/GTC Credentials

Note: The date must be properly set on the device to authenticate a certificate.

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [. . .] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit.**

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

EAP-TLS Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.
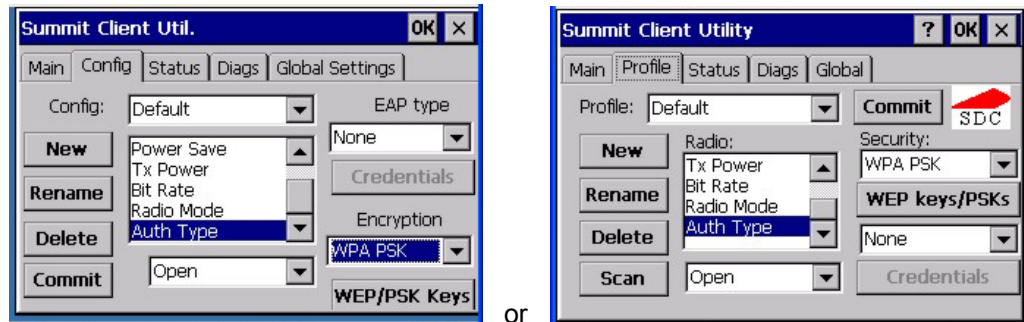
Tap the **Config or Profile** tab.
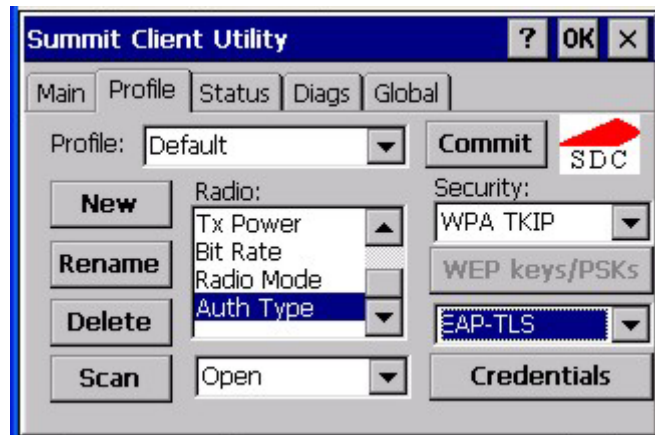
Figure 5-25 Configure a Summit Profile with EAP-TLS

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to EAP-TLS.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network. If the username and password are left blank during setup, see *Sign-On vs. Stored Credentials* earlier in this chapter.

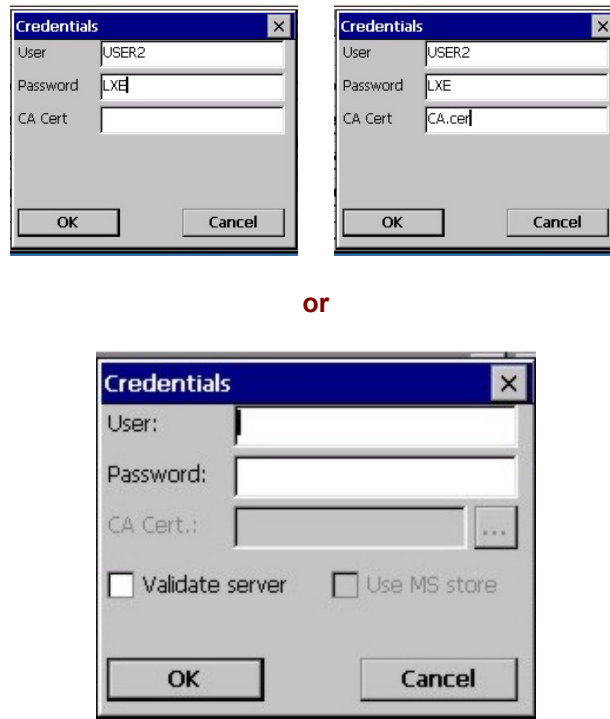*Note: The date must be properly set on the device to authenticate a certificate.*
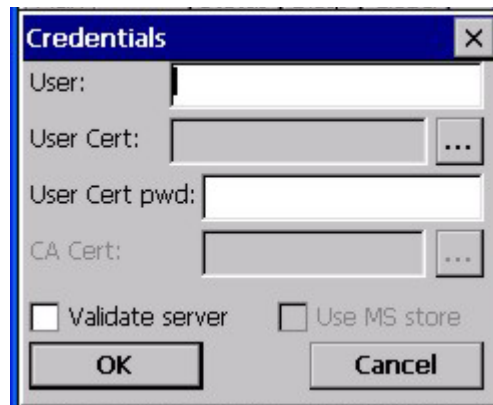
Figure 5-26 EAP-TLS Credentials Dialog

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [. . .] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit.**

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using EAP-TLS for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

Wireless Zero Config Utility and the Summit Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the Wireless Zero Config application is enabled and the HX2 is not connected to a network.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network.

LXE recommends using the Summit Client Utility to manage wireless connectivity.

To use Wireless Zero Config, first open the Summit Client Utility.

1. Select **ThirdPartyConfig** in the Active Config / Active Profile drop down box.
2. A message appears that a Power Cycle is required to make settings activate properly. Tap **OK**.
3. Tap the **Disable Radio** button to remove the connection to the Summit Client Utility. The text on the button changes to Enable Radio.
4. Tap the **Power** button to place the HX2 in **Suspend**, then tap the Power button to **wake the HX2** from Suspend mode.

The Wireless Zero Config utility begins.

Certificates

📖	Please refer to the *LXE Security Primer* to prepare the Authentication Server and Access Point for communication.
Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Root Certificates

Download a Root CA Certificate

The easiest way to get the root CA certificate is to **use a browser on a desktop PC** to navigate to the CA (Certificate Authority). To request the root CA certificate, **open a browser** to

> http://<CA IP address>/certsrv

Sign into the CA with any valid username and password.
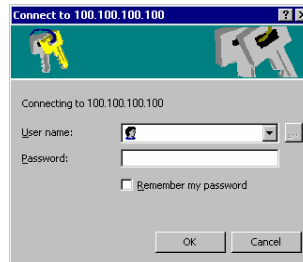
Figure 5-27 Logon to Certificate Authority
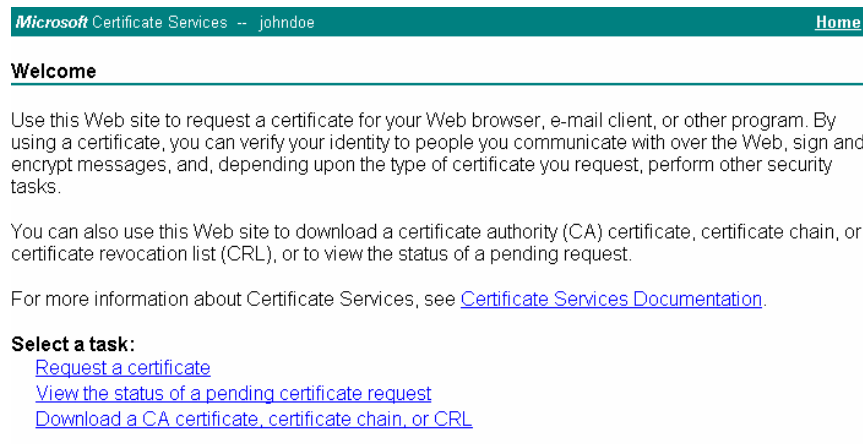
Figure 5-28 Certificate Services Welcome Screen

Tap the **Download a CA certificate, certificate chain or CRL** task link.

Make sure the correct root **CA certificate** is selected in the list box.
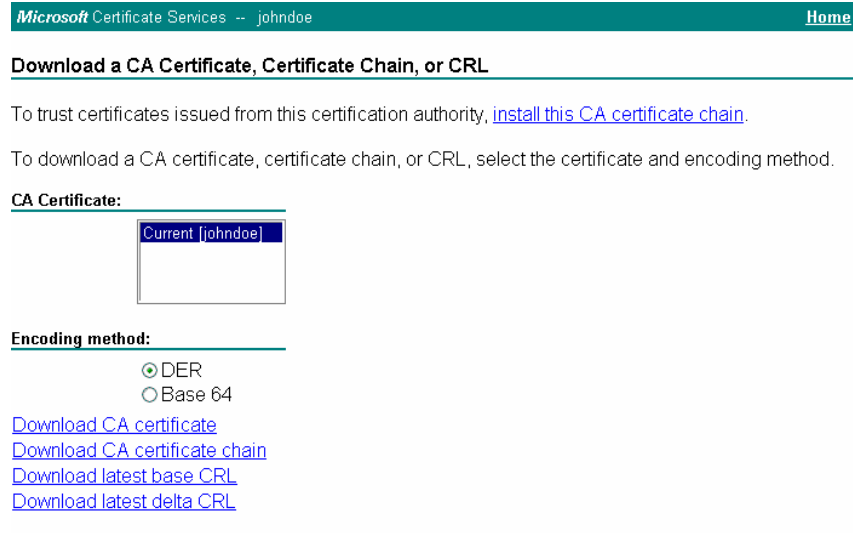
Figure 5-29 Download CA Certificate Screen

Tap the **DER** button.

To download the CA certificate, tap on the **Download CA certificate** link.
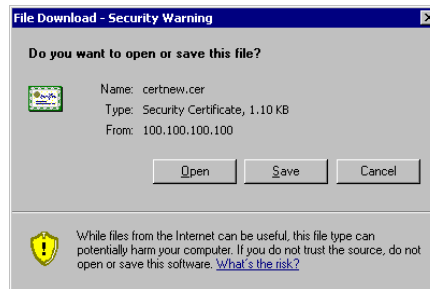
Figure 5-30 Download CA Certificate Save to Desktop

Tap the **Save** button and save the certificate to the desktop PC. Keep track of the name and location of the certificate as the certificate file name and file location is required in later steps.

Installing a Root CA Certificate on the Mobile Device

Copy the certificate file from the desktop PC to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Figure 5-31 Certificate Stores

Tap the **Import** button.

Figure 5-32 Import Certificate From a File

Make sure **From a File** is selected and tap OK.

Figure 5-33 Browsing to Certificate Location

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

Tap **OK** to import the certificate.

Once the certificate is installed, return to the proper authentication section, described later in this chapter.

User Certificates

Generating a User Certificate for the HX2

The easiest way to get the user certificate is to **use a browser on a PC** to navigate to the CA. To request the user certificate, open a browser to

http://<CA IP address>/certsrv

Sign into the CA with the username of the user certificate required.

Figure 5-34 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. Windows CE devices such as the HX2 require the private key to be saved as a separate file rather than including the private key in the user certificate.
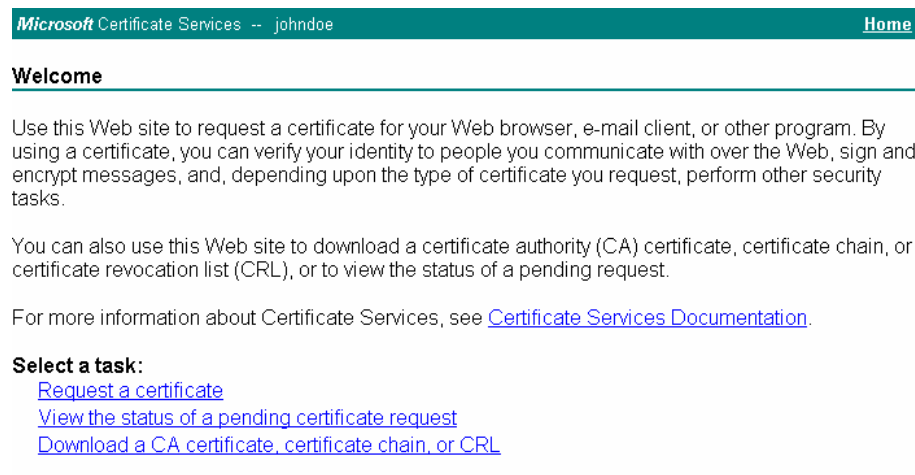
Figure 5-35 Certificate Services Welcome Screen

Tap the **Request a certificate** task link.

Microsoft Certificate Services -- johndoe   **Home**

Request a Certificate

Select the certificate type:
   User Certificate

Or, submit an *advanced certificate request*.
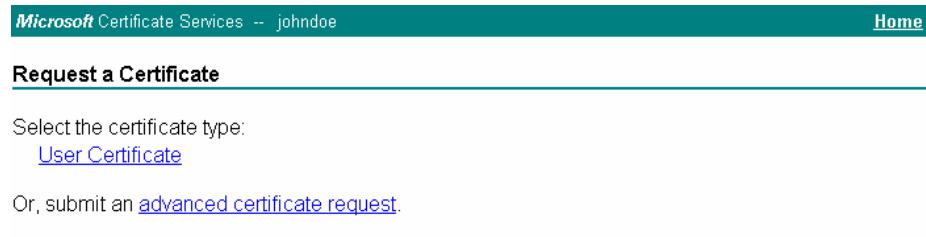
Figure 5-36 Request a Certificate Type

Tap on the **advanced certificate request** link.

Microsoft Certificate Services -- johndoe   **Home**

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

   Create and submit a request to this CA.

   Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

   Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
   Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 5-37 Advanced Certificate Request Screen

Tap on the **Create and submit a request to this CA** link.

Figure 5-38 Advanced Certificate Details

For the Certificate Template, select **User**.

Check the **Mark keys as exportabl**e and the **Export keys to file** checkboxes.

Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

⚠	Be sure to note the name used for the private key file, for example HX2USER.PVK. The certificate file created later in this process must be given the same name, for example, HX2USER.CER.

DO NOT check "Enable strong private key protection".

Make any other desired changes and tap the **Submit** button.
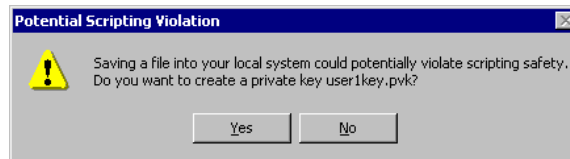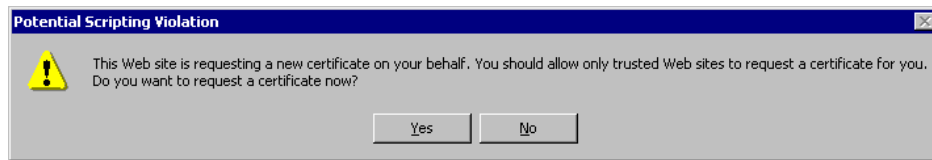
Figure 5-39 Script Warnings

If any script notifications occur, tap the **Yes** button to continue the certificate request.

Figure 5-40 Script Warnings

When prompted for the private key password:

- Tap **None** if you do not wish to use a password, *or*
- Enter and confirm your desired password then tap **OK**.
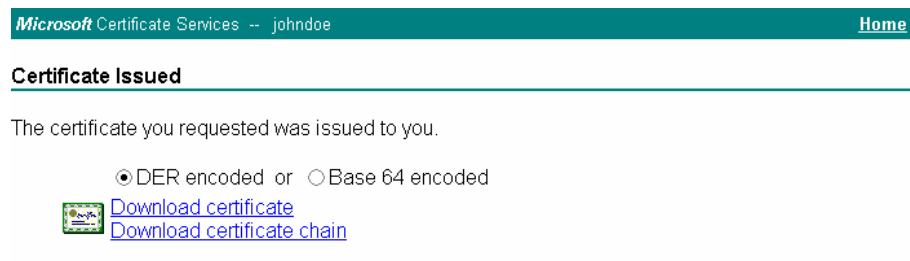
Figure 5-41 User Certificate Issued

Tap the **Download certificate** link.

Figure 5-42 Download Certificate Security Warning

Tap **Save** to download and store the user certificate **to the PC**. Keep track of the name and location of the certificate as the file name and location is required in later steps. The private key file is also downloaded and saved during this process.

⚠️	Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as HX2USER.PVK then the certificate file created must be given the same name, for example, HX2USER.CER.

Installing a User Certificate on the HX2 (WPA-TLS Only)

> *Note: TLS is not supported by LXE in this release. Contact your LXE representative for availability.*

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select **My Certificates** from the pull down list.
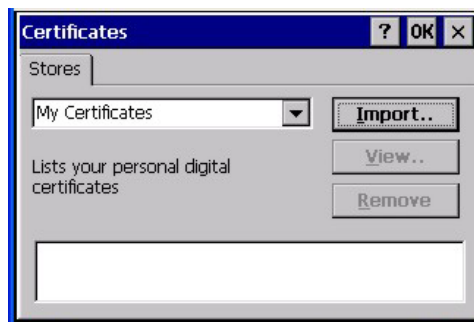
Figure 5-43 My Certificates Stores

Tap the **Import** button.
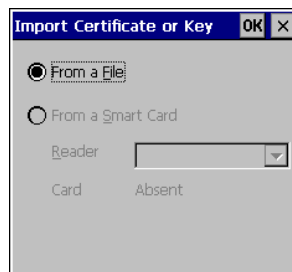
Figure 5-44 Import User Certificate

Make sure **From a File** is selected and tap OK.

Figure 5-45 Browsing to Certificate Location

Using the explorer buttons, browse to the location on the mobile device where you copied the certificate, select the certificate desired and tap OK.

Tap **Yes** to import the certificate. The certificate is now shown in the list.

Highlight the certificate you just imported and tap the **View. .** button.

From the Field pull down menu, select **Private Key**.

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen.

Tap **import**.

Figure 5-46 Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the **Type** pull down list to **Private Keys**, select the certificate desired and tap **OK**.

Tap on **View** to see the certificate details again.

The private key should now say "Present". If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example HX2USER.CER for the certificate and HX2USER.PVK for the private key file. If the file names are not the same, rename the private key file and import it again.

Chapter 6 AppLock

Introduction

> *Note:* *AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels. For example, Keypad Control Panel LaunchApp and RunCmd options .*

> *Note:* *LXE has made the assumption, in this chapter, that the first user to power up a new mobile device is the system administrator.*

LXE's AppLock is designed to be run on LXE certified Windows CE based devices only. LXE loads the AppLock program as part of the LXE customer installation process.

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end-user can still warm boot the mobile device, tap the touch screen, respond to dialog boxes, and if enabled by the administrator, select applications using the Switchpad.

When the mobile device is reset to factory default values the Administrator may need to reconfigure the AppLock parameters and the application switching activation key sequence.

> *Note:* *AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.*

> *Note:* *A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see **Auto Re-Launch**) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.*

> *Note:* *Alpha Mode 3 Tap Keypad Only -- If the input panel is not the HX2 default input method, the administrator may not be able to switch to user mode since the HX2 does not have any shift state keys. The Dual Alpha and Triple Tap keypads are not affected by the available-key exception.*

Application Panel
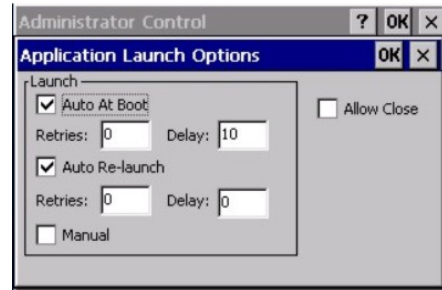
Application – Launch Panel

Security Panel

Status Panel
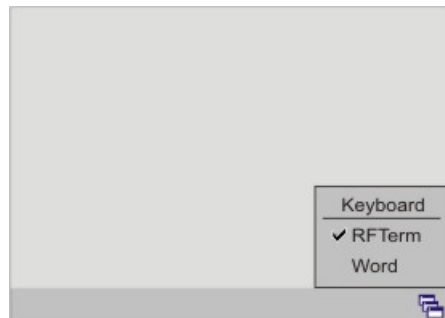
End-User Switchpad

Figure 6-1 AppLock Screens

Setup a New Device

Prerequisites:

- The touch panel must be enabled.
- All "normal" keys must be identified/available by the System Administrator. See Chapter 2 – Physical Description and Layout, section titled Keypad.
- See Creating Hotkey and Switch Key Sequences later in this chapter.
- An HX2 default input method (Input Panel, Transcriber, or custom input method) is assigned.

LXE CE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies an application to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Insert a fully charged battery and press the Power button.
2. Adjust screen display, audio volume and other parameters if desired. Install accessories, if necessary.
3. Tap **Start | Settings | Control Panel | Administration** icon.
4. Assign a **Switch Key** (hotkey) sequence for AppLock. See *Security Panel*.
5. Assign an application on the **Application** tab screen. More than one application can be assigned on the Application tab screen. See *Application Panel*.
6. Assign a **password** on the Security tab screen. See *Security Panel*.
7. Select a **view level** on the Status tab screen, if desired. See *Status Panel*.
8. Tap **OK**.
9. Press the **hotkey sequence** to launch AppLock and lock the configured application(s). If the Dual Alpha or Triple Tap keypad are in use, the AppLock default Administrator Hotkey sequence (Shift+Ctrl+A) must be modified.
10. The device is now in **end-user mode**.

Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.

Creating Hot Key and Switch Key Sequences

HX2 hotkeys are used when switching between AppLock Administration and User mode and therefore need to be key sequences that the end-user would not normally use.

The Alpha Mode 3 Tap limited keypad does not provide enough keys for the Administrator to define a shifted state (Shift, Alt, or Ctrl) key combination for the hotkey.

The Dual Alpha and Triple Tap keypads are not affected by this exception. See *Setting an Activation Hotkey* in *Security Panel* later in this chapter if using an HX2 with a Dual Alpha or Triple Tap keypad.

The AppLock administrator, or system administrator, must use the Input Panel and the Alpha Mode 3 Tap keypad to enter setup information in the Administration tab and to initiate a hotkey switch. The shift state keys are selected using the Input Panel and the normal key is selected using the HX2 keypad.

Example:

Suppose the administrator sets up Ctrl+Shift+7 as the mode switching hotkey for an HX2 with the Alpha Mode 3 Tap keypad. Once in user mode, the administrator should follow the steps below to activate the hotkey and initiate a mode switch into administration mode.

1. Select the Switchpad by tapping the Switchpad icon (it looks like three tiny windows one above the other in the taskbar in the lower right corner of the screen).
2. Activate the Input Panel by tapping Keyboard on the menu that pops up.
3. From the Input Panel, select the shift state keys. For the example hotkey, tap both Shift and Ctrl as shown in the figure that follows:
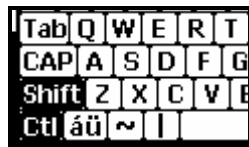
4. Finally, press the normal key on the Alpha Mode 3 Tap keypad. In our example, press '7' on the keypad.

At this point the mode switch will occur resulting in either a password prompt, if a password is configured, or full access to the HX2 with an Alpha Mode 3 Tap keypad.

The Switchpad

The end-user can switch between locked applications using the Switchpad on the HX2. The user should tap the Switchpad icon first; it looks like three tiny windows one above the other in the taskbar. The Switchpad is displayed.
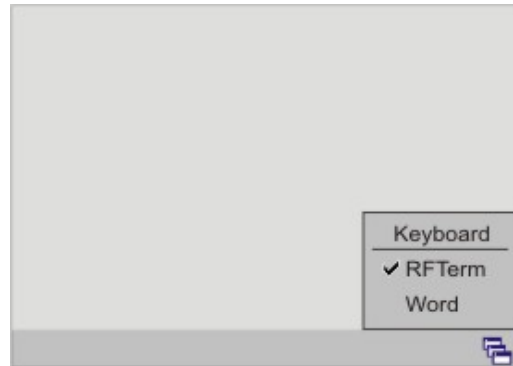
Figure 6-2 Switchpad

If Keyboard is selected, the HX2 default input method is activated. This allows the administrator to choose a different input method (such as the transcriber or a custom input method) as the default and the end-user will have access to that method in the locked applications.
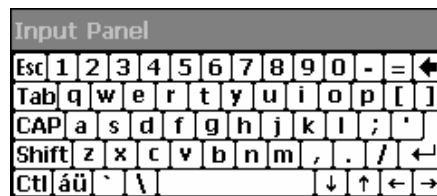
Figure 6-3 Keyboard (Input Panel) Selected

If the HX2 default input method is Keyboard, the input panel is displayed and the Switchpad is closed. The next time the Switchpad is opened, a check mark appears next to Keyboard to show the input method is activated.

See *Chapter 3 – System Configuration*, section titled *Transcriber* for instruction if using the Microsoft OS Transcriber option.

See Also: *Application Panel | Global Key*

Administration Mode

Access: **| Settings | Control Panel | Administration icon**

Administration mode gives full access to the mobile device and configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application, or applications, to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	Shift+Ctrl+A
Password	none
Application path and name	none
Application command line	none

Note: The AppLock default Administrator Hotkey must be modified during initial setup of a new device. See Security Panel for instruction.

End-User Mode

End-user mode locks the end-user into the configured application (or applications). The end-user can still reboot, tap the touch screen, respond to dialog boxes, and if enabled by the administrator, select applications using the Switchpad. AppLock is automatically launched, and runs in full screen mode when the mobile device boots up.

Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, etc. are disabled. The Windows CE desktop icons, menu bars, and system trays are not visible or accessible. Windows Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user taps on the Close icon on the application's title bar and the application remains active.

See Also: *Application Panel | Launch Button*

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three tries) to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt – this is because the other situations result in invalid end-user operation.

These conditions include:

1. If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
2. If the application name, which is mandatory for end-user mode, is missing in the configuration.
3. Invalid installation of AppLock (e.g. missing DLLs).
4. Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Troubleshooting – Can't locate the password that has been set by the administrator? Enter the LXE back door key sequence: Ctrl+5 | Ctrl+9 | Ctrl+3 (Does not apply to the Alpha Mode 3 Tap keypad.)

Multi-Application Configuration

Access: 🏁 **| Settings | Control Panel | Administration icon**

Note: *AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to Administration mode.*

Application Panel

Access: 🏁 **| Settings | Control Panel | Administration icon**

Figure 6-4 Application Panel – Multi-Application

Use the **Application** tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the application switcher panel.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order.

Option	Explanation
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled *End-user Internet Explorer* for more details.
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the *Activation* key. Refer to *Global Key and the HX2 with an Alpha Mode 3 Tap Keypad*.
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the **Clear** button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right **scroll buttons** to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Global Key and the HX2 with an Alpha Mode 3 Tap Keypad

If the administrator wants the user to be able to switch between multiple locked applications with the keypad, they must remap an HX2 (with an Alpha Mode 3 Tap keypad) function key (F1, F2, F3 or F4) to one of the key combinations defined in Applock as switching keys.

These keys include:

- Ctrl+Z
- Ctrl+Y
- Ctrl+Space
- Ctrl+T
- Ctrl_J
- Ctrl+9
- Ctrl+8
- Ctrl+7

The Dual Alpha and Triple Tap keypads are not affected by the available-key exception.

Launch Button

When clicked, displays the launch options panel for the selected Filename (see the Administration panel) as shown below:
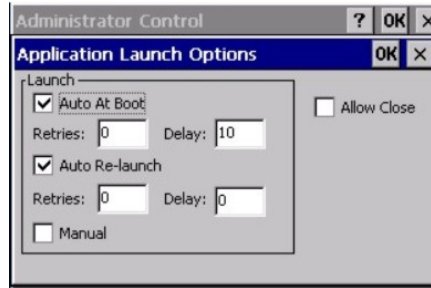
Figure 6-5 Application Launch Options

Auto At Boot

Default is Enabled. Auto At Boot, when enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 "no delay" and a maximum of 999 seconds.

Auto At Boot **Retries** is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Auto At Boot **Delay** timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A "Global Delay" can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch

Default is Enabled. Auto Re-Launch, when enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.
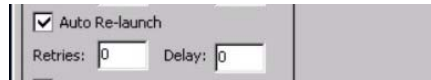
> *Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.*

Auto Re-Launch **Retries** default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Auto Re-Launch **Delay** timer default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)

Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

<u>Allow Close</u>

Default is Disabled. When enabled, the associated application can be closed by the end-user.
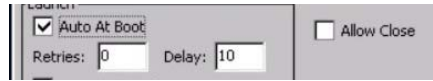
This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Internet / End-user Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end-user can run an application by entering the application name and path in Internet Explorer's address bar.

When the Internet checkbox is enabled (checked), the **Menu** and **Status** check boxes are available. Default is Disabled and the Menu and Status checkboxes are dimmed (unavailable).

To prevent the end-user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end-user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end-user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the **Internet** checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the **Application** text box.

Enabling the **Menu** checkbox displays the EUIE's menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the **Status** checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel

Figure 6-6 Security Panel – Multi-Application

Refer to *Global Key and the HX2 with an Alpha Mode 3 Tap Keypad*.

Administrator Hotkey

Specify the key sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence must be created by the AppLock administrator.

A multi-key keypress is an invalid keypress for a hotkey sequence. Only face keys can be used as the normal key in the hotkey or switch key sequence. Therefore, keys accessed via a modifier key, Green, Orange, Blue or any other modified key may not function properly as the hotkey.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application. **See Also**: *Creating Hotkey and Switch Key Sequences*.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with **Shift** and **Ctrl** text strings representing the shift state keys. The normal (face) keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the Input Panel are not guaranteed to work properly when switching operational modes.

For example, if the 'Ctrl' key is pressed followed by 'A', "Ctrl+A" is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the Input Panel keyboard when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the Input Panel keyboard.

Note: The AppLock default Administrator Hotkey must be modified during initial setup of a new device.

Password

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords **are** case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: *Passwords* and *Troubleshooting Multi-Application AppLock*

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.
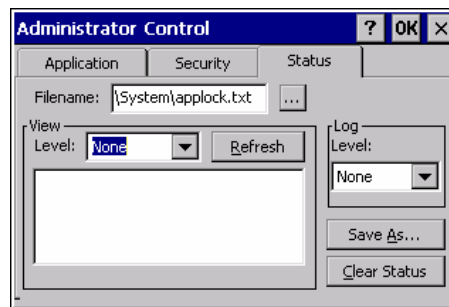
Figure 6-7 Status Panel – Multi-Application

Filename   Move the cursor to the **Filename** text box and either type the logfile path or tap the Browse button (the … button).

The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

View

Error Level   Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.

Process Level   Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.

Extended Level   Extended status provides more detailed information than that logged by Process Logging.

All Level   All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

> *Note:*   *If a level higher than Error is selected, the status log should be cleared frequently by the administrator. Tap the Clear Status button.*

In addition to the three view filter levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is None; however to reduce registry use, the administrator may want to select **None** after verifying the configuration.

The Logging Level options are: None, Error, Processing, Extended and All.

Buttons

Save As   When the 'Save As'… button is tapped, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

Clear Status   Tap the Clear Status button to clear the status information (generated by the settings in the Log section) from the registry.

See Also: *Error Messages.*

End-User Switching Technique

> *Note:*   *The touch screen must be enabled.*

Switchpad Menu   Switchpad Icon in Taskbar
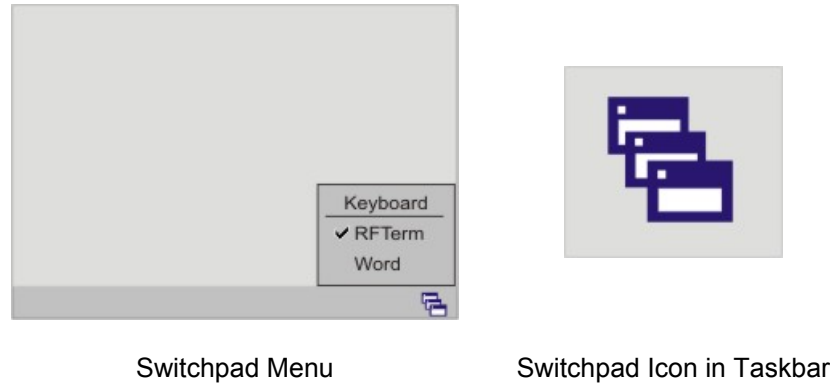
Figure 6-8 Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the HX2 default input method (Input Panel, Transcriber, or custom input method) is activated.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the taskbar. The taskbar is always visible on top of the application in focus.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

The figure shown above is an example and is shown only to aid in describing how the user can switch between applications using a stylus. The switchpad lists user applications as well as the Keyboard option.

See Also: *Application Panel | Launch | Manual (Launch) and Allow Close*

Using the Switch key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: *Application Panel | Global Key*

Refer to *Global Key and the HX2 with an Alpha Mode 3 Tap Keypad*.

Troubleshooting Multi-Application AppLock

> **The mobile device won't switch from Administration mode to end-user mode.**

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

> **The hotkey sequence needed is not allowed. What does this mean?**

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

> Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
****************	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete applock.exe from the \Windows directory and reboot the unit. Deleting applock.exe in this manner triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX

Message	Explanation and/or corrective action	Level
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete applock.exe from the \Windows directory and reboot the unit. Deleting applock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX

Message	Explanation and/or corrective action	Level
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX

Message	Explanation and/or corrective action	Level
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. . If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the "Registry read failure" above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

AppLock Registry Settings

This system application runs at startup via the *launch* feature of LXE Windows CE devices. When the launch feature is installed on the mobile device, the following registry settings are created. The launch feature registry settings are embedded in the mobile device OS image:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Filename=AppLock.exe
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Installed=
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\FileCheck=
```

AppLock registry settings identify the application that is going to be locked and any parameters that are needed by the application. These registry settings are as follows:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Administration\\AppName
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppCommandLine=
```

In addition to the registry settings needed to specify the application, additional registry settings are needed to store the configuration options for AppLock. These options include, among others, the administrator's password and hotkey.

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\HotKey=
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\EP=
```

Appendix A Key Maps

23 Key Keypad

Alpha Mode 3 Tap	The HX2 default keypad on all HX2s shipped prior to September 2007. Setup requires no user interaction.
Dual Alpha	Set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped. Setup requires no user interaction with the My Device / Windows / Dual_Alpha.reg file.
Triple Tap	Requires file activation to setup the Triple Tap keypad for daily use. Setup requires the My Device / Windows / Triple_Tap.reg file be tapped and the HX2 warmbooted. Warmboot the HX2 by tapping Start | Run and, using the SIP, typing WARMBOOT. Tap OK.

Alpha Mode 3 Tap

Hints

- When using a sequence of keys that require an alpha key, first press the Alpha key.
- Double tap the Alpha key for upper case alphabetic characters.
- Single tap the Alpha key to enter and exit Alpha mode.
- Default Alpha mode produces lower case alphabetic characters when numeric keys are pressed.
- Pressing the Alpha key forces "Alpha" mode for all keys.

- To create a combination of numbers and letters before pressing Enter, remember to tap the Alpha key to toggle between Alpha and Numeric mode.
- Use the Input Panel to enter characters that are not available using the 23-key keypad.
- When using a sequence of keys that do not include the Alpha key (Orange) but does include a sticky key (Blue), press the Blue key first then the rest of the key sequence.

To Get This Key / Function	First Press This Key		Then Press This Key
	Blue	Alpha	
Power / Suspend			Power
Volume Up	X		Up Arrow
Volume Down	X		Down Arrow
Blue Mode (Toggle)			Blue
Alpha Mode (Toggle)			Alpha
Diamond Key	X		Enter
⊞ (Start Button)			Only Available when Mapped
Display Brightness Increase / Decrease			Only Available when Mapped
Uppercase Alpha (Toggle) [6]		Alpha	Doubleclick
Alpha key [4]			
Lowercase Alpha [4]			N/A (default)
Space		Alpha	0
Enter			Enter
CapsLock Mode [4]		Alpha times 2	Alpha
Back Space			Backspace
Escape	X		Backspace
Tab	X		Right Arrow
BackTab	X		Left Arrow
Up Arrow (Cursor Up)			Up Arrow
Down Arrow (Cursor Down)			Down Arrow
Right Arrow (Cursor Right)			Right Arrow
Left Arrow (Cursor Left)			Left Arrow
F1			F1
F2			F2
F3			F3
F4			F4
F5	X		F1
F6	X		F2
F7	X		F3
F8	X		F4
F9			Only Available when Mapped [3]
F10	X		0
F11	X		1
F12	X		2
F13	X		3
F14	X		4
F15	X		5
F16	X		6
F17	X		7
F18	X		8
F19	X		9
F20 through F24			Only Available When

[6] See *Using the 23 Key Keypad* for explanation.

To Get This Key / Function	First Press This Key		Then Press This Key
	Blue	**Alpha**	
			Mapped [3]
a		**Alpha**	2
b		**Alpha**	22
c		**Alpha**	222
d		**Alpha**	3
e		**Alpha**	33
f		**Alpha**	333
g		**Alpha**	4
h		**Alpha**	44
i		**Alpha**	444
j		**Alpha**	5
k		**Alpha**	55
l		**Alpha**	555
m		**Alpha**	6
n		**Alpha**	66
o		**Alpha**	666
p		**Alpha**	7
q		**Alpha**	77
r		**Alpha**	777
s		**Alpha**	7777
t		**Alpha**	8
u		**Alpha**	88
v		**Alpha**	888
w		**Alpha**	9
x		**Alpha**	99
y		**Alpha**	999
z		**Alpha**	9999
A		**Alpha times 2**	2
B		**Alpha times 2**	22
C		**Alpha times 2**	222
D		**Alpha times 2**	3
E		**Alpha times 2**	33
F		**Alpha times 2**	333
G		**Alpha times 2**	4
H		**Alpha times 2**	44
I		**Alpha times 2**	444
J		**Alpha times 2**	5
K		**Alpha times 2**	55
L		**Alpha times 2**	555
M		**Alpha times 2**	6
N		**Alpha times 2**	66
O		**Alpha times 2**	666
P		**Alpha times 2**	7
Q		**Alpha times 2**	77
R		**Alpha times 2**	777
S		**Alpha times 2**	7777
T		**Alpha times 2**	8
U		**Alpha times 2**	88
V		**Alpha times 2**	888
W		**Alpha times 2**	9
X		**Alpha times 2**	99
Y		**Alpha times 2**	999
Z		**Alpha times 2**	9999
1			1 and 11111 (Alpha Mode)

To Get This Key / Function	First Press This Key		Then Press This Key
	Blue	Alpha	
2			2 and 2222 (Alpha Mode)
3			3 and 3333 (Alpha Mode)
4			4 and 4444 (Alpha Mode)
5			5 and 5555 (Alpha Mode)
6			6 and 6666 (Alpha Mode)
7			7 and 77777 (Alpha Mode)
8			8 and 8888 (Alpha Mode)
9			9 and 99999 (Alpha Mode)
0			0 and 00 (Alpha Mode)
. (period)		Alpha	1
\		Alpha	11
* (asterisk)		Alpha	111
- (dash or minus sign)		Alpha	1111
< >			Use Input Panel
[ ]			Use Input Panel
{ }			Use Input Panel
( )			Use Input Panel
_ (underscore)			Use Input Panel
+ (plus sign)			Use Input Panel
: ;			Use Input Panel
" '			Use Input Panel
? /			Use Input Panel
` ~			Use Input Panel
!			Use Input Panel
@			Use Input Panel
#			Use Input Panel
$			Use Input Panel
%			Use Input Panel
^			Use Input Panel
&			Use Input Panel
|			Use Input Panel

Dual Alpha Keypad

> **Hints**
>
> - Any key press exits out of the volume and backlight control modes.
> - Modifier keys are sticky.
> - A modifier key (Green, Orange, Blue, Shift and Control) pressed after itself toggles that modifier key off.
> - Any key other than a modifier key following any modifier key, unsticks the modifier keys.

To Get This Dual Alpha Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	◁1	
Power / Suspend						Power/Suspend
Volume Up		X			X	Up Arrow
Volume Down		X			X	Down Arrow
Display Backlight Increase			X		X	Up Arrow
Display Backlight Decrease			X		X	Down Arrow
Alt Mode	X					Ctrl
Ctrl Mode						Ctrl
Escape						ESC
Green Mode (Toggle)	X					Green
Orange Mode (Toggle)		X				Orange
Blue Mode (Toggle)			X			Blue
Diamond 1 Mode					X	--
Diamond 2 Mode	X				X	--
(Start Button)						CTRL + ESC
Uppercase Alpha (Toggle)						Shift
Lowercase Alpha						-- (alpha is the default setting)
Space	X					BKSP (Backspace)
Enter						Enter
Capslock (Toggle)						N/A
Back Space						Backspace
Tab						Tab

To Get This Dual Alpha Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	①	
BackTab	X					Tab
Up Arrow (Cursor Up)						Up Arrow
Down Arrow (Cursor Down)						Down Arrow
Right Arrow (Cursor Right)	X					Down Arrow
Left Arrow (Cursor Left)	X					Up Arrow
Insert		X	X			5
Delete		X	X			1
Home		X	X			7
End		X	X			3
Page Up		X	X			0
Page Down		X	X			BKSP (Backspace)
F1	X					1
F2	X					2
F3	X					3
F4	X					4
F5	X					5
F6	X					6
F7	X					7
F8	X					8
F9	X					9
F10	X					0
F11	X			X		1
F12	X			X		2
F13	X			X		3
F14	X			X		4
F15	X			X		5
F16	X			X		6
F17	X			X		7
F18	X			X		8
F19	X			X		9
F20	X			X		0
F21	X		X	X		1
F22	X		X	X		2
F23	X		X	X		3
F24	X		X	X		4
a		X				1
b			X			1
c		X				2
d			X			2
e		X				3
f			X			3
g		X				4
h			X			4
i		X				5
j			X			5
k		X				6
l			X			6
m		X				7
n			X			7
o		X				8
p			X			8
q		X				9

To Get This Dual Alpha Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	①	
r			X			9
s		X				Up Arrow
t			X			Up Arrow
u		X				0
v			X			0
w		X				BKSP
x			X			BKSP
y		X				Down Arrow
z			X			Down Arrow
A		X		X		1
B			X	X		1
C		X		X		2
D			X	X		2
E		X		X		3
F			X	X		3
G		X		X		4
H			X	X		4
I		X		X		5
J			X	X		5
K		X		X		6
L			X	X		6
M		X		X		7
N			X	X		7
O		X		X		8
P			X	X		8
Q		X		X		9
R			X	X		9
S		X		X		Up Arrow
T			X	X		Up Arrow
U		X		X		0
V			X	X		0
W		X		X		BKSP
X			X	X		BKSP
Y		X		X		Down Arrow
Z			X	X		Down Arrow
1						1
2						2
3						3
4						4
5						5
6						6
7						7
8						8
9						9
0						0
. (period)		X				Tab
* (asterisk)			X			Tab
- (dash or minus sign)	X		X			Tab
/	X		X			0
' (single quote)	X		X			1
[	X		X			2
]	X		X			3

To Get This Dual Alpha Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	①	
\	X		X			4
' (apostrophe)	X		X			5
, (comma)	X		X			6
` (accent)	X		X			7
; (semicolon)	X		X			8
= (equal sign)	X		X			9
!				X		1
@				X		2
#				X		3
$				X		4
%				X		5
^				X		6
&				X		7
* (asterisk)				X		8
(				X		9
)				X		0
" (double quote)	X	X				1
{	X	X				2
}	X	X				3
| (broken bar)	X	X				4
~ (tilde)	X	X				5
<	X	X				6
>	X	X				7
: (colon)	X	X				8
+ (plus sign)	X	X				9
?	X	X				0
_ (underscore)	X	X				TAB

Triple Tap Keypad

> **Hints**
>
> - Any key press exits out of the volume and backlight control modes.
> - Modifier keys are sticky.
> - A modifier key (Green, Orange, Blue, Shift and Control) pressed after itself toggles that modifier key off.
> - Any key other than a modifier key following any modifier key, unsticks the modifier keys.

To Get This Triple Tap Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	◁1	
Power / Suspend						Power/Suspend
Volume Up		X			X	Up Arrow
Volume Down		X			X	Down Arrow
Display Backlight Increase			X		X	Up Arrow
Display Backlight Decrease			X		X	Down Arrow
Alt Mode	X					Ctrl
Ctrl Mode						Ctrl
Escape						ESC
Green Mode (Toggle)	X					Green
Orange Mode (Toggle)		X				Orange
Blue Mode (Toggle)			X			Blue
Diamond 1 Mode					X	--
Diamond 2 Mode	X				X	--
⊞ (Start Button)						CTRL + ESC
Uppercase Alpha (Toggle)						Shift
Lowercase Alpha						-- (alpha is the default setting)
Space	X					BKSP (Backspace)
Enter						Enter
Capslock (Toggle)						N/A
Back Space						Backspace
Tab						Tab

To Get This Triple Tap Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	①	
BackTab	X					Tab
Up Arrow (Cursor Up)						Up Arrow
Down Arrow (Cursor Down)						Down Arrow
Right Arrow (Cursor Right)	X					Down Arrow
Left Arrow (Cursor Left)	X					Up Arrow
Insert		X	X			5
Delete		X	X			1
Home		X	X			7
End		X	X			3
Page Up		X	X			0
Page Down		X	X			BKSP (Backspace)
F1	X					1
F2	X					2
F3	X					3
F4	X					4
F5	X					5
F6	X					6
F7	X					7
F8	X					8
F9	X					9
F10	X					0
F11	X			X		1
F12	X			X		2
F13	X			X		3
F14	X			X		4
F15	X			X		5
F16	X			X		6
F17	X			X		7
F18	X			X		8
F19	X			X		9
F20	X			X		0
F21	X		X	X		1
F22	X		X	X		2
F23	X		X	X		3
F24	X		X	X		4
a			X			2
b			X			22
c			X			222
d			X			3
e			X			33
f			X			333
g			X			4
h			X			44
i			X			444
j			X			5
k			X			55
l			X			555
m			X			6
n			X			66
o			X			666
p			X			7
q			X			77

To Get This Triple Tap Keypad Function	First press these keys . . .					Then press this key
	Green	Orange	Blue	Shift	①	
r			X			777
s			X			7777
t			X			8
u			X			88
v			X			888
w			X			9
x			X			99
y			X			999
z			X			9999
A			X	X		2
B			X	X		22
C			X	X		222
D			X	X		3
E			X	X		33
F			X	X		333
G			X	X		4
H			X	X		44
I			X	X		444
J			X	X		5
K			X	X		55
L			X	X		555
M			X	X		6
N			X	X		66
O			X	X		666
P			X	X		7
Q			X	X		77
R			X	X		777
S			X	X		7777
T			X	X		8
U			X	X		88
V			X	X		888
W			X	X		9
X			X	X		99
Y			X	X		999
Z			X	X		9999
1						1
2			X			2 or 2222
3			X			3 or 3333
4			X			4 or 4444
5			X			5 or 5555
6			X			6 or 6666

To Get This Triple Tap Keypad Function	First press these keys . . .					Then press this key
	Green	**Orange**	**Blue**	**Shift**	①	
7			X			7 or 77777
8			X			8 or 8888
9			X			9 or 99999
0						0
. (period)		X				Tab
* (asterisk)			X			Tab
- (dash or minus sign)	X		X			Tab
/	X		X			0
' (single quote)	X		X			1
[	X		X			2
]	X		X			3
\	X		X			4
' (apostrophe)	X		X			5
, (comma)	X		X			6
` (accent)	X		X			7
; (semicolon)	X		X			8
= (equal sign)	X		X			9
!				X		1
@				X		2
#				X		3
$				X		4
%				X		5
^				X		6
&				X		7
* (asterisk)				X		8
(				X		9
)				X		0
" (double quote)	X	X				1
{	X	X				2
}	X	X				3
	(broken bar)	X	X				4
~ (tilde)	X	X				5
<	X	X				6
>	X	X				7
: (colon)	X	X				8
+ (plus sign)	X	X				9
?	X	X				0
_ (underscore)	X	X				TAB

Appendix B Technical Specifications

Physical Specifications

Features	Specifications	Comments		
CPU	Intel Xscale operating at 400 MHz	32 bit CPU (with on-chip cache)		
Memory	128MB SDRAM / 128MB flash			
Display	QVGA Transflective Color	Transflective LCD with touchscreen. LED backlight		
Mass Storage	SD Card	SD/MMC 1-bit interface		
PCMCIA Interface	None			
Weights	Unit with network card, standard battery and ring scanner	1 lb 0.5 oz	462 g	
	Battery, Standard Battery, Extended	4.1 oz 7.2 oz	116 g 205 g	
	Wireless Card – 2.4GHz Type II	0.5 oz	15 g	
	Ring Scanner Ring Imager	1.7 oz 1.8 oz	48 g 51 g	
External Connectors/Interface	Serial Port (COM2) (2) Tethered cable	Ring scanner. Max baud rate 230.4Kbps. Main Battery		
	Cradle Connection (COM1)	Asynchronous port. Max baud rate 230.4Kbps.		
	Bluetooth Connection (COM3)	Max baud rate 921.6Kbps.		
Audio/Microphone Connector	Tethered cable.	Audio / Battery / HX2 Cable		
HX2 Dimensions	Length	3.50 in	8.89 cm	
	Width	4.98 in	12.55 cm	
	Height	1.40 in	3.56 cm	
Scanner	No Scanner SE955 SR laser SE4400 2D Imager	Tethered.		

Features		Specifications	Comments
Batteries	Main	Li-Ion battery pack 7.2V.	Tethered. Voltage range 6.0-8.4VDC.
	Backup (CMOS)	Internal Nickel Cadmium (NiCd) 4.8V / 1.2V nominal.	Automatically charges from main battery during normal operation. Memory operational for 24 hours when main battery is depleted

Display Specifications

Feature	Specification
Type	QVGA – Transflective Active Color / LED Back Light
Resolution	320 horizontal x 240 vertical pixels
Size	One Quarter VGA portrait
Diagonal Viewing Area	2.5" (6.3 cm)
Active Area	1.47" x 1.97" (3.7 cm x 5 cm)
Color Scale	TFT display color depth of 64K

Environmental Specifications

Feature	Specification
Operating Temperature	14°F to 122°F (-10°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 60°C)
Water and Dust	IEC 60529 compliant to IP54
Operating Humidity	5% to 90% non-condensing at 104°F (40°C)
Standards	See *HX2 User's Guide, Appendix B*.
Contamination	Resistant to exposure to skin oil and other lubricants.
ESD	8 KV air, 4kV direct contact

Network Card Specifications

Summit Client 2.4GHz Type II

Bus Interface	Compact Flash adapter
Network Frequencies	2.4 - 2.4897 GHz IEEE 802.11b 802.11g DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	18 dBm 64mW Max
Channels	11 US, 13 Europe, 13 Japan
Operating Temperature	see HX2 Environmental Specs
Storage Temperature	see HX2 Environmental Specs
Connectivity	Novell, TCP/IP, Ethernet, ODI

Bluetooth

Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 ft (10 meters) line of sight
Bluetooth Version	2.0 + EDR

List of Valid VK Codes for CE 5

This is the list of codes parsed by KEYCOMP compiler. Refer to Microsoft Windows documentation for further clarification of the meaning of these key codes. Any VK keys not defined here are not valid for use under Windows CE 5.

VK_ADD	VK_F3	VK_NUMPAD9
VK_APOSTROPHE	VK_F4	VK_OEM_CLEAR
VK_APPS	VK_F5	VK_OFF
VK_ATTN	VK_F6	VK_PA1
VK_BACK	VK_F7	VK_PAUSE
VK_BACKQUOTE	VK_F8	VK_PERIOD
VK_BACKSLASH	VK_F9	VK_PLAY
VK_BROWSER_BACK	VK_FINAL	VK_PRINT
VK_BROWSER_FAVORITES	VK_HANGUL	VK_PRIOR
VK_BROWSER_FORWARD	VK_HANJA	VK_RBRACKET
VK_BROWSER_HOME	VK_HELP	VK_RBUTTON
VK_BROWSER_REFRESH	VK_HOME	VK_RCONTROL
VK_BROWSER_SEARCH	VK_HYPHEN	VK_RETURN
VK_BROWSER_STOP	VK_INSERT	VK_RIGHT
VK_CANCEL	VK_JUNJA	VK_RMENU
VK_CAPITAL	VK_KANA	VK_RSHIFT
VK_CLEAR	VK_KANJI	VK_RWIN
VK_COMMA	VK_LAUNCH_APP1	VK_SCROLL
VK_CONTROL	VK_LAUNCH_APP2	VK_SELECT
VK_CONVERT	VK_LAUNCH_MAIL	VK_SEMICOLON
VK_CRSEL	VK_LAUNCH_MEDIA_SELECT	VK_SEPARATOR
VK_DECIMAL	VK_LBRACKET	VK_SHIFT
VK_DELETE	VK_LBUTTON	VK_SLASH
VK_DIVIDE	VK_LCONTROL	VK_SLEEP
VK_DOWN	VK_LEFT	VK_SNAPSHOT
VK_END	VK_LMENU	VK_SPACE
VK_EQUAL	VK_LSHIFT	VK_SUBTRACT
VK_EREOF	VK_LWIN	VK_TAB
VK_ESCAPE	VK_MBUTTON	VK_UP
VK_EXECUTE	VK_MEDIA_NEXT_TRACK	VK_VOLUME_DOWN
VK_EXSEL	VK_MEDIA_PLAY_PAUSE	VK_VOLUME_MUTE
VK_F1	VK_MEDIA_PREV_TRACK	VK_VOLUME_UP
VK_F10	VK_MEDIA_STOP	VK_ZOOM
VK_F11	VK_MENU	
VK_F12	VK_MULTIPLY	
VK_F13	VK_NEXT	
VK_F14	VK_NOCONVERT	
VK_F15	VK_NONAME	
VK_F16	VK_NUMLOCK	
VK_F17	VK_NUMPAD0	
VK_F18	VK_NUMPAD1	
VK_F19	VK_NUMPAD2	
VK_F2	VK_NUMPAD3	
VK_F20	VK_NUMPAD4	
VK_F21	VK_NUMPAD5	
VK_F22	VK_NUMPAD6	
VK_F23	VK_NUMPAD7	
VK_F24	VK_NUMPAD8	

ASCII Control Codes

The following table lists ASCII Control codes in hexadecimal and their corresponding Control-key combinations.

Char	Hex	Control-Key	Control Action	
NUL	0	^@	NULl character	Ctrl-Shift-`
SOH	1	^A	Start Of Heading	VK_CONTROL (0x11) down VK_A (0x41) down WM_CHAR (0x1) VK_A (0x41) up VK_CONTROL (0x11) up
STX	2	^B	Start of TeXt	Ctrl-b
ETX	3	^C	End of TeXt	Ctrl-c
EOT	4	^D	End Of Transmission	Ctrl-d
ENQ	5	^E	ENQuiry	Ctrl-e
ACK	6	^F	ACKnowledge	Ctrl-f
BEL	7	^G	BELl, rings terminal bell	Ctrl-g
BS	8	^H	BackSpace (non-destructive)	Ctrl-h
HT	9	^I	Horizontal Tab (move to next tab position)	Ctrl-i
LF	a	^J	Line Feed	Ctrl-j
VT	b	^K	Vertical Tab	Ctrl-k
FF	c	^L	Form Feed	Ctrl-l
CR	d	^M	Carriage Return	Ctrl-m
SO	e	^N	Shift Out	Ctrl-n
SI	f	^O	Shift In	Ctrl-o
DLE	10	^P	Data Link Escape	Ctrl-p
DC1	11	^Q	Device Control 1, normally XON	Ctrl-q
DC2	12	^R	Device Control 2	Ctrl-r
DC3	13	^S	Device Control 3, normally XOFF	Ctrl-s
DC4	14	^T	Device Control 4	Ctrl-t
NAK	15	^U	Negative AcKnowledge	Ctrl-u
SYN	16	^V	SYNchronous idle	Ctrl-v
ETB	17	^W	End Transmission Block	Ctrl-w

Char	Hex	Control-Key	Control Action	
CAN	17	^X	CANcel line	Ctrl-x
EM	19	^Y	End of Medium	Ctrl-y
SUB	1a	^Z	SUBstitute	Ctrl-z
ESC	1b	^[	ESCape	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1b VK_PACKET up VK_CONTROL up
FS	1c	^\	File Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1c VK_PACKET up VK_CONTROL up
GS	1d	^]	Group Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1d down WM_CHAR (0x1d) up VK_PACKET up VK_CONTROL up
RS	1e	^^	Record Separator	VK_CONTROL (0x11)down VK_SHIFT (0x10) down WM_CHAR 0x36 down WM_CHAR 0x36 up VK_SHIFT up VK_CONTROL up
US	1f	^_	Unit Separator	VK_CONTROL (0x11) down VK_SHIFT (0x10) down VK_PACKET (0xe7) down WM_CHAR 0x1f VK_PACKET (0xe7) up VK_SHIFT (0x10) up VK_CONTROL (0x11) up

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded	Desired ASCII	Hex Value	Hat Encoded
NUL	0x00	^@	ESA	0x87	~^G
SOH	0x01	^A	HTS	0x88	~^H
STX	0x02	^B	HTJ	0x89	~^I
ETX	0x03	^C	VTS	0x8A	~^J
EOT	0x04	^D	PLD	0x8B	~^K
ENQ	0x05	^E	PLU	0x8C	~^L
ACK	0x06	^F	RI	0x8D	~^M
BEL	0x07	^G	SS2	0x8E	~^N
BS	0x08	^H	SS3	0x8F	~^O
HT	0x09	^I	DCS	0x90	~^P
LF	0x0A	^J	PU1	0x91	~^Q
VT	0x0B	^K	PU2	0x92	~^R
FF	0x0C	^L	STS	0x93	~^S
CR	0x0D	^M	CCH	0x94	~^T
SO	0x0E	^N	MW	0x95	~^U
SI	0x0F	^O	SPA	0x96	~^V
DLE	0x10	^P	EPA	0x97	~^W
DC1 (XON)	0x11	^Q		0x98	~^X
DC2	0x12	^R		0x99	~^Y
DC3 (XOFF)	0x13	^S		0x9A	~^Z
DC4	0x14	^T	CSI	0x9B	~^[
NAK	0x15	^U	ST	0x9C	~^\\
SYN	0x16	^V	OSC	0x9D	~^]
ETB	0x17	^W	PM	0x9E	~^^
CAN	0x18	^X	APC	0x9F	~^_ (Underscore)
EM	0x19	^Y	(no-break space)	0xA0	~ (Tilde and Space)
SUB	0x1A	^Z	¡	0xA1	~!
ESC	0x1B	^[	¢	0xA2	~"
FS	0x1C	^\\	£	0xA3	~#
GS	0x1D	^]	¤	0xA4	~$
RS	0x1E	^^	¥	0xA5	~%
US	0x1F	^_ (Underscore)	¦	0xA6	~&
	0x7F	^?			
	0x80	~^@	§	0xA7	~'
	0x81	~^A	¨	0xA8	~(
	0x82	~^B	©	0xA9	~)
	0x83	~^C	ª	0xAA	~*
IND	0x84	~^D	«	0xAB	~+
NEL	0x85	~^E	¬	0xAC	~,
SSA	0x86	~^F	(soft hyphen)	0xAD	~- (Dash)

Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded	Desired ASCII	Hex Value	Hat Encoded
®	0xAE	~. (Period)	×	0xD7	~W
¯	0xAF	~/	Ø	0xD8	~X
°	0xB0	~0 (Zero)	Ù	0xD9	~Y
±	0xB1	~1	Ú	0xDA	~Z
²	0xB2	~2	Û	0xDB	~[
³	0xB3	~3	Ü	0xDC	~\\
´	0xB4	~4	Ý	0xDD	~]
µ	0xB5	~5	Þ	0xDE	~\^
¶	0xB6	~6	ß	0xDF	~_ (Underscore)
·	0xB7	~7	à	0xE0	~`
¸	0xB8	~8	á	0xE1	~a
¹	0xB9	~9	â	0xE2	~b
º	0xBA	~:	ã	0xE3	~c
»	0xBB	~;	ä	0xE4	~d
¼	0xBC	~<	å	0xE5	~e
½	0xBD	~=	æ	0xE6	~f
¾	0xBE	~>	ç	0xE7	~g
¿	0xBF	~?	è	0xE8	~h
À	0xC0	~@	é	0xE9	~i
Á	0xC1	~A	ê	0xEA	~j
Â	0xC2	~B	ë	0xEB	~k
Ã	0xC3	~C	ì	0xEC	~l
Ä	0xC4	~D	í	0xED	~m
Å	0xC5	~E	î	0xEE	~n
Æ	0xC6	~F	ï	0xEF	~o
Ç	0xC7	~G	ð	0xF0	~p
È	0xC8	~H	ñ	0xF1	~q
É	0xC9	~I	ò	0xF2	~r
Ê	0xCA	~J	ó	0xF3	~s
Ë	0xCB	~K	ô	0xF4	~t
Ì	0xCC	~L	õ	0xF5	~u
Í	0xCD	~M	ö	0xF6	~v
Î	0xCE	~N	÷	0xF7	~w
Ï	0xCF	~O	ø	0xF8	~x
Ð	0xD0	~P	ù	0xF9	~y
Ñ	0xD1	~Q	ú	0xFA	~z
Ò	0xD2	~R	û	0xFB	~{
Ó	0xD3	~S	ü	0xFC	~|
Ô	0xD4	~T	ý	0xFD	~}
Õ	0xD5	~U	þ	0xFE	~~
Ö	0xD6	~V	ÿ	0xFF	~^?

Hat Encoded Characters Hex AE through FF

Decimal – Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42[7]	0x2A	82	0x52	122	0x7A
3	0x03	43	0x2B	83	0x53	123	0x7B
4	0x04	44	0x2C	84	0x54	124	0x7C
5	0x05	45	0x2D	85	0x55	125	0x7D
6	0x06	46	0x2E	86	0x56	126	0x7E
7	0x07	47	0x2F	87	0x57	127	0x7F
8	0x08	48	0x30	88	0x58	128	0x80
9	0x09	49	0x31	89	0x59	129	0x81
10	0x0A	50	0x32	90	0x5A	130	0x82
11	0x0B	51	0x33	91	0x5B	131	0x83
12	0x0C	52	0x34	92	0x5C	132	0x84
13	0x0D	53	0x35	93	0x5D	133	0x85
14	0x0E	54	0x36	94	0x5E	134	0x86
15	0x0F	55	0x37	95	0x5F	135	0x87
16	0x10	56	0x38	96	0x60	136	0x88
17	0x11	57	0x39	97	0x61	137	0x89
18	0x12	58	0x3A	98	0x62	138	0x8A
19	0x13	59	0x3B	99	0x63	139	0x8B
20	0x14	60	0x3C	100	0x64	140	0x8C
21	0x15	61	0x3D	101	0x65	141	0x8D
22	0x16	62	0x3E	102	0x66	142	0x8E
23	0x17	63	0x3F	103	0x67	143	0x8F
24	0x18	64	0x40	104	0x68	144	0x90
25	0x19	65	0x41	105	0x69	145	0x91
26	0x1A	66	0x42	106	0x6A	146	0x92
27	0x1B	67	0x43	107	0x6B	147	0x93
28	0x1C	68	0x44	108	0x6C	148	0x94
29	0x1D	69	0x45	109	0x6D	149	0x95
30	0x1E	70	0x46	110	0x6E	150	0x96
31	0x1F	71	0x47	111	0x6F	151	0x97
32	0x20	72	0x48	112	0x70	152	0x98
33	0x21	73	0x49	113	0x71	153	0x99
34	0x22	74	0x4A	114	0x72	154	0x9A
35	0x23	75	0x4B	115	0x73	155	0x9B
36	0x24	76	0x4C	116	0x74	156	0x9C
37	0x25	77	0x4D	117	0x75	157	0x9D
38	0x26	78	0x4E	118	0x76	158	0x9E
39	0x27	79	0x4F	119	0x77	159	0x9F

Decimal – Hexadecimal Chart (0 to 159 Decimal)

---

[7] The answer to Life, the Universe and Everything.

160	0xA0	200	0xC8	240	0xF0
161	0xA1	201	0xC9	241	0xF1
162	0xA2	202	0xCA	242	0xF2
163	0xA3	203	0xCB	243	0xF3
164	0xA4	204	0xCC	244	0xF4
165	0xA5	205	0xCD	245	0xF5
166	0xA6	206	0xCE	246	0xF6
167	0xA7	207	0xCF	247	0xF7
168	0xA8	208	0xD0	248	0xF8
169	0xA9	209	0xD1	249	0xF9
170	0xAA	210	0xD2	250	0xFA
171	0xAB	211	0xD3	251	0xFB
172	0xAC	212	0xD4	252	0xFC
173	0xAD	213	0xD5	253	0xFD
174	0xAE	214	0xD6	254	0xFE
175	0xAF	215	0xD7	255	0xFF
176	0xB0	216	0xD8		
177	0xB1	217	0xD9		
178	0xB2	218	0xDA		
179	0xB3	219	0xDB		
180	0xB4	220	0xDC		
181	0xB5	221	0xDD		
182	0xB6	222	0xDE		
183	0xB7	223	0xDF		
184	0xB8	224	0xE0		
185	0xB9	225	0xE1		
186	0xBA	226	0xE2		
187	0xBB	227	0xE3		
188	0xBC	228	0xE4		
189	0xBD	229	0xE5		
190	0xBE	230	0xE6		
191	0xBF	231	0xE7		
192	0xC0	232	0xE8		
193	0xC1	233	0xE9		
194	0xC2	234	0xEA		
195	0xC3	235	0xEB		
196	0xC4	236	0xEC		
197	0xC5	237	0xED		
198	0xC6	238	0xEE		
199	0xC7	239	0xEF		

Decimal – Hexadecimal Chart (160 to 255 Decimal)

Index

C

D

T

U

V

W