MX3X Reference Guide

(Microsoft® Windows® CE .NET Equipped)

Copyright © November 2005 by LXE Inc.
All Rights Reserved
E-EQ-MX3XRG-E

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 manual is copyrighted. All rights 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 © 2005 by LXE Inc. An EMS Technologies Company.
125 Technology Parkway, Norcross, GA 30092 U.S.A. (770) 447-4224

Trademarks:

LXE® is a registered trademark of LXE Inc. Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries. 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. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations. When this guide is in PDF format: "Acrobat ® Reader Copyright © 1987-2005 Adobe Systems Incorporated. All rights reserved. Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated." Applies.

Initial Release June 2004, Revision B Released August 2004, Revision C Released December 2004, Revision D Released April 2005, Revision E Released November 2005.

Li-Ion Battery

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

Revision Notice

Chaper 1 – Introduction	Added Scanner Clip Strap (85XX scanners only) to "Accessories." Deleted obsolete tethered scanners.
Chapter 4 – System Configuration	Updated Date/Time figure and instruction to explain Sync button function. Updated "LAUNCH.EXE" in section titled "Utilities". Added "2.4GHz Radio Configuration" section and "Configuring IPv6 Broadcast Messages." Removed "Cisco – Aironet Configuration Utility (ACU)" and "Symbol" sections. This information is now included in Chapter 7.
Chapter 7 – Wireless Network Configuration	Added new chapter containing ACU and Symbol sections removed from Chapter 4. Added MX3X WPA information and instruction.

Table of Contents

Illustrations

Chapter 1 Introduction

Overview

The LXE MX3X is a rugged, portable, hand-held Microsoft® Windows® CE .NET equipped mobile computer capable of wireless data communications. The mobile device can transmit information using a 2.4 GHz radio (with an internally mounted antenna) and it can store information for later transmission through an RS-232, InfraRed, or USB port.

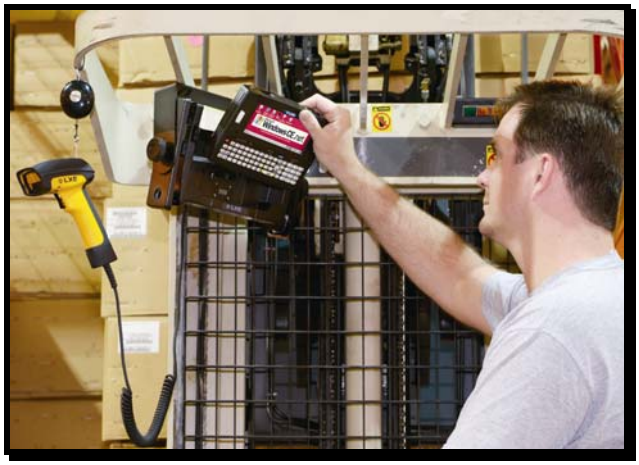
The mobile device is horizontally oriented and features backlighting for the display. The touch-screen display supports graphic features and Windows icons that the Windows CE .NET operating system supports. The keys on the keypad are constructed of a phosphorescent material that can easily be seen in dimly lighted areas.

Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

The MX3-RFID version of the MX3X has an RFID module permanently attached to the back of the device. If there is no distinction between directions for the user with an MX3X and a user with a MX3-RFID mobile device, the instruction or information in this guide is the same for both versions unless noted.

This device is a Windows CE .NET compatible computer that can be scaled from a limited function batch computer to an integrated RF scanning computer.

The stylus in the Stylus Kit (shipped with unit) is used to assist in entering data and configuring the unit. Protective film for the touchscreen is available as an accessory.



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

Related Manuals

The "MX3X User's Guide" contains mobile device installation, user instruction and safety statements.

Please refer to the "MX3 Cradle Reference Guide" for technical information relating to the MX3X-compatible Desk Top and Vehicle Mount cradles.

If you need to set up the integrated SE923 scanner barcode reading parameters, please refer to the "Integrated Scanner Programming Guide" on the LXE Manuals CD or the LXE website www.lxe.com.

Note: Always store unused mobile devices with a fully charged main battery installed. LXE recommends an in-use mobile device be frequently connected to an external power source to retain optimum power levels in the main battery and the backup battery. When the backup battery and main battery are dead, the mobile device reverts to it's default values when a fully charged main battery is installed and the device is powered On again.

Components

Front and Back Views

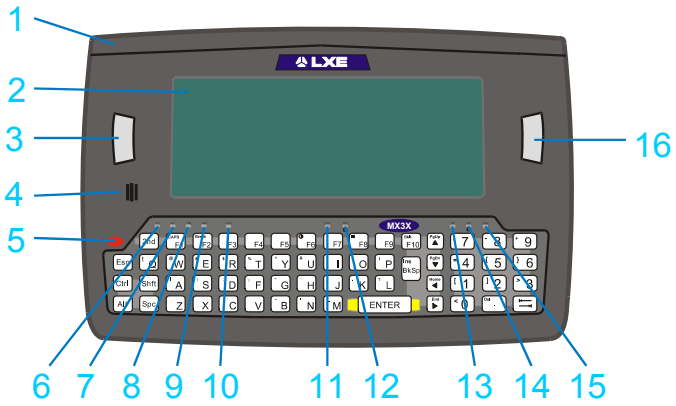


Figure 1-1 Front

1	Endcap	9	Shift LED
2	Display	10	Caps LED
3	Scan, Enter or Field Exit (programmable)	11	Scanner LED
4	Beeper	12	Backup Battery LED
5	On/Off Button	13	Status LED
6	2nd LED	14	Main Battery LED
7	Alt LED	15	Charger LED
8	Ctrl LED	16	Scan or Enter (programmable)

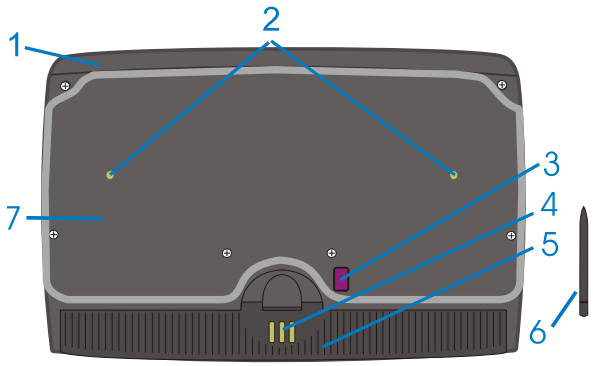


Figure 1-2 Back

1	Endcap	5	Main Battery
2	Leather Handstrap Connector (N/A on RFID Module)	6	Stylus
3	IR Port (Com 2 Port)	7	RFID Module (MX3-RFID device only)
4	Cradle Input Contacts		

Endcap Options

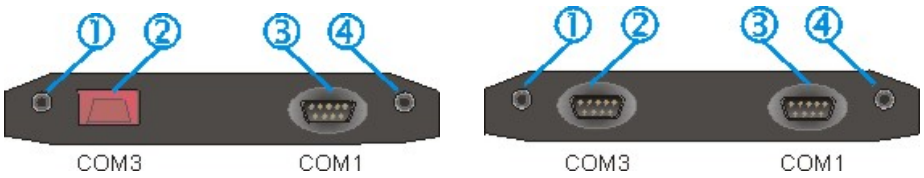


Figure 1-3 Endcaps

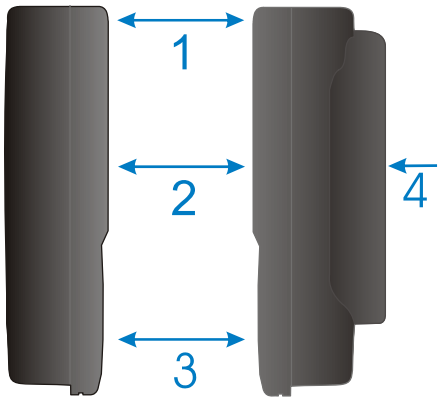
1	DC Power Jack	3	Serial Com 1 or USB Client Port
2	Serial Com 3 or USB Host or Scanner Port	4	Audio Jack

MX3X	
Left Port	**Right Port**
Serial COM3	Serial COM1
Serial COM3	USB Client
USB Host	Serial COM1
USB Host	USB Client
Scanner	Serial COM1
Scanner	USB Client

MX3-RFID	
Left Port	**Right Port**
Scanner	USB Client

See “Chapter 2 Physical Description and Layout”, section titled “Endcaps” for further information.

MX3-RFID Module



1 Endcap w/Laser Scanner

2 Touchscreen

3 Keypad

4 RFID Module

Figure 1-4 Side View

When to Use This Guide

As the reference for LXE's MX3X / MX3-RFID 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 device and it's capabillities, 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.

Instruction and safety information for the general user are contained in the "MX3X User's Guide."

This chapter, **"Introduction",** describes this reference guide's structure, contains setup and installation instruction, briefly describes data entry processes, and explains how to get help.

Chapter 2 "Physical Description and Layout", describes the function and layout of the configuration, controls and connectors.

Chapter 3 "Power Supply" describes the power sources and battery charging stations.

Chapter 4 "System Configuration" takes you through the system setup and file structure.

Chapter 5 "MX3-RFID" describes the function, layout and system setup for an MX3X with an RFID module.

Chapter 6 "AppLock" contains explanation and instruction when working with mobile devices running AppLock.

Chapter 7 "Wireless Network Configuration" details 2.4GHz radio setup. Configuration for WEP and WPA is included.

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

Appendix B "Technical Specifications" lists technical and environmental specifications for the mobile device.

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 guide uses the convention "choose File | Save".
"Quotes"	Indicates the title of a book, chapter or a section within a chapter (for example, "Document Conventions").
< >	Indicates a key on the keypad (for example, <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

Important

If the mobile device has AppLock installed, please refer to "Chapter 6 – AppLock" for setup and processing information before continuing with "Getting Started."

Note: When your mobile device is pre-configured, the radio, PCMCIA card and endcaps are assembled by LXE to your specifications.

This section's instructions are based on the assumption that your new system is pre-configured and requires only accessory installation (e.g. handstrap, stylus) and a power source. 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.

Use this guide as you would any other source book – reading portions to learn about the device, and then referring to it when you need more information about a particular subject. This guide takes you through an introduction to and operation of the MX3X with and without the RFID module.

In general, the sequence of events is:

1. Insert a fully charged battery and press the Power button.
2. Connect an external power source to the unit (if required).
3. If the screen does not automatically display, press the Power button.
4. Adjust screen display, audio volume and other parameters if desired.

Troubleshooting

Can't align the screen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts access to the control panels. Contact your System Administrator. See Also: Chapter 6 "AppLock".

Insert Main Battery

Press the Power button after the battery is inserted into the battery compartment.

Note: ***New batteries must be charged prior to first use****. This process takes up to four hours in an LXE Multi-Charger Plus and eight hours with an external power source attached to the mobile device.*

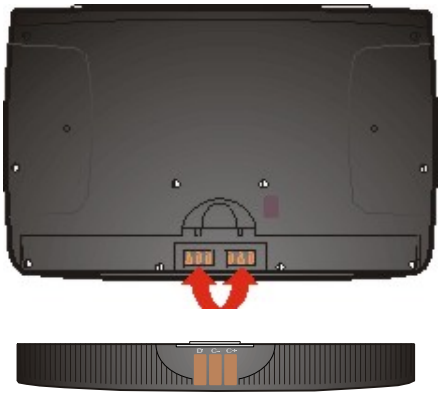


Figure 1-5 Battery Contacts and Main Battery

The Main Battery compartment is located at the bottom of the back of the computer. The arrows in the figure titled "Battery Contacts" point to the battery contacts in the computer. The figure titled "Main Battery" show the cradle and charger contacts on the back of the main battery.

Place the battery in the compartment, making sure the side of the battery with six contacts matches up with the battery contacts in the computer battery compartment. Do not slide the battery sideways into the compartment.

Firmly press the battery into the compartment until the Retaining Clip on the battery clicks. The battery is now securely fastened to the computer. The computer draws power from the battery immediately upon successful connection.

Check Battery Status

Tap the **Start | Settings | Control Panel | Power** icon. Main and backup battery level, status and Power Scheme timeout setting options are displayed.

About Lithium-Ion Batteries

Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the mobile device is always 'on' even when in the Suspend state and draws battery power at all times. Use the **Start | Settings | Control Panel | Power | Battery** tab to check the battery status and power reading.

Always replace the used main battery with a fully charged main battery. The Battery Low Warning LED illuminates red at approximately 35% of power left in the main battery. You need to determine the point at which battery life becomes unacceptable for your business practices and replace the main battery before that point.

Refer to the documentation received with the battery charger for complete information.

Attach Handstrap (Optional)

Note: These instructions are not to be used for the MX3-RFID.

Once installed, the elastic handstrap provides a means for the user to secure the computer to their hand. It is adjustable to fit practically any size hand and does not interfere with battery charging when the MX3X is in a cradle.

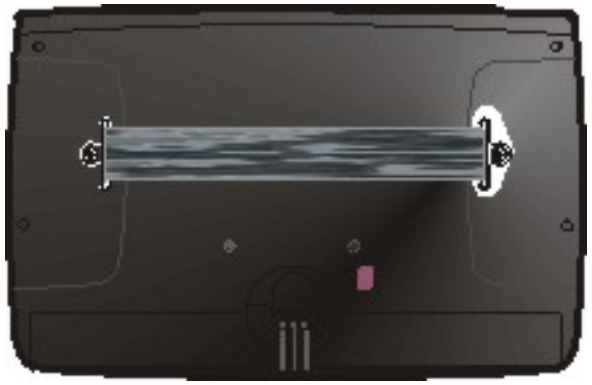


Figure 1-6 MX3X With Handstrap Installed

Tool Required: #1 Phillips Screwdriver

Installation

1. Place the MX3X, with the screen facing down, on a flat stable surface.
2. Attach the handstrap to the MX3X with the screws and washers provided.
3. Test the strap's connection making sure the MX3X is securely connected to each end of the strap connectors.

Attach the Stylus Clip (Optional)

Carefully remove the paper backing from the Stylus Clip sticky. Firmly press the sticky side of the clip onto the mobile device and hold in place for 15 seconds. Thread the tether through the end of the stylus and tie the ends firmly to the Stylus Clip so that the ends don't interfere with placing the stylus in the Stylus Clip. Place the stylus in the Stylus Clip when not in use.

An extra or replacement stylus can be ordered from LXE. See the section titled "Accessories" for the stylus part number.

Attach to Hip-Flip (Optional)

Note: The MX3-RFID device does not fit the Hip-Flip accessory. ***The Hip-Flip is not to be used with the MX3-RFID device.***

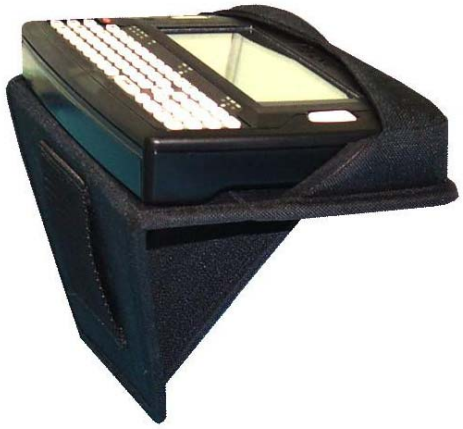


Figure 1-7 Hip-Flip Accessory

Note: #1 flat head screwdriver is not supplied by LXE. A waist belt accessory can be ordered from LXE.

Once the MX3X is attached to the hip-flip and the hip-flip securely fastened to the user by a belt around their waist, the MX3X can be operated at a convenient height, leaving the user's hands free.

The hip-flip adjusts downward to allow removing and replacing the main battery without removing the unit from the hip-flip or the user's body.

The MX3X must be removed from the hip-flip before being placed in a docking station.

Caution: Never use the MX3X in the hip-flip without first securing the device to the hip-flip with the screws.

Installation

1. If the MX3X has a handstrap, remove the handstrap and set it aside along with the handstrap screws and washers.
2. Slide the MX3X into the pocket in the hip-flip, making sure the keypad is up and the endcap ports are visible in the openings at the base of the hip-flip.
3. Place the MX3X (in the hip-flip) on a flat stable surface with the keypad down.
4. Tighten the assembly with the black screws provided, using the holes used for the handstrap (if used) on the back of the MX3X.
5. Test the hip-flip's connection making sure the MX3X is securely attached.
6. Slide the waist-belt through the loop in the hip-flip and secure the belt around your body.

Connect External Power Supply (Optional)

There are three external power supplies available for the mobile device and the MX3 desktop cradle:

- US AC/DC 12V Power Supply
- Cigarette Lighter Adapter
- International AC/DC 12V Power Supply

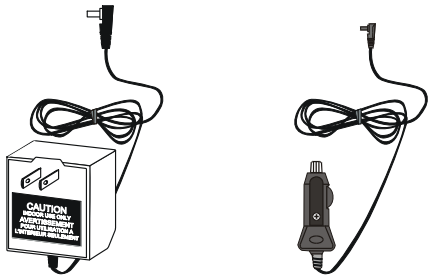


Figure 1-8 US AC/DC 12V Power Supply and Automotive Power Adapter

Figure 1-9 International AC/DC 12V Power Supply

The DC power jack is located on the endcap. The cradle power jack is located on the back of the cradle.

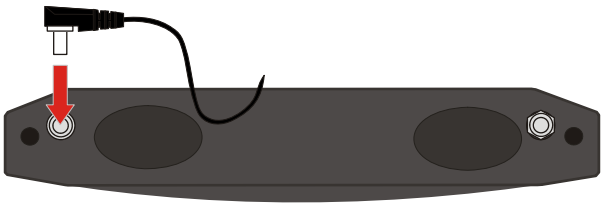


Figure 1-10 Connect External Power Supply

1. Insert the barrel connector into the power jack on the endcap and push in firmly.

2. The CHGR LED above the keypad illuminates when the computer is receiving external power through the power jack.

Note: When the mobile device is receiving external power through a powered cradle, the cradle's Status LED and the mobile device's CHGR LED are illuminated.

See section titled "LED Functions" for explanations of the LEDs for the BATT B and BATT M illuminations.

Connect Audio Jack (Optional)

The audio jack is located on the endcap.

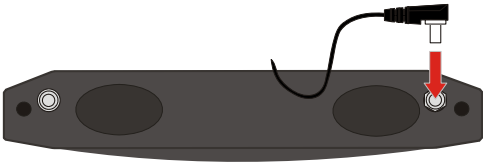


Figure 1-11 Connect Audio Jack

Insert the 2.5mm barrel end of the connector into the audio jack on the endcap and push the connector in firmly. See section titled “Set the Audio Speaker Volume”.

Note: The audio option draws power from the battery.

Power Button

Note: Refer to the section titled “Power Modes” later in this chapter for information relating to the power states of the mobile device.

Figure 1-12 Power Button

The power button is located above the ESC key on the keypad. When a battery is inserted in the mobile device press the Power button.

Quickly tapping the Power button places the device immediately in Suspend mode. Quickly tapping the Power button again, or touching the screen, immediately returns the device from Suspend.

When the Windows desktop is displayed or an application begins, the power up (or reboot) sequence is complete.

Please refer to the section titled “Power Modes” later in this guide for a list of the kinds of activities (Primary Events) that will return the device from Suspend Mode.

Restart Sequence

Tap **Start | Run,** then type **`warmboot`** in the textbox and p**ress Enter**. If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

When the Windows CE. NET desktop is displayed or an application begins, the power up (or restart) sequence is complete. If you have previously saved your settings, they will be restored on reboot.

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 object to write on the touchscreen.

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.

Like 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 integrated barcode scanner or an input/output device connected to the serial port.

An extra or replacement stylus can be ordered from LXE. See the section titled “Accessories” for the stylus part number.

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

- Press Tab and an Arrow key to select a file.
- Press Shift and an Arrow key to select several files.
- Once you’ve selected a file, press Alt then press Enter to open its Properties dialog.
- Press 2nd then press numeric dot to delete a file.
- To force the Start menu to display, press Ctrl then press Esc.

Touchscreen Calibration

If the touchscreen is not responding properly to pen touch 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.

If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

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

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

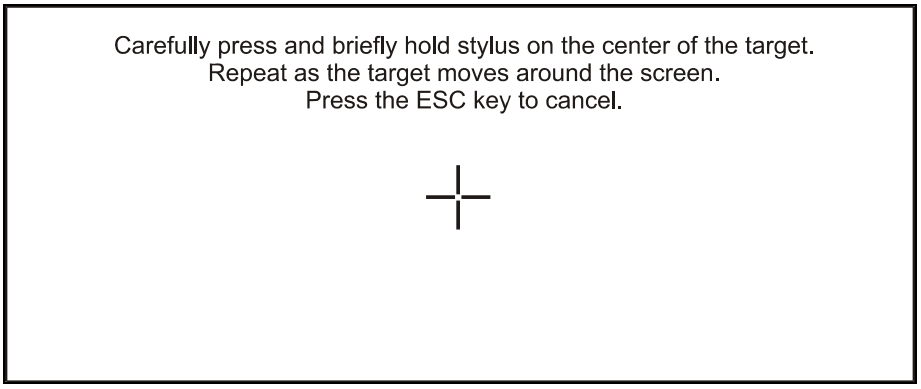


Figure 1-13 Touchscreen Recalibration

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

Set The Display Contrast

Adjusting screen contrast lightens or darkens the characters to make them visible at a comfortable level. The contrast is incremented or decremented one step each time the contrast key is pressed.

◐ To adjust screen contrast, locate the <F6> key at the top of the keypad. Adjust the display contrast by pressing the:

- 2nd key then the <F6> key
- Use the Up Arrow and Down Arrow keys to adjust contrast until the display lightens or darkens to your satisfaction.
- Press the Enter key to exit this mode.

The LED for the 2nd key blinks until the special editing mode (set contrast) is complete.

Set the Display Backlight Timer

Note: Refer to the section titled "Power Modes" later in this guide for information relating to the power states of the mobile device.

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

The first option affects the mobile device when it is running on battery power only. The second option affects the device when it is running on external power (e.g. AC adapter, cigarette adapter, 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 backlight will remain on all the time when both checkboxes are blank.**

The transmissive color display backlight timer *dims the backlight* at the end of the specified time. The transflective monochrome display backlight timer *turns the backlight off* at the end of the specified time.

Set The Display Brightness

The brightness adjustment feature depends on the display type, color versus monochrome. Adjusting screen brightness lightens or darkens the background to make characters visible at a comfortable level. The brightness on a color display is incremented or decremented one step each time the arrow key is pressed until either the maximum or minimum brightness is achieved (8 steps). The brightness setting is recalled at power up.

Color – To adjust MX3X and MX3-RFID screen brightness, locate the <F10> key at the top of the keypad. Adjust the display brightness by pressing the:

- 2nd key then the <F10> key
- Use the Up Arrow and Down Arrow keys to adjust brightness until the display lightens or darkens to your satisfaction.
- Press the Enter key to exit this mode.

Monochrome – MX3X only. The 2nd key + F10 key sequence toggles the backlight from it's brightest (On) to it's dimmest (Off) readable settings.

The LED for the 2nd key blinks until the special editing mode (set display brightness) is complete.

Set the Power Schemes Timers

Note: Refer to the section titled "Power Modes" later in this guide for information relating to the power states of the mobile device.

Select **Start | Settings | Control Panel | Power | Schemes** tab. Change the parameter values and tap OK to save the changes.

Battery Power Scheme

Use this option when the 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 device will be running on external power (e.g. AC adapter, cigarette adapter, 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

These 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.

Set 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 speaker is located on the front of the device above the Power button. The audio volume can be adjusted to a comfortable level for the user. The volume is increased or decreased one step each time the volume key is pressed. The device has an internal speaker and a jack for an external headset. Operational "beeps" are emitted from the speaker.

Using the Keypad

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

◄ To adjust speaker volume, locate the <F8> key at the top of the keypad. Adjust the speaker volume by pressing the:

- 2nd key then the <F8> key to enter Volume change mode.
- Use the Up Arrow and Down Arrow keys to adjust volume until the speaker volume is satisfactory.
- Press the Enter key to exit this mode.

The LED for the 2nd key blinks until the special editing mode (set audio speaker volume) is complete.

Using the Touchscreen

Select **Start | Settings | Control Panel | Volume & Sounds | Volume** tab. Change the volume setting and tap OK to save the change. 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.

Setup the Radio and Network

Prerequisites

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

See “Chapter 7 Wireless Network Configuration” for complete information.

Access the 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), make sure your mobile client is communicating with the Access Point.
2. From the **Start | 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.

Installing PCMCIA and CF Cards

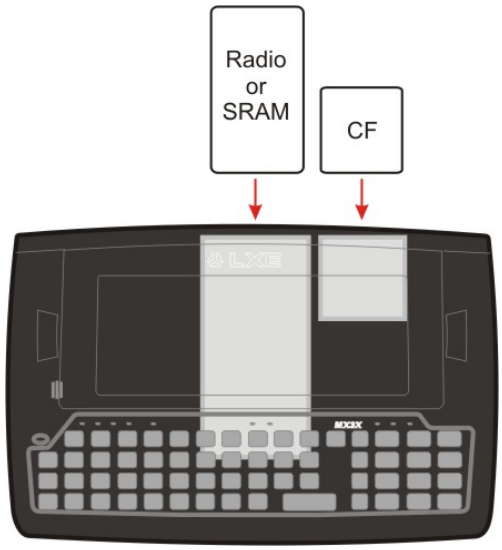


Figure 1-14 PCMCIA and CF Card Location

There is one PC card slot (Slot 0) and one Compact Flash card slot (Slot 1) located under the endcap. Slot 0 powers a radio PC card, PC SRAM card, ATA Flash card or a linear Flash card. The slots hold only one card at a time. Slot 0 supplies .75 of an amp at 5V or 3.3V.

The second slot (Slot 1) is designed to support a Type I or II Compact Flash disk.

See "Chapter 2 Physical Description and Layout", section titled "PCMCIA Cards" for further information.

Installing / Removing Cards

Preparation

Requirement: A screwdriver (not supplied by LXE)

- LXE recommends that installation or removal of the card be performed on a clean, well-lit surface.
- Using a screwdriver, remove or loosen the screws on the endcap.
- Carefully slide the endcap to the side, taking care not to dislodge or disconnect any cables.
- Remove or loosen all cables to the card(s) to be removed/replaced. If a radio card, disconnect the radio antenna from the radio card.

Installation

1. Slide the card, connector side first, into the slot until it seats. Use caution not to pull or snag the antenna connector.
2. If the card is difficult to seat in the slot, remove the card, turn it around and re-install.
   - The radio antenna connector must be positioned up and toward the front of the device (near the display).

- Gently snap the antenna cables into the connectors on the radio card. Use caution not to damage either the antenna cable connectors or the connectors on the radio. Connect **all** antenna cables to the PCMCIA radio card.

3. Replace the endcap, making sure all connections are secure and ribbons/antennas are not crimped between the endcap and the body of the mobile device.

Removal

1. Grasp the top of the card and pull it straight upward to remove.
2. Use caution not to pull or snag the antenna connector on the Radio card, if installed.

If you anticipate keeping the PCMCIA or CF card out of the mobile device for a long period of time place it in an enclosed electrostatic-protected storage container. Store in an area that is protected from dirt, moisture, and electrostatic contact.

Enter Data

You can enter data into the mobile device through several different methods. The Scanner window accepts barcode data entry, the RS-232 and the IR port are used to input/output data, and the keypad and stylus provide manual entry.

The RFID module can either read or read and write tag data. See Chapter 5 “MX3-RFID” for instruction.

Keypad Entry

The keypad is used to manually input data that is not collected otherwise. Almost any function that a full sized computer keyboard can provide is duplicated on the mobile device’s keypad but it may take a few more keystrokes to accomplish a keyed task.

Almost every key has two or three different functions. The primary alpha or numeric character is printed on the key.

For example, when the 2nd key is pressed, the 2nd key LED illuminates. By then pressing the desired second-function key the device will then produce the 2nd character. The specific 2nd character is printed above the corresponding key. The 2nd key LED turns off when key sequence finishes (unless when setting volume or contrast – the 2nd key LED will flash at those times).

Please refer to “Appendix A – Key Maps” for instruction on the specific keypresses to access all keypad functions.

Stylus Entry

The stylus performs the same function as a 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. Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp object to write on the touchscreen.

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 touchscreen responds to an actuation force (touch) of 4 oz. (or greater) of pressure.

The stylus can be used in conjunction with the keyboard and scanner and an input/output device connected to one of the serial ports.

- 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 unit is ready to accept data from either the keyboard, integrated scanner or a scanner connected to the serial port, if the scanner applet is configured correctly.

Input Panel

The Input Panel icon looks like a keyboard and is shown in the System tray. To show or hide the input panel, tap the Input Panel icon. Use the input panel to enter information in any program.

Integrated Laser Scanner Data Entry

Read all cautions, warnings and labels **before** using the laser scanner.

To scan with the integrated laser barcode reader, point the laser window towards a barcode and press the Scan button. You will see a red laser beam strike the barcode. The laser scanner has an SE923 scan engine.

Figure 1-15 Scan Beam

Align the red beam so that the barcode is centered within the beam. The laser beam must cross the entire barcode. Move the mobile device towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.

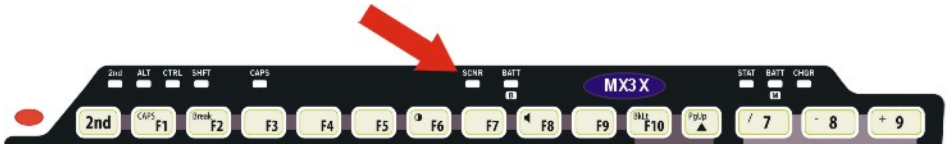


Figure 1-16 Scanner LED Location

The SCNR LED turns red when the laser beam is on. Following a barcode scan and read the SCNR LED turns green and the mobile device beeps, indicating a successful scan.

The laser and SCNR LED automatically turn off after a successful or unsuccessful read. The scanner is ready to scan again when the Scan key is pressed.

Large barcodes can be scanned at the maximum distance. Hold the scanner closer to small barcodes (or with bars that are very close together).

When the scan is successful, the Scan LED turns green, then switches off, and the mobile device emits a distinctive audible tone.

When the scan is unsuccessful, the SCNR LED remains red until the 3 second timeout (default) occurs or the Scan key is released. The mobile device emits distinctive audible tones. Check the following:

- Check the barcode for marks or physical damage e.g. ripped label, missing section, etc.
- Try scanning test symbols of the same code type at different distances and angles.
- Is the scan aperture unscratched and unsoiled?

See the “Integrated Scanner Programming Guide” for barcode samples, default scanning ranges, barcode reading instruction and troubleshooting.

Tethered Scanner

*Do **not** connect a tethered scanner cable to a USB-C or USB-H labeled endcap port. The USB ports cannot power a tethered scanner*.

Tethered scanners connect to RS232-labeled ports on the endcap and, *for the MX3X only*, can connect to the RS232 port on a powered cradle.

The Scan buttons have no effect on tethered barcode scanners (connected to the RS232 labelled serial port). Tethered scanners read barcode scans only when the trigger on the tethered scanner is pressed. The tethered scanner requires power on pin 9 of the RS232 serial port.

To set the mobile device to use a tethered scanner, select **Start | Settings | Control Panel | Scanner | COM1 (or 2 or 3)**.

Tap the "**Power on Pin 9 (+5V)**" checkbox for the COM port selected. The COM port that accepts the scanner data can be configured for data rate, parity, stop bits and data bits.

See Also: Section titled "Tethered Scanner and Cradles" when using a tethered scanner with a cradle.

RFID Tag Data Collection

When the RFID Read button is pressed, the reader turns on and the MX3-RFID beeps once if the tag was located and read successfully. The reader turns off at a predetermined time limit after a good read or a failed read.

There may be a buzz sound during the time the reader is "searching and reading" if the RFID reader is configured to buzz during a read cycle.

See Chapter 5 "MX3-RFID".

ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the radio link, serial port, USB or the infrared port on the mobile device.

*Note: ActiveSync **does not transmit through the IR port in MX3 vehicle cradles**. It will through the IR port of specific MX3X desktop cradles. Please refer to section titled "Accessories" for the part identified as the Desktop Cradle for the MX3X.*

Requirement: ActiveSync version 3.7 (or higher) must be resident on the host (desktop/laptop) computer. ActiveSync is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync on your desktop computer.

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your desktop computer with the mobile device and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

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

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

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

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The following instructions relate to the initial setup of ActiveSync. When there is a Connect icon on the desktop, this section can be bypassed.

The partnerships can only be created using direct serial or USB cable connection. After the partnerships are established, ActiveSync communication can be initiated using serial, USB, IrDa and radio. See section titled "Connect and Communicate" for cable/port compatibility.

Serial Connection

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

Serial 1 @ 57600

Note: The default is 57600 baud.

This will set up the mobile device to use COM 1. If the device has a dual-serial port endcap, the Serial 3 @ 57600 can also be selected. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel.

Select Scanner and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

USB Connection

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

USB "Client"

This will set up the mobile device to use the USB port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel.

IMPORTANT – DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

The MX3-RFID requires USB connection for ActiveSync. There is no ActiveSync connection through the MX3-RFID passive cradle.

Radio

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using direct serial / USB cable connection.

Once the relationship is established using the serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is radio.

Select **Start | Settings | Programs | Communication | ActiveSync**. From the popup list, choose Network and then tap the Connect button.

IrDA Connection

Note: The ActiveSync connection does true IrDA, not serial over IR, or TCP/IP (Winsock) over IR, like many infrared connections. Therefore, it is important to use a PC infrared interface which supports the handshaking needed for ActiveSync. This, unfortunately, precludes using many brands of laptops, which only use a simple infrared interface, even though they may call it IrDA.

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

IR @ 115200

This will set up the mobile device to use the Infrared port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel.

Select Scanner and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

To initiate synchronization from your device, tap **Start | Programs | Communication | ActiveSync** to begin the process.

Tap Sync to connect and synchronize. View synchronization status.

Tap Tools to synchronize or change synchronization settings. View connection status.

Tap Stop to stop synchronization.

Tap **Start | Help** for context-sensitive help.

Connect and Communicate

Connect the correct** cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the client (**Start | Programs | Communications | Connect**).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB will start automatically when the USB cable is connected, not requiring you to select "Connect" from the start menu.

** Cables for initial ActiveSync Configuration:

USB Client to PC/Laptop	USB-Client cable	MX3XA069CBLD9USBCLNT
Serial Client to PC/Laptop	RS-232 9 Pin to 9 Pin	9000A054CBL6D9D9

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows CE .NET image. This, however, includes most of the files in the \Windows folder).

Copy the MX3X LXEbook to the MX3X (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 Website. See the full format User Guides"MX3X User's Guide" on LXE Manuals CD.

Mobile Device	Required Adobe Acrobat Reader Version
MX3X / MX3-RFID	Windows CE. NET PDF Viewer (pre-installed by LXE).

First, using your desktop computer download "LXEbook – MX3X Users Guide" from the LXE Manuals CD to your desktop computer.

Next, connect the mobile device to your desktop computer and run ActiveSync.

When the mobile device and the desktop ActiveSync applications are synchronized, click Explore on the ActiveSync menu on your desktop to display the contents of the mobile device folders.

Then, open the folder on your desktop computer containing the downloaded LXEbook User's Guide. Click and drag the LXEbook User Guide to the My Documents folder on the mobile device.

When the file copy process is finished, disconnect the mobile device from the synchronization equipment and close ActiveSync.

To view the LXEbook on the mobile device, select Start / Programs / Adobe Reader / File / Open. Locate the LXEbook on the mobile device and "open" the file.

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

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established. See section "ActiveSync – Initial Setup".

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a mobile device with a serial port. The desktop or laptop PC must be running Windows 95, 98, NT or 2000.
- Null modem cable with all control lines connected. LXE recommends using the null modem cable part number listed in "Accessories".

Infrared Port Transfer

- A desktop or laptop PC with an infrared port and a mobile device with an infrared port. The desktop or laptop PC must be running Windows 95 SR2, 98 or 2000.

USB Transfer

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows 98 SR2 or Windows 2000.
- Use the LXE-specific USB cable as listed in "Accessories".

Connect

Connect the modem cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the mobile device (**Start | Programs | Communications | Connect)**.

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected, not requiring you to select "Connect" from the Start menu.

Disconnect

Serial Connection

- Disconnect the cable from the mobile device.
- Put the mobile device into suspend by tapping the red Suspend button.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IRDA Connection

- Move the mobile device so the infrared beam is broken.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

USB Connection

- Disconnect the cable from the mobile device.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IMPORTANT – Do not put the mobile device into suspend while connected via USB. The device will be unable to connect to the host PC when it resumes operation.

Radio Connection

- Put the mobile device into suspend by tapping the red Suspend button.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. 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 between a unique client can be established to two hosts.

When the mobile device 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. (**Control Panel | System | Device Name**)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device 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.

ActiveSync with a Cradle

To ActiveSync, the cradle must be powered off, the ActiveSync cradle cable attached to the desktop PC and the cradle, then the cradle connected to external AC/DC power.

Note: ActiveSync transfers files to the MX3X over the RS-232 connector on the cradle using the MX3X070CBLD9RS232AS cable.

Note: There is no cabled ActiveSync connection through the MX3-RFID passive cradle.

Figure 1-17 ActiveSync Cable Connected to Serial port on Cradle

RFID Device and LXE Cradles

The MX3-RFID device is too bulky to fit in the standard MX3 powered cradles. There is a passive vehicle cradle available for the MX3-RFID device that secures the device to the cradle only. See section titled “Accessories”.

Main battery charging and host communication is not available through the passive vehicle cradle. The passive vehicle cradle does not have LEDs or indicators. It does not accept DC power connection.

The MX3-RFID can be connected to DC Power while secured in the passive vehicle cradle. It can also communicate wirelessly with the host while in the passive vehicle cradle.

Troubleshooting ActiveSync

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the MX3X is already in a powered docking cradle cabled to a PC, remove and reinsert the MX3X into the powered cradle.

If the MX3X is connected to a PC by a cable, disconnect the cable from the MX3X and reconnect it again.

Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

See Also: "Cold Boot and Loss of Host Reconnection".

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-tapping REPLLOG.EXE on the CE device, the word "CLIENT" appears on the display in ASCII format. When using a serial port monitor, you see the host echo "CLIENT", followed by "SERVER". After this point, the data stream becomes straight (binary) PPP.

Storage Cradles

Note: The "MX3 Cradle Reference Guide" contains cradle installation and technical information.

There are two types of cradles for the MX3X: a desktop cradle for table top charging/communication applications and a vehicle mount cradle for vehicle mounted charging/communication applications.

A passive vehicle cradle is available for the MX3-RFID device. See the following section "The MX3-RFID and Cradles".

The powered cradles give the MX3X the ability to communicate with a host computer and other equipment. In addition, using wall AC adapters or DC/DC converters, the cradle transfers power to the internal charging circuitry of the MX3X and, in turn, the operating system recharges the main battery.

The MX3X can be either on or in Suspend mode while in the cradle. The MX3X can be inserted and removed from the cradle with one hand.

Cables are available from LXE for connecting the cradle to a printer, a personal computer or a barcode printer. Tethered scanners (for RS-232 cradle connection) are also available from LXE.

Status LED

An LED indicator on the front of the cradle shows the status of the cradle. When the indicator is not illuminated, there is no power applied to the cradle.

Cradle Power	**Amber**	External power applied to the cradle.
Docked	**Green**	Power applied to the cradle and charging connection made with the MX3X.
IR Active	**Red**	IR communication is active.

Desktop Cradle

*Note: LXE recommends the correct Desktop Cradle always be used to store / charge / communicate with the MX3X. The MX3X Desktop Cradle label is located on the bottom of the device. The MX3X Desktop cradle Product Number is **2381A002DESKCRADLE**.*

Lower the mobile device straight into the cradle, tilt it forward and then let it rest backward in the cradle. Ensure that the mobile device is properly seated on the charging contacts. The CHGR LED will illuminate green when the MX3X is correctly seated in the cradle. The CHGR LED will illuminate red when the MX3X main battery is being charged (in a cradle connected to an external power source). To remove the MX3X, tilt the MX3X forward and lift it straight up out of the cradle.

Note: Do not "slam" or slide the mobile device sideways into the cradle. Damage may result.

Connectors

The Power connector is located on the back of the cradle in the top left hand corner. The cradle can be powered, if required, by an LXE US AC Adapter or an LXE International AC Adapter. When powered, the cradle transfers power to the internal charging circuitry of the MX3X allowing it to recharge the main battery. A powered cradle supports RS-232 and IR communications.

The RS-232 connector is located in the back center of the cradle. When the MX3X is properly docked, the bi-directional half-duplex transceivers in the MX3X and cradle are aligned through their IR windows. The half-duplex IR signals from the MX3X are converted to RS-232 signals in the cradle and available at this connector.

Vehicle Mount Cradle

This cradle is specifically designed for vehicle mount applications. The cradle restrains the MX3X and isolates the computer from shock and vibration. The MX3X is inserted into the cradle by placing the base of the unit in the pocket and then firmly pressing the unit backwards until the release mechanisms latch and hold the unit in the cradle. The MX3X is removed from the cradle by pressing the release mechanisms and pulling the MX3X up and away from the cradle.

Connectors

The Power connector is located on the back of the cradle below and to the left of the RS232 port. The cradle is powered by either a vehicle's 12V battery or from an approved accessory for vehicles with higher voltage (24 to 60 VDC) batteries. When powered, the cradle transfers external power to the MX3X, which in turn, recharges the main battery. A powered cradle allows RS-232 and IR communication.

The RS-232 connector is located on the back of the cradle below and to the right of the power connector. When the MX3X is properly docked, the bi-directional half-duplex transceivers in the MX3X and cradle are aligned through their IR windows. The half-duplex IR signals from the MX3X are converted to RS-232 signals in the cradle and available at this connector.

Note: ActiveSync will transfer files over the RS-232 connector on the vehicle cradle.

ActiveSync with a Cradle

To ActiveSync, the cradle must be powered off, the ActiveSync cradle cable attached to the desktop PC and the cradle, then the cradle powered up.

Note: ActiveSync transfers files to the MX3X over the RS-232 connector on the cradle using the MX3X070CBLD9RS232AS cable.

Note: The MX3-RFID uses a passive, non-powered cradle. ActiveSync connects through powered cradles only.

Tethered Scanner and a Cradle

To use a tethered scanner connected to the RS232 port on the cradle, the cradle must be powered off, the ActiveSync cable removed and the cradle powered up. Then, the scanner can be attached to the cradle.

The MX3-RFID and Cradles

The MX3-RFID device is too bulky to fit in the standard MX3 powered cradles. There is a passive vehicle cradle available for the MX3-RFID device that secures the device to the cradle only. See section titled “Accessories”.

See Chapter 5 “MX3-RFID”.

Getting Help

All LXE user guides 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 check the LXE ServicePass website for the latest manual releases.

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 ServicePass website.

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

Manuals

MX3X User's Guide
LXEbook – MX3X User's Guide (download to MX3X)
MX3 Cradle Reference Guide
MX3 Multi-Charger Plus User's Guide

Accessories

1 Cable, USB Host D9F to USB, 6' (Endcap only)
MX3XA069CBL09USBCLNT

2 Cable, D9F to D9F for ActiveSync only, 6' (Cradle use only)
MX3XA070CBLD9RS232AS / Cradle 2381A002DESKCRADLE

3 Cable, USB Client D9F to USB, 6' (Endcap only)
MX3XA071CBLD9USBTYPB

Cable, 12 in., D9F / USB Type A Receptacle
MX3XA068CBLD9USBHOST

Tethered Scanners	
Scanner, Powerscan SR, 8’ Cbl, WW	8300A326SCNRPWRSR8DA9F
Scanner, Powerscan SR, 12’ Cbl, US	8300A327SCNRPWRSR12DA9F
Scanner, Powerscan LR, 8’ Cbl, WW	8310A326SCNRPWRLR8DA9F
Scanner, Powerscan LR, 12’ Cbl, US	8310A327SCNRPWRLR12DA9F
Scanner, Powerscan XLR, 8’ Cbl, WW	8320A326SCNRPWRXLR8DA9F
Scanner, Powerscan XLR, 12’ Cbl, US	8320A327SCNRPWRXLR12DA9F
Scanner, LS3408ER, 9’ Cbl, US See Note	8520A326SCNRERDA9F
Scanner, LS3408FZ, Fuzzy Logic, 9’ Cbl, US See Note	8510A326SCNRFZYDA9F
Scanner Clip Strap (85XX scanners only)	9000A411SCNRSTRAP
Holding Accessories	
Strap, Hand, Nylon	2381A497HANDSTRAP
MX3X Nylon Holster for use with Belt	2381A401HOLSTER
MX3X Nylon Hip Flip	9000A408HIPFLIP
Adjustable Belt for Hip Flip – Velcro ends	9200L67
MX3-RFID Nylon Case with Shoulder Strap	MX3XA411RFIDCASE
MX3X Nylon Case with Shoulder Strap	9000A409CASE
Stand, Scanner For 5300IP Series Scanner, Tethered	8100A001STAND
Bracket, Mounting LS300 Scanner, Tethered	8010A001BRKT
Holster, Hood, Nylon, 5300IP Series Scanner, Tethered	8100A401HLSTRHOOD
Miscellaneous	
Pen, Stylus, Black	9000A501PASSIVEPEN
Stylus Kit	9000A501PASSIVEPEN
MX3X SDK	MX3XA504CENET42SDK
Touchscreen Protective Film, Monochrome Display	MX3XA502PROTFILMMONO
Touchscreen Protective Film, Color Display	MX3XA503PROTFILMCOLR
Battery Chargers and Battery	
Battery Charger/Analyzer, US V1.01	9000A377CHGR5US
Battery Charger/Analyzer, WW	9000A377CHGR5WW
Battery, Li-Ion, Replacement, RFID Device	MX3A380RFIDBATT
Battery, Li-Ion	MX3A378BATT

Cradles and Power Supplies	
MX3-RFID Passive Mounting Cradle	MX3XA001RFIDCRADLE
MX3-RFID RAM Mounting Kit for Passive Cradle	9000A019RAMKIT
MX3X Desktop Cradle [1]	2381A002DESKCRADLE
MX3X Vehicle Mount Cradle [1]	2381A003VMCRADLE
MX3X Vehicle Mount Cradle, 19.2K baud rate	9000A005VMCRADLE19KB
Power Supply, Vehicle Cradle, 9-30VDC	2381A054CRDLDCPWR30V
Power Supply, Vehicle Cradle, 30-80VDC	2381A055CRDLDCPWR80V
AC Power Supply, External, US	9000A301PSACUS
AC Power Supply, External, AC, International	9000A302PSACWW
Power Cord, AC, US	9000A066CBLPWRAC
P/S, External, Cigarette Lighter Adapter	9000A303PSCIGLTADPT
Power Adapter, Bare Wire 12 VDC	1300A053CBL12ML3
Power Adapter, 24-72 VDC, Bare Wire (Vehicle)	9000A316PS24V72VMX13
Power Adapter, 110-240 VAC	1300A303PSACWW
Cables for Cradle and Endcap Serial Ports	
Cable, Null Modem, PC, D9F to D9F, 6’	9000A054CBL6D9D9
Cable, Null Modem, Printer/PC, D9F to D25F, 6’	9000A053CBL6D9D25
Cable, USB D9F to USB Type A Receptacle	MX3XA068CBLD9USBHOST
Cable, USB D9F to USB Type A Plug	MX3XA069CBLD9USBCLNT
Cable, USB D9F to USB Type B Plug	MX3XA071CBLD9USBTYPEB
Cable, D9F to D9F for ActiveSync only, 6’ See Note	MX3XA070CBLD9RS232AS

Note: The MX3X Desktop Cradle supports RS-232 ActiveSync communication via the MX3XA070CBLD9RS232AS cable.

Note: When using the 8500 Series tethered scanners (LS3408), the tethered scanner Power Mode must be set to “Reduced Power Mode”to conserve the device’s main battery life. The reduced power mode setting will not impact performance of the 8500 series scanner. The default mode is “Continuous On”. Please refer to the tethered scanner manufacturer’s user guide for instruction.

[1] Power Adapter Required.

Chapter 2 Physical Description and Layout

Hardware Configuration

Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

The MX3X and MX3-RFID hardware configuration is shown in the following figure.

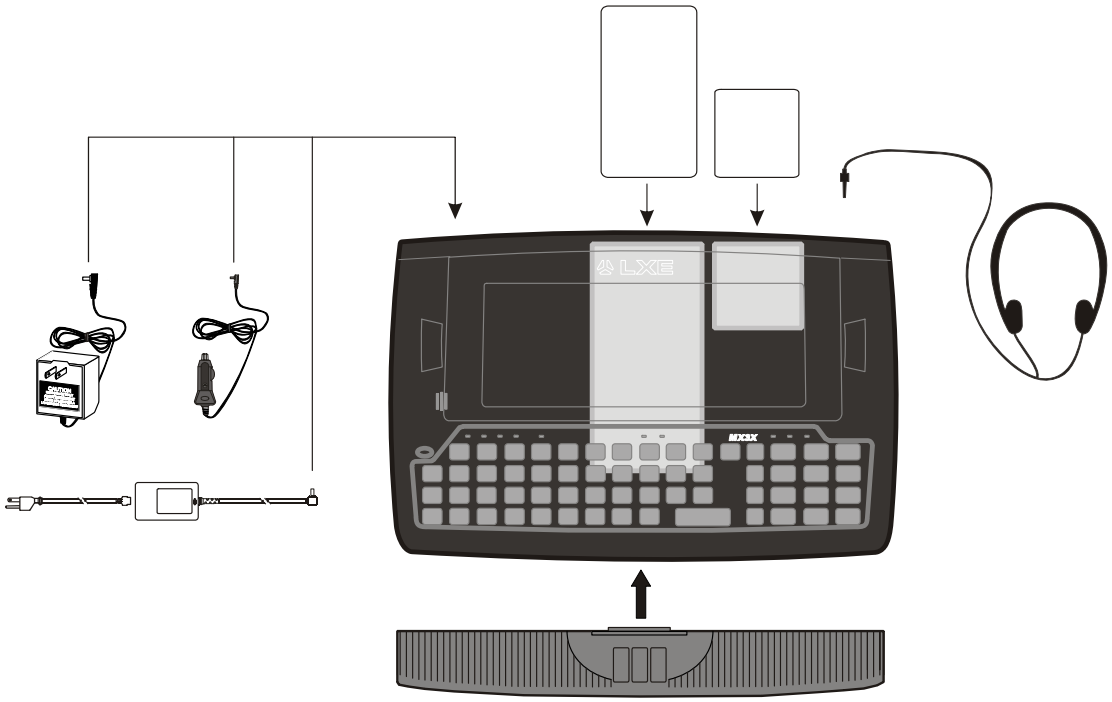


Figure 2-1 Hardware

Central Processing Unit

The CPU is an Intel Xscale PXA255 running at 400 MHz.

System Memory

A CF Card FLASH is used for ROM, Flash for Windows CE .NET and Flash memory for bundled applications. The Flash is configured as the primary boot device and contains the Windows CE .NET image, boot loader, OAL, applications, utilities and device drivers.

Any flash remaining beyond the Windows CE .NET image is formatted for use as a persistent memory drive (which appears in My Computer as the folder "System"). Any programs or data stored in this folder will not be lost if the memory backup battery fails.

The computer has one Type II CF+ slot. The computer supports and auto detects up to 256MB of Type I compact flash memory.

Core Logic

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

- One PCMCIA slot (supports Type I or II PCMCIA cards).
- One compact Flash card port (supports Type I and II cards).
- One InfraRed port.
- One Digitizer Input port (see section titled “Touchscreen”).
- Two I/O ports in six configurations (see section titled "Endcaps and COM Ports.").

Video Subsystem

The display has a 640 pixel (horizontal) by 240 pixel (vertical) format. The display contrast is adjustable with key sequences. Backlighting is available and can be adjusted with key sequences. The turn-off timing is configured through the Control Panel. The display controller supports Windows CE graphics modes. Touchscreen allows mouse functions (pointing and clicking on the display or Signature Capture) using an LXE approved stylus.

There are two types of displays available: transflective greyscale monochrome; and transmissive color. The transmissive color display is optimized for indoor lighting. It cannot be used without the backlight. The transflective monochrome is optimized for outdoor use but may also be used indoors. The monochrome display has an electroluminescent backlight. The color displays have a CCFL (Cold-Cathode Fluorescent Lighting) backlight.

The transflective display appears to have a greenish hue when the display is off or suspended. The transmissive display appears black when the display is off or suspended.

See Section “Display” .

Power Supply

The mobile device uses two batteries for operation.

- A 1900 mAh replaceable Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while the computer is in a powered cradle or when connected to the optional external power sources. The main battery can be removed and inserted in the MX3 Multi-Charger which simultaneously charges up to six battery packs in four hours.
- An internal 50 mAh Nickel Cadmium (NiCd) backup battery. The backup battery is recharged directly by the main battery when it is in the mobile device. Full charging of the backup battery may take several hours. The recharging of the backup battery is automatically controlled by the operating system. The backup battery must be replaced by qualified service personnel.

See Chapter 3 “Power Supply”.

Optional AC adapters are available – external AC power supplies (US and International) and a cigarette lighter adapter. See Chapter 3 “Power Supply”, “External Power Supply”.

Audio Interface

An interface is available for headset operation. When a headset is plugged into the audio jack on the endcap, the main speaker is disabled.

PCMCIA Slots

Use and operation of the Personal Computer Memory Card International Association (PCMCIA) device (e.g. PC card) is dependent upon both the type of device installed and the application(s) running on the computer.

Make sure the proper software is pre-loaded and PC cards are properly configured.

Slot 0 – Radio or SRAM Cards

Note: When removing or installing the radio, protect the internal components and the radio from electrostatic discharge.

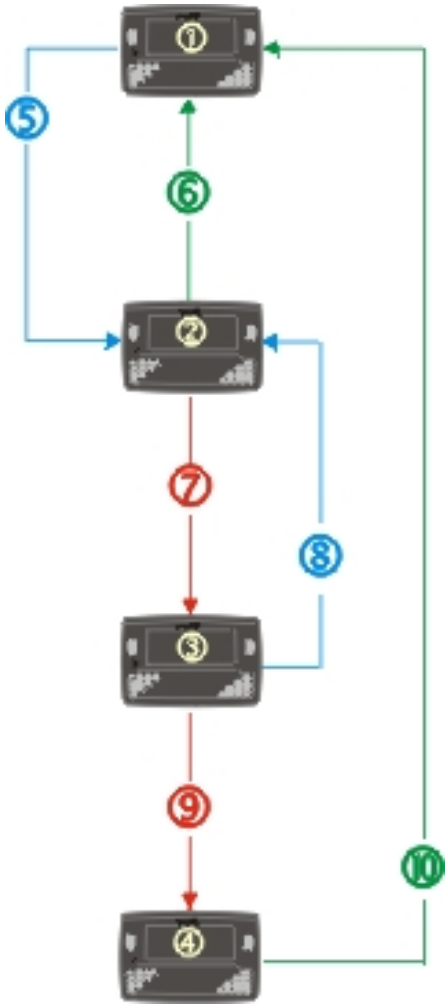
The mobile device has one internal PCMCIA slot that conforms electrically to PCMCIA 2.1 specifications. The PC Slot supplies 0.75 of an amp at 5Volts or 3.3Volts. Battery voltage is supplied through unused pin 35 to support a WAN radio in the slot.

The PC slot is accessible by the use of a Phillips screwdriver to first loosen the endcap. It accepts Type I or II cards only. Slot 0 accepts PCMCIA 2.4GHz radio cards or SRAM/Flash memory cards.

Slot 1 – Compact Flash Card

The mobile device has one internal Compact Flash card port that supports Type I and II CF+ cards. The slot is accessible when the endcap has been loosened.

Power Modes



1 – On

2 – Suspend

3 – Critical Suspend

4 – Off

5 – Power Button or Power Off Timer expires

6 – Primary Event

7 – Power fail. Also from Suspend (2) or On (1).

8 – Restoration of power.

9 – Backup battery and main battery dead

10 – Power applied. New main battery installed or external power applied. Tap the Power button.

Note: After event 8, the only primary event (6) which functions is a power button tap.

Figure 2-2 Power Modes – On, Suspend, Critical Suspend and Off

Primary Events Listing

Any key on the keypad	COM1 activity
Stylus touch on the touchscreen	COM2 activity
Power button tap	COM3 activity
PC card activity	USB client connection
External power connection	Scanner activity

On Mode

The Display

When the display is On:

- the keyboard, touchscreen and all peripherals function normally
- the display backlight is on until the Backlight timer expires (default is 3 seconds) 15 seconds afterwards, the display turns off.
- when the main battery is hot-swapped, the display is turned Off.

The Mobile Device

After a new mobile device has been received, a charged main battery inserted, and the Power button tapped, the computer is always On until both batteries are drained completely of power.

When the main 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 main battery is inserted or external power is applied. Press the Power button to turn the device on.

User Idle Mode

Note: When the display backlight is Off, the unit is still On. The unit functions normally – a tethered scanner trigger press or an integrated scanner Scan key press will cause scans. Communications through the radio or serial ports continue.

User Idle timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

The display backlight is turned off when one of the following occurs:

- the user idle timer expires before a wakeup event takes place
- the Power button is tapped which immediately places the unit into Suspend Mode.

Display Backlight Suspend timers are set using **Start | Settings | Control Panel | Display | Backlight** tab.

Any of the following primary events will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display backlight wakes up, the User Idle Timer begins the countdown again. When any of the above events occur prior to the timer expiring, the timer begins the countdown again.

The first display backlight wakeup key press or touch is sent to the operating system or running application. Once the display is On, the keyboard and touchscreen function normally.

System Idle Mode

Note: When the display is Off, the unit is still On. The unit functions normally – tethered scanner trigger press or integrated scanner Scan key press will cause scans. Communications through the radio or serial ports continue.

System Idle timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

The display is turned off when the System Idle timer expires before a wakeup event takes place.

The Power button is tapped which immediately wakes the unit up.

The Status LED blinks green when the Display enters Off mode.

Any of the following primary events will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display wakes up, the System Idle Timer begins the countdown again. When any of the above events occur prior to the timer expiring, the timer begins the countdown again.

The first display wakeup key press or touch is sent to the operating system or running application. Once the display is On, the keyboard and touchscreen function normally.

Suspend Mode

The Suspend mode is entered when the device is either inactive for a predetermined period of time, the user taps the Power button or the user selects **Start | Suspend**.

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

Any of the following can be configured to wake the unit and reset both the display and display backlight timers:

Any key on the keypad	PC card activity
Power button tap	Stylus touch on the touchscreen
COM1 CTS	External power connection
COM3 CTS	USB client connection

When the device wakes up, the User Idle, System Idle and the Suspend timers begin the countdown again. When any one of the above events occurs prior to the Suspend timer expiring, the timer starts the countdown again.

The first wakeup key press or touch is not sent to the operating system or running application – the first keypress or touch is only used to wake up the unit and reset the timers. Once the unit has transitioned from the Suspend mode to the On mode, the unit, keyboard and touchscreen function normally.

Critical Suspend Mode

The purpose of the Critical Suspend mode is to reduce power consumption to a lower level that still retains the contents of SDRAM. The device enters Critical Suspend Mode only when the main battery has failed or is removed/hot-swapped. The backup battery is supplying power to the unit during Critical Suspend Mode.

When hot-swapping (the main battery is removed and replaced), the display turns off, the BATT M LED begins to flash red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card.

When the device is in the Critical Suspend state (the main battery is in place and the device is being powered by the backup battery), the display turns off, the BATT M LED begins to flash red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card. The operating system is saving the state prior to the main battery failing and cannot be used.

If a fully charged main battery is installed before the backup battery is depleted (approximately 5 minutes) the device transitions to the Suspend state. To resume operation tap the Power key.

If the backup battery is depleted before a fully charged main battery is inserted, the device immediately turns itself Off and all unsaved information is lost. Insert a fully charged main battery and press the Power button to turn the device On.

Off Mode

The unit is in Off Mode when the main battery and the backup battery are depleted.

Insert a fully charged main battery and press the Power button to turn the device On.

Physical Controls

Power Button

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

The power button is located above the ESC key on the keypad. When a battery is inserted for the first time, the Power button must be pressed.

Figure 2-3 Location of the Power (PWR) Button

Quickly tapping the Power button places the device immediately in Suspend mode. Quickly tapping the Power button again, or touching the screen, immediately returns the device from Suspend.

Restart Sequence

Tap **Start | Run,** then type **`warmboot`** in the textbox and press **Enter.**. If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

When the Windows desktop is displayed or an application begins, the power on (or reboot) sequence is complete. If any changes to the settings had been saved previously, they are restored on reboot.

Any RFID tag data retrieved and not saved is lost during a reboot or reset.

Note: To reset to factory default values, please refer to Chapter 4 "System Configuration" section titled "Utilities".

Endcaps and COM Ports

The computer supports three COM port options. Two external serial ports are dependent on the end cap chosen. A third serial port is used to support an infrared transciever (barcode reader). An additional endcap configuration supports serial and USB “slave” input/output at 1.5 MBps.

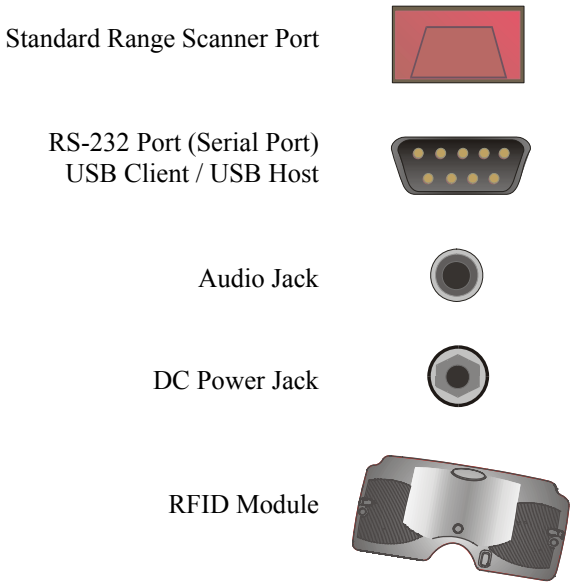


Figure 2-4 Endcap and COM Ports

The COM 2 port is always the IR port on the back of the mobile device, regardless of the type of endcap installed. COM 2 can only be accessed when a tethered scanner is connected to the RS-232 port on the cradle, and the MX3X is in the cradle. The cradle does not need to be powered by an alternate AC or DC power source. Tethered scanners receive power from the mobile device's main battery.

On the Standard Range Scanner / Serial Port endcap COM 3 is the Integrated Scanner port. The integrated barcode scanner scans only when the Scan button is pressed. To edit Scanner Com Port parameters, select **Start | Settings | Control Panel | Scanner**. Change the parameter values and tap OK to save the changes.

On the Dual Serial Port endcap the COM1 port is the serial port on the right side of the endcap when the display is facing you.

Caution -- Do Not Use the RS-232 Labelled Endcap Port for Cables with USB Plugs/Receptacles:

Caution -- Do Not Use the USB Labelled Endcap Ports for Serial Tethered Scanners:

Figure 2-5 Serial Ports and Cables

Endcap Combinations

Left Port	Right Port
Serial COM3	Serial COM1
Serial COM3	USB Client
USB Host	Serial COM1
USB Host	USB Client
Scanner	Serial COM1
Scanner	USB Client
Rear **IR Port** is COM2 Barcode scanners, tethered to the serial port on a cradle, send ASCII data to the MX3X in the cradle through the COM2 Port.	
MX3X with RFID Module RFID Module – COM1 IR Port – COM2 Integrated Scanner port on Endcap – COM3 USB-C Labelled port on Endcap – USB-C	

Figure 2-6 Endcap Combinations

COM Port Switching

The COM 2 port is always the IR port on the back of the computer, regardless of the type of endcap installed.

On the Standard Range Scanner / Serial Port endcap COM 3 is the Integrated Scanner port.

On the Dual Serial Port endcap the COM1 port is the serial port on the right side of the endcap when the display is facing you.

The process used to enable the MX3X COM1 serial port for use with a tethered scanner is as follows:

Note: Use the scanner control panel to setup using both the integrated laser scanner and a tethered scanner.

To switch active scanner Com ports select **Start | Settings | Control Panel | Scanner | Main** tab.

Note: If there is an integrated laser scanner, COM3 is greyed out – if there is no integrated laser scanner, Internal is greyed out. See Chapter 5 "MX3-RFID" for Scanner settings when there is an RFID module in use.

To assign baud rate, parity, stop bits and data bits to Com 1, Com 2 or Com3, select **Start | Settings | Control Panel | Scanner | COM ..** tab.

See Also: Section titled "Tethered Scanners".

Integrated Scanner Port

The integrated laser barcode scanner is used to collect barcode data from any nearby compatible barcode label. Depending on the size of the barcode, size of bars and spacing and quality of the barcode, the scanner is used to read barcodes between 3" and 30". The barcode scanner reads UPC/EAN, Code 39, Code 93, I 2 of 5, Discrete 2 of 5, Code 128, Codabar and MSI symbologies.

The integrated laser scanner scans only when the Scan button is pressed. Scan buttons have no effect on tethered barcode scanners connected to a serial port on the endcap or to the serial port on a cradle holding an MX3X. The SCNR LED illuminates during any mobile device integrated scanner activation.

The mobile device has an SE923 scanner engine.

If you need to set up the integrated scanner **barcode reading parameters**, please refer to the "Integrated Scanner Programming Guide" and the "MX3" barcode scanner type. The guide is on the LXE Manuals CD and the LXE / ServicePass website.

After scanning the barcodes that change Baud Rate, Parity, or Stop Bits go to **Start | Settings | Control Panel | Scanner | COM 3,** make the same changes, and save the changes by tapping OK.

Serial Port

RS-232 connection is made through a labelled RS-232 Serial Port if installed. The connector is an industry-standard RS-232. The connector is a PC/AT standard 9-pin "D" male connector.

Figure 2-7 RS-232 Port

Pin	Signal	Description
1	DCD	Carrier Detect
2	RXD	Receive Data - Input
3	TXD	Transmit Data - Output
4	DTR	Data Terminal Ready
5	GND	Signal/Power Ground
6	DSR	Data Set Ready
7	RTS	Ready To Send
8	CTS	Clear To Send
9	RI or +5V DC	Ring Indicator - Input

Figure 2-8 9-Pin RS-232 Pinout

LXE Connection Cable Technical Specification

The exact serial cable is crucial. Many commercial null modem cables will not work. LXE recommends the following cable:

Serial cable:

9000A054CBL6D9D9

Pinout:

D9 female	D9 female
1	7
2	3
3	2
4	6, 8
5	5
6, 8	4
7	1
9	no connection

Figure 2-9 Pinout – Serial Cable for Synchronization

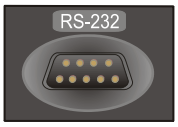
Some laptop devices do not properly implement all control lines on the serial port – the laptop connection will not work.

USB Host / Client Port

USB Host / Client connection is made through an optional USB Port if installed. The connector is an industry-standard 9-pin "D" male connector.

The optional LXE USB cable is required to adapt the connection to a standard USB connector. Please refer to section titled "Accessories" for the USB part number when ordering.

Caution -- Do Not Use the RS-232 Labelled Port for Cables with USB Plugs/Receptacles:

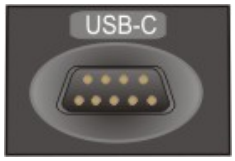


Caution -- Do Not Use the USB Labelled Endcap Ports for Tethered Scanners:

Figure 2-10 Endcap Ports

USB Host Cable

MX3XA069CBLD9USBCLNT



Port Label on Endcap

Mobile Device End	Goes To	USB Type A Plug End
1 Host Detect		1
2 Not Used		
3 D + (Green Wire)		3
4 Not Used		
5 Ground (Black Wire)		4
6 Not Used		
7 D - (White Wire)		2
8 Not Used		
9 Not Used		

Figure 2-11 USB Type A to Serial Port Cable Pinout

ActiveSync

Connect from USB-C port to USB Type A Host -- a laptop/desktop, etc.

USB Client Cable

MX3XA071CBLD9USBTYPB

Port Label on Endcap

Mobile Device End	Goes To	USB Type B Plug End
1 Not Used		
2 Not Used		
3 D + (Green Wire)		3
4 Not Used		
5 Ground (Black Wire)		4
6 Not Used		
7 D - (White Wire)		2
8 Not Used		
9 Power		1

Figure 2-12 USB Type B to Serial Port Cable Pinout

Connect from USB-H serial port to USB Type B Male receptacle on a USB hub, camera, etc.

Tethered Scanners

*Do **not** connect a tethered scanner cable to a mobile device's USB-C or USB-H labeled endcap port*. These ports cannot power a tethered scanner. Tethered scanners connect to RS232-labeled ports on the endcap and can connect to the RS232 port on a powered cradle.

The Scan buttons have no effect on tethered barcode scanners (connected to a serial port). Tethered scanners read barcode scans only when the trigger on the tethered scanner is pressed. The tethered scanner requires power on pin 9 of the mobile device's serial port.

To set the MX3X to use a tethered scanner, select **Start | Settings | Control Panel | Scanner | COM1 (or 2 or 3)**.

Tap the "**Power on Pin 9 (+5V)**" checkbox for the COM port selected. The COM port that accepts the scanner data can be configured for data rate, parity, stop bits and data bits.

See Also: Section titled "Cradles" when using a tethered scanner with an powered cradle.

Programmable Scan Buttons

Figure 2-13 Programmable Buttons

There are two buttons, one on each side of the display. The buttons can be programmed to perform specific functions. The programmable keys have no effect on barcode scanners tethered to the device. When there is no integrated scanner installed, both buttons default to Enter buttons (with the exception of IBM 5250 terminal emulation devices – in this case, the left button is labelled and functions as "Field Exit").

Note: The programmable Scan key is the Field Exit key when the MX3X is an IBM 5250 / TN5250 compatible device. It can also be programmed as the RFID Read key for an MX3-RFID device.

To edit the button parameters, select **Start | Settings | Control Panel | Scanner**. Change the parameter values and tap OK to save the changes.

The default setting for the right button for the MX3X is Enter; for the MX3-RFID it is RFID Read. The default setting for the left button is Scan. When the device does *not* have an integrated scanner, both buttons default to Enter keys and the Scan selection is greyed out.

Each button can be setup as:

- Disabled – no response when pressed
- Scan – initiate a barcode scan sequence (integrated scanner only)
- Enter Key
- Tab Key
- Field Exit (IBM 5250 / TN5250 devices only)
- Virtual Key (default values F20 and F21)
- RFID Read

Field Exit Key Function (IBM 5250/TN5250 Only)

The Field Exit key is used to exit an input field. If the field is an Auto Enter field, the auto transmit function is activated. This key function is present on the IBM 5250/TN5250 specific keypad only.

Scan Buttons and the SCNR LED

The SCNR LED, located above the keypad, illuminates during an integrated barcode scanner function. It is affected by internal scanner algorithms.

- Red - scanning.
- Green - good scan.
- Unlit – laser scanner is inactive.

The Scan buttons have no effect on tethered barcode scanners connected to a serial port. Tethered scanners read barcode scans only when the trigger on the tethered scanner is pressed. Pressing the trigger on the tethered scanner has no effect on the device's Scan buttons.

The Keypad

The QWERTY keypad is phosphorescent. A phosphorescent keypad does not use a keypad backlight but glows in dim/dark areas after exposure to a light source.

The keypad is installed and configured by LXE.

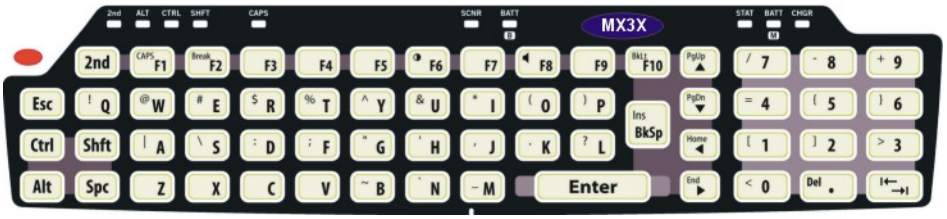


Figure 2-14 The QWERTY Keypad

The keymaps (keypress sequences) are located in "Appendix A - Key Maps."

Key Functions

Key	Function
Scan	**(*Scanner integrated into endcaps only.*)** The Scan key activates the scanner when a scanner endcap is installed and the Scan button is pressed. The internal scanner scans only when the Scan button is pressed. A Scan button press has no effect on externally attached scanners. See previous section titled "Programmable Buttons." When there is no integrated scanner endcap, the Scan keys function as Enter keys. For IBM 5250 configurations, the left button is the "Field Exit" key.
Enter	The Enter key is used to confirm a forms entry or to transmit information. How it is used is determined by the application running on the computer.
2nd	The 2nd key is used to activate the 2nd functions of the keypad. Printed on many keys at the upper left corner are small characters that represent the 2nd function of that key. Using the 2nd key activates the second key function. Note that the 2nd key only stays active for one keystroke. Each time you need to use the 2nd function you must press the 2nd key. To cancel a 2nd function before pressing another key, press the 2nd key again. When the 2nd function is active, the 2nd LED illuminates.
Ctrl	The Ctrl key enables the control functions of the keypad. This function is similar to a regular keyboard's Control key. Note that the Ctrl key only stays active for one keystroke. Each time you need to use a Ctrl function, you need to press the Ctrl key before pressing the desired key. When the Ctrl function is active, the Ctrl LED illuminates.

Key	Function
Alt	The Alt key enables the alternate functions of the keypad. This function is similar to a regular keyboard's Alt key. Note that the Alt key only stays active for one keystroke. Each time you need to use an alternate function, you need to press the Alt key before pressing the desired key. When the Alt function is active, the Alt LED illuminates.
Shft	The Shft key enables the shifted functions of the keypad. This function is similar to a regular keyboard's Shift key. Note that the Shift key only stays active for one keystroke. Each time you need to use a Shifted function, you need to press the Shft key before pressing the desired key. When the Shft function is active, the Shft LED illuminates. When the Shft key is pressed the next key is determined by the major key legends, i.e., the alpha keys display lower case letters -- when CAPS is On alpha characters are capitalized. For example, when CAPS is on and the Shft key and the G key are pressed, a lower case g is displayed.
Spc	The Spc key adds a space to the line of data on the display. This function is similar to a regular keyboard's Spacebar. Note that the Spc key only stays active for one keystroke.

Caps Key and CapsLock Mode

This function is similar to a regular keyboard's CapsLock key. Note that the CapsLock mode stays active until the CapsLock key sequence is pressed again. Each time you need to use a Caps function, you need to press the Caps key sequence first. To cancel a CapsLock function press the Caps key sequence again. When the CapsLock mode is active, the Caps LED illuminates.

The CapsLock key sequence is 2^{nd} + F1.

- No CapsLock AND No Shift keypress – result is a lowercase letter.
- CapsLock OR Shift – result is an uppercase letter.
- CapsLock AND Shift keypress – result is a lowercase letter.

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

- Press Tab and an Arrow key to select a file.
- Press Shift and an Arrow key to select several files.
- Once you've selected a file, press Alt then press Enter to open its Properties dialog.
- Press 2^{nd} then press numeric dot to delete a file.
- To force the Start menu to display, press Ctrl then press Esc.

Keypress Sequences

See Appendix A for all key press sequences.

Custom Key Maps

Custom Key Maps should not be confused with the process the system administrator uses to re-map the Scan buttons on either side of the touchscreen display.

See Appendix A “Keymaps”, section titled “Creating Custom Keymaps”.

To activate the Custom keymap, select **Start | Settings | Control Panel | Keyboard** icon. Select the Custom keymap from the keyboard popup menu, and close the control panel with the OK button. To return to the default keymap, select **0409** from the keymap popup and tap OK.

*Note: Mobile device’s host connection and Custom Key Maps: before connecting to a host using Remote Desktop Connection, go to **Start | Settings | Control Panel | Keyboard** and select **0409** from the keymap popup. Tap OK.*

LED Functions

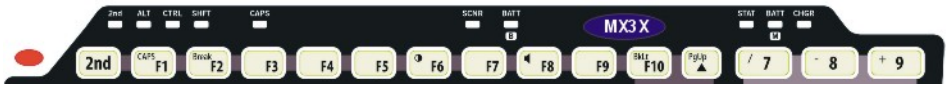


Figure 2-15 LED Functions

Across the top of the keypad are LEDs that provide visual cues to current computer operation. When the LED is not illuminated, the function is inactive.

LED	When illuminated ...
2nd	The next keypress is a 2nd keypress. • Amber when on • Blinks amber during configuration key sequence.
ALT	The next keypress is an ALT keypress. • Amber when on and unlit when off.
CTRL	The next keypress is a CTRL keypress. • Amber when on and unlit when off.
SHFT	The next letter is the uppercase letter on alpha keys and the shifted character on the numeric keypad keys. • Amber when on and unlit when off.
CAPS	Uppercase letters are active until the CAPS key sequence is pressed again. • Amber when on and unlit when off.
SCNR	Barcode scanner function, affected by both tethered scanners and the scanner endcap. • Red - scanning. • Green - good scan. • Unlit - scanner is inactive.
BATT B	Backup Battery. When illuminated, the backup battery is charging. When unlit, the backup battery is not charging
STAT	Status Indicator. • Amber – device is booting up. • Blinking Green when display Suspend state begins.
BATT M	Main Battery. When illuminated, main battery capacity is low. • Red – low battery. • Blinking Red – power fail. • Unlit - Main battery is not low OR all charge is depleted in both batteries..
CHGR	Charger. When on, the mobile device is receiving external power either from the DC power jack or the MX3X is seated in a powered cradle. • Red - Main battery is charging. • Amber – Fault or temporary standby (Contact LXE Customer Support). • Green - battery charge is complete and the mobile device is connected to external power through the power jack or a powered cradle.

Display

The touchscreen display is an LCD unit capable of supporting VGA graphics modes. Display size is 640 x 240 pixels. The display covering is designed to resist stains. The touchscreen allows signature capture and touch input. A pen stylus is included. The touchscreen responds to an actuation force (touch) of 4 oz. of pressure (or greater).

There are two types of displays available: transflective greyscale monochrome and transmissive color. The transmissive color display is optimized for indoor lighting. It cannot be used without the backlight. The transflective monochrome is optimized for outdoor use but may also be used indoors. The monochrome display has an electroluminescent backlight. The color display has a CCFL (Cold-Cathode Fluorescent Lighting) backlight.

The transflective display appears to have a greenish hue when the display is off. The transmissive display appears black when the display is off.

The choice between font sizes is made in the Control Panel option **Display | Appearance**. Font size selection may be overridden by a user supplied application.

The display is automatically turned off when the System Idle timer or Suspend timer expires.

Display and Display Backlight Timer

When the System Idle timer expires the display is turned off. The default value for the battery power timer is 15 seconds. The default value for the external power timer is 2 minutes.

When the User Idle timer expires the screen display backlight is turned off. The default value for the battery power timer is 3 seconds. The default value for the external power timer is 2 minutes.

Both values can be adjusted using the Control Panel option "Display | Backlight" or "Power | Schemes". Any of the following will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display wakes up, the timers will begin the countdown again. When any of the above events occurs prior to the timers expiring, the timers start the countdown again.

Touchscreen

The touchscreen provides a means of inputting information into the device by touching the screen using the LXE approved stylus (the Passive Pen – see Chapter 1 section titled “Accessories.”)

Touchscreen operation is not affected by Display Backlighting.

Touchscreen operation is affected by the Display mode. If the display is off, a stylus touch on the display will turn on the display. No touch data is sent to the running application until the next stylus touch.

Applying the Protective Film to the Display

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

Remove the protective film from it's 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.

Cleaning the Glass Display/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 scan aperture and display. If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex(R) 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.

Speaker

The speaker is located on the front of the mobile device above the Power button.

The Speaker has a loudness of at least 90 dB (2700 Hz) at 10 cm measured from the front of the unit. The Speaker volume is adjustable via the keypad or the Control Panel or by an application through the use of an API call. There are 16 distinct volume levels. The minimum volume level is 0 (no sound) with a default setting of maximum non-distorted volume. The volume sticks at maximum and minimum levels.

The speaker is disabled when a headset is plugged into the Audio Jack on the endcap.

Speaker volume is enabled and adjusted using the Control Panel "Volume & Sounds" option. After the speaker has been enabled using the Control Panel option, speaker volume is adjusted using the 2nd + <F8> key sequence, if desired.

Operational “beeps” are emitted from the speaker.

Infrared (IR) Port

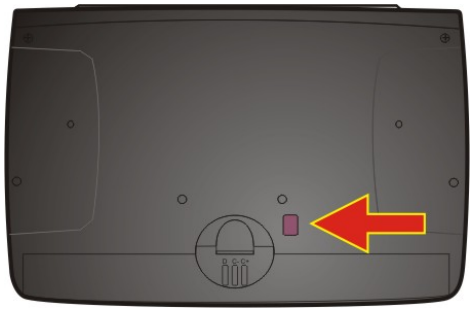


Figure 2-16 Infrared Port - COM2 Port

At the back of the mobile device is an Infrared (IR) Data Port. The IR Port is designed to provide a data link between the mobile device and a similarly equipped piece of equipment such as a printer. The IR port is the mobile device’s COM 2 port and is a bi-directional half-duplex communication port. It supports baud rates up to 115k, SIR (Slow IR). It will support serial port emulation, as well as IrDA and Winsock over IR protocols. It also supports ActiveSync.

The IR operating envelope has a distance range of 2 cm (.79 inches) to 1 meter (3.2 feet) with a viewing angle of 30 degrees.

The mobile device uses IrDA protocol to send data in both directions, but not simultaneously. When sending data through the IR port, make sure the IR port on the first mobile device and the IR port on the second mobile device are in close proximity to each other. IrDA is not required and not used by terminal emulation programs.

When the MX3X is docked in a cradle, the Status LED *on the cradle* is red when data is being transmitted through the IR port.

The MX3-RFID uses a passive cradle.

Chapter 3 Power Supply

Introduction

Note: LXE recommends that the correct MX3 Multicharger Plus always be used to charge the mobile device's main battery. The Multicharger plus label is located on the back of the device and the charger must have been upgraded to V1.01 to charge the mobile device's main battery pack to 100%. Please contact your LXE representative for further information about theV1.01 upgrade kit, if needed.

Note: LXE recommends the correct Desktop Cradle always be used to store / charge / communicate with the MX3X. The MX3X Desktop Cradle label is located on the bottom of the device. The MX3X Desktop cradle Product Number is ***2381A002DESKCRADLE****.*

The mobile device is designed to work with a Lithium-Ion (Li-Ion) battery pack from LXE.

Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

The mobile device receives continuous power from two batteries. There is a Lithium-Ion main battery that can be recharged separately by an LXE approved battery charging unit. The main battery is recharged, if required, while installed in a powered cradle or when the mobile device is connected to external power using the power jack. There is a 50 mAh Nickel-Cadmium (NiCd) backup battery inside the mobile device that is recharged only by the main battery.

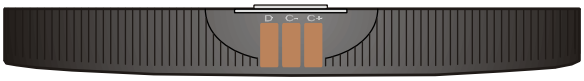


Figure 3-1 Main Battery

Note: ***New batteries must be charged prior to use****. This process takes up to four hours in an LXE Multi-Charger and eight hours when the mobile device is connected to external power through it's power jack.*

Check Battery Status

Tap the **Start | Settings | Control Panel | Power** icon. Main and backup battery level, status and Power Scheme timeout setting options are displayed.

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.

Caution 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.

Li-Ion Battery

When disposing of the main battery, the following precautions should be observed:

The battery should be disposed of promptly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

Main Battery

The main battery 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 LXE Multi-Charger or the mobile device battery well.

When the main battery is properly installed in the unit it provides up to eight hours of operation depending upon operation and accessories installed. The battery pack is resistant to impact damage and falls of up to four feet to a concrete surface.

Under normal conditions it should last approximately eight hours before requiring a recharge. The more you use the scanner, the radio, or the backlight at it's brightest setting, the shorter the time required between battery recharges.

Battery Hot-Swapping

When the main battery power level is low, the mobile device will signal the user with a warning dialog box on the display and the BATT M LED illuminates red. The Batt-M LED is illuminated until the main battery is replaced, the battery completely depletes, external power is applied to the mobile device using the power jack, or the MX3X is placed in a powered cradle.

You can replace the main battery by simply removing the discharged battery and installing a fully charged battery within a five minute time limit (or before the backup battery depletes).

When the main battery is removed, the mobile device automatically transitions to the Critical Suspend state. During Critical Suspend, the mobile device's backup battery will continue to power the unit for at least five minutes. Though data is retained, the mobile device cannot be used until a fully charged main battery is installed. After installing the fully charged battery, the mobile device automatically transitions to the Suspend state. To resume from the Suspend state, tap the Power button. Full operational recovery from Suspend can take several seconds while the radio (if installed) is reestablishing an RF link.

If the backup battery depletes before a fully charged main battery can be inserted, the mobile device will turn OFF and the Power key must be used after the main battery is installed.

All configuration data is saved to flash memory before the computer powers off.

Low Battery Warning

It is recommended that the main battery be removed and replaced when it's energy depletes. When the Low Battery Warning appears do an orderly shut down of the mobile device, minimizing the operation of any optional equipment and insuring any information is saved that should be saved.

When the mobile device is in an ON state, a low battery warning dialog box appears on the display and the Batt-M LED illuminates red.

An uninterrupted external power source (wall AC adapters or DC/DC converters) transfers power to the mobile device internal charging circuitry which, in turn, recharges the main battery and backup battery.

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

Critical Suspend State

The Critical Suspend state or mode can only be entered because of a main battery Power failure. A main battery Power failure can occur because the battery's energy has been depleted or the battery has been removed.

When the mobile device is in the Critical Suspend state the main battery LED illuminates, the System LED blinks red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card(s). The operating system is saving the state prior to the backup battery failing and cannot be used.

If a new fully charged main battery is installed before the backup battery fully depletes the operating system will transition to the Suspend state. To resume operation tap the Power key.

Backup Battery

The mobile device 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 need for recharging of the backup battery is automatically detected and controlled by the operating system. The energy needed to charge the backup battery comes from the main battery.

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

The backup battery is replaced by LXE.

Note: An uninterrupted external power source (wall AC adapters or DC/DC converters) transfers power to the mobile device's internal charging circuitry which, in turn, recharges the main battery and backup battery.

About Lithium-Ion Batteries

Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember -- the mobile device is always 'on' even when in the Suspend state and draws battery power at all times. Use the **Start | Settings | Control Panel | Power | Battery** tab to check the battery status and power reading.

Always replace the used main battery with a fully charged main battery. The Battery Low Warning LED illuminates red at approximately 35% of power left in the main battery. You need to determine the point at which battery life becomes unacceptable for your business practices and replace the main battery before that point.

Maintenance

*Note: Make sure there is a fully charged main battery in the mobile device **before** running the backup battery Discharge Utility. The backup battery can be discharged and charged while the mobile device is receiving external power through the Power Jack or from a powered MX3X cradle.*

The NiCd backup battery should be discharged completely once or twice a year. The main battery will fully charge the backup battery. This process will allow longer life for the backup battery.

The backup battery is discharged by selecting **Control Panel | Battery** and tapping the "Discharge" button. The discharge utility shows the progress of the discharging. At this time, the program can be exited while continuing the discharge process. Normal use of the mobile device can resume during the discharge, with the exception of Hot-Swapping the main battery. When the backup battery is fully discharged, the mobile device will automatically stop the discharge process and begin to recharge the backup battery.

DO NOT REMOVE THE MAIN BATTERY from the mobile device until the backup battery is completely discharged -- in approximately 1 hour and recharged in approximately 2.5 hours.

Battery Chargers

Note: LXE recommends that the correct MX3 Multicharger Plus always be used to charge the main battery. The Multicharger plus label is located on the back of the device and the charger must have been upgraded to V1.01. Please contact your LXE representative for further information about the V1.01 upgrade kit, if needed.

MX3 Multi-Charger Plus

Figure 3-2 MX3 Multi-Charger Plus

The mobile device's main battery can be charged/analyzed in the MX3 Multi-Charger Plus.

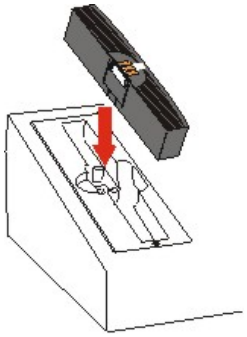


Figure 3-3 Insert Main Battery in Charge Pocket

Lower the battery pack straight into the battery charger pocket and push it down firmly until the retaining clip catches on the retaining pins.

Do not "slam" the battery into the charging cup or slide it in sideways.

Failure to follow these instructions can result in damage to the main battery or the charger.

Please refer to the specific battery charger user's guide for technical information and operating instructions.

External Power Supply (Optional)

The DC power jack is located on the endcap. The main battery is trickle-charged using external power supplies.

The cradle power jack is located on the back of the cradle.The mobile device (and the Desktop Cradle) connect to any of the following power supplies through the DC Power Jack.

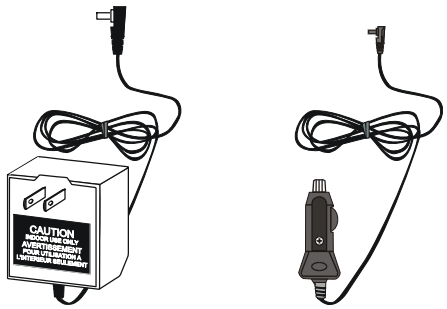


Figure 3-4 US AC/DC 12V Power Supply and Cigarette Lighter Adapter

Figure 3-5 International AC/DC 12V Power Supply

Note: When the MX3X is receiving external power through a cradle, the cradle's Status LED and the CHGR LED on the mobile device are illuminated.

Important Battery Charger Version Information

Battery Chargers Affected

MX3 Multi-Charger Plus
9000A377CHGR5

Use LXE V1.01 Upgrade Kit

MX3 Multi-Charger
MX3A378CHGR6
(Not Available After 7-2003)

Use LXE V1.20 Upgrade Kit

The MX3X main battery will be incompatible with MX3 Battery Chargers that have not been upgraded to V1.20 or V1.01. To successfully charge the mobile device Battery Pack, pre-existing MX3 Battery Chargers must be returned to LXE for a software upgrade.

Using a Multi-Charger Plus Battery Charger with the Mobile Device's Battery Pack

The mobile device device is designed to use a 2.2Ahr main battery to achieve 8+ hours of continuous operation.

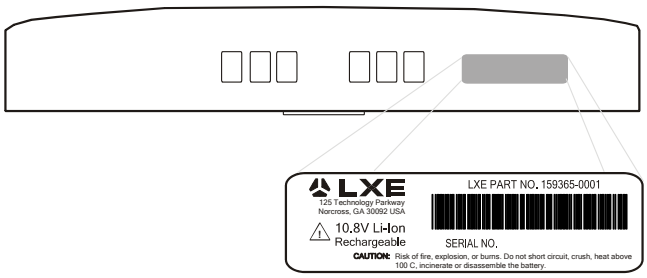
If the battery pack is inserted into a MX3 Multi-Charger Plus (*without the V1.01 upgrade*) bay, the battery may not become fully charged in the charger's 4 hour time limit and a red LED illuminates after 4 hours have elapsed indicating a Battery Problem.

Remove and reinsert the battery pack into the same charging bay. This will reset the timer and allow the charger to complete the charge cycle for the mobile device's main battery in approximately 2 hours..

LXE does not supply an external timing device with the Multi-Charger Plus.

Battery Label Location

The mobile device battery pack has a silver label (as opposed to the white labels on LXE's MX3 and MX3-CE battery packs).



Chapter 4 System Configuration

Introduction

Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

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

Windows CE .NET 4.2

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

This chapter's contents assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows 95, 98, NT, XP or 2000 desktop computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the mobile device and it's Windows CE .NET environment.

2.4 GHz Radio Configuration

All 2.4GHz radio configuration is included in Chapter 7, "Wireless Network Configuration".

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 MX3X / MX3-RFID you receive the software files required by the separate programs needed for operation and radio communication. The files are loaded by LXE and stored in subdirectories in the mobile device.

This section lists the contents of the subdirectories and the general function of the files. Files installed in the mobile device are specific to the intended function of the mobile device.

Files installed in each mobile device configured for an RF environment contain PCMCIA card radio specific drivers – the drivers for each type of radio are specific to the manufacturer (e.g. Cisco, Symbol) for the radios installed in the RF environment and are not interchangeable.

Software Load

The software loaded on the mobile computer consists of Windows CE .NET 4.2 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

Operating System

- Microsoft CE .NET version 4.2.

Radio Drivers

- Only one radio is installed at any one time. The 2.4GHz type of PC radio card resident in the device determines the type of radio driver running on the device.

RFID Driver

- Includes a configuration utility to be used when programming an RFID Tag reader.

Note: Please contact your LXE representative for software updates as they are released by LXE.

Software Applications

The following applications are included:

- WordPad (was PocketWord in previous versions of Windows CE)
- Pocket Inbox
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer
- Scanner Wedge (LXE developed)
- Transcriber
- Media Player
- Internet Explorer

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

Desktop

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

The Desktop appearance is similar to that of a desktop PC running Windows 95, 98, NT, 2000 or XP.

At a minimum, it has the following 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 mobile device is always powered On (when a fully charged main battery and backup battery are present).

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

Tap the screen once more or tap the Power button to "wake" the unit up.

Desktop Icon	Function
My Computer	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
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 Computer Folders

Folder	Description	Preserved upon Reboot?
System	Internal ATA Card (64 Meg total, 28 Meg free for User installed / created applications)	Yes
Network	Mounted network drive	No
Storage Card	ATA Card in Compact Flash Slot 1	Yes
Windows	Operating System in ROM	Yes
Program Files	Applications	No
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Temp	Location for temporary files	No

Folders Copied at Startup

The following folders are copied on startup:

System\Desktop -> Windows\Desktop
System\Favorites -> Windows\Favorites
System\Fonts -> Windows\Fonts
System\Help -> Windows\Help
System\Programs -> Windows\Programs

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

The following folders are *NOT* copied on startup:

Windows\AppMgr
Windows\Recent
Windows\Startup

because copying these has no effect on the system, or an incorrect effect.

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 Launch.

AppLock

The AppLock program is accessed by the user or the AppLock Administrator at bootup or upon completion of warm boot. Set parameters using the Administration option in the Control Panel.

See Also: Chapter 6 “AppLock” for instruction.

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: **Start | Programs**

Cisco	**Set Cisco radio / network parameters** (See Chapter 7, "Wireless Network Configuration" for instruction.)
Communication	**Stores Network communication options**
ActiveSync	Transfer files between a mobile device and a desktop computer
Connect	Run this command after setting up a connection
Start FTP Server	
Stop FTP Server	
Diagnostics	**Diagnostic tests for the Mobile Device**
Registry Editor	Edit the mobile device registry (c a r e f u l l y)
Test Utility	Select a test to run e.g. Display, keyboard, audio.
Microsoft File Viewers	**View downloaded files** (see Note)
Excel Viewer	View Excel 97 / 2000 / 2002 documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word 97 / 2000 / 2002 and RTF files
Symbol	Tap the Network icon in the toolbar to set up the Symbol radio (See Chapter 7, "Wireless Network Configuration" for instruction.)
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
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server.
LXE RFID Config	Configure the RFID reader. *(Placed in Control Panel after Revision C)*
Transcriber	Enter data using the stylus on the touchscreen.
Windows Explorer	File management program

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

Communication

Access: **Start | Programs | Communication**

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

ActiveSync

After a connect setup is selected, **Start | Programs | Communication | Connect** will start to connect to a host. After this connection is made and an ActiveSync relationship established, the ActiveSync menu item can be used to establish the connection over the radio link.

See Chapter 1 “Introduction” section titled “ActiveSync”.

Connect

After a connect setup is selected, **Start | Programs | Communication | Connect** will start to connect to a host. Connect is used to initiate a cabled connection to a host. Several pre-defined connect setups are included in the factory setup:

- COM1 direct connect at 57600 or 115200 baud
- Infrared connect at 57600 or 115200 baud
- COM3 direct connect at 57600 or 115200 baud
- USB direct connect

The default connect setup is USB direct connect.

Select "Make New Connection" and follow the instructions on the screen to create a connection while following the directions in the section titled "Backup Data Files using ActiveSync" later in this chapter.

See Also: Chapter 1 “Introduction”, section titled “ActiveSync”, subsection titled “Cold Boot and Loss of Host Re-connection”

Start FTP Server / 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.

Command Prompt

Access: **Start | Programs | Command Prompt**

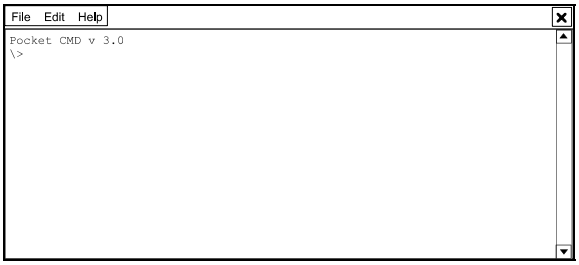


Figure 4-1 Pocket CMD Prompt Screen

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: **Start | Programs | Inbox**

This option requires a connection to a mail server. There are a few changes in the CE .NET 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 mobile device inbox and a desktop inbox.

Internet Explorer

Access: **Start | Programs | Internet Explorer**

This option requires a radio card and an Internet Service Provider. There are a few changes in the CE .NET version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the "?" button to access Internet Explorer Help.

Media Player

Access: **Start | Programs | Media Player**

There are few changes in the CE .NET version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options. Tap the "?" button to access Media Player Help.

Remote Desktop Connection

Access: **Start | Programs | Remote Desktop Connection**

There are few changes in the CE .NET version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options.

Select a computer from the drop down list and tap the Connect button.

Tap the **Options >>** button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the "?" button to access Remote Desktop Connection Help.

*Note: Custom Key Maps: before connecting to a host using Remote Desktop Connection, go to **Start** | **Settings** | **Control Panel** | **Keyboard** and select **0409** from the keymap popup. Tap OK.*

LXE RFID Config

Access: **Start | Programs | LXE RFIDConfig *or***
Start | Settings | Control Panel | RFID

See Chapter 5 “MX3-RFID” for information and instruction.

Transcriber

Access: **Start | Programs | Transcriber**

Select Transcriber on the **Start | Programs** menu. To make changes to the Transcriber application, enable or disable the current Transcriber session, etc., tap the “hand with a pen” icon in the toolbar. Tap the “?” button or the Help button to access Transcriber Help.

Windows Explorer

Access: **Start | Programs | Windows Explorer**

There are a few changes in the CE .NET 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: **Start | Settings | Taskbar and Start Menu**

The Taskbar can also be accessed by tapping on the taskbar and holding the stylus on the taskbar. Choose Properties from the popup menu.

Factory Default Settings	
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled

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

When the taskbar is auto hidden, press the **Ctrl** key then the **Esc** key to make the Start button appear.

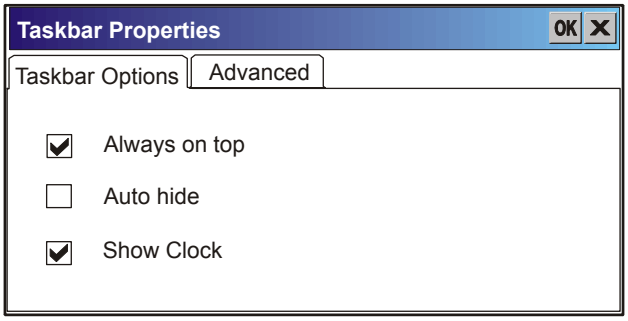


Figure 4-2 Taskbar Properties

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.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

Control Panel Options

Access: **Start | Settings | Control Panel** or **My Computer | Control Panel**

Getting Help

Please tap the "?" box to get Help when changing Control Panel options.

Option	Function
About	Displays hardware and software details.
Accessibility	Customize the way the keyboard, display or mouse functions.
Administration	Configure AppLock parameters.
Aironet Client Utility	Set the parameters for a Cisco radio. (See Chapter 7, "Wireless Network Configuration" for instruction.)
Battery	View the status of the Main and Backup batteries.
Bluetooth Device	Set the parameters for a Bluetooth radio.
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 (not supplied/supported by LXE).
Display	Set background graphic, color scheme appearance, and power scheme properties.
Input Panel	Select the current key / data input method.
Internet Options	Set General, Connection, Security and Advanced options for Internet connectivity.
Keyboard	Set key repeat delay and key repeat rate.
Mixer	Adjust the volume, record gain, and sidetone for microphone input.
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 owner details.
Password	Set access password properties.
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.
PCMCIA	Radio card in Slot 0, Internal ATA in Slot 2.
Power	Set Power Off, Backlight properties. Review battery status and perform backup battery charging/discharging.
Regional Settings	Set appearance of numbers, currency, time and date based on regional and language settings.
Remove Programs	Remove user installed programs in their entirety.

Option	Function
RFID	RFID Configuration Utility. Set Tag, Filter, Power, Read, and Format parameters. Use this option to upgrade RFID firmware.
Scanner	Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.
Storage Manager	Manage storage devices, create partitions.
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.
Volume and Sounds	Set volume parameters and assign sound wav files to CE .NET events.

About

Access: **Start | Settings | Control Panel | About**

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	LXE Utilities, LXE Drivers, LXE Image, LXE API, and Internet Explorer
Network IP	Current network connection IP and MAC address.

User application version information can be shown in the Version window. Version window information is taken 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: **Start | Settings | Control Panel | Accessibility**

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sound function. There is no change from general desktop Accessibility options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Administration

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

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

LXE 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.

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: **Start | Settings | Control Panel | Battery**

View the status of the Main and Backup batteries.

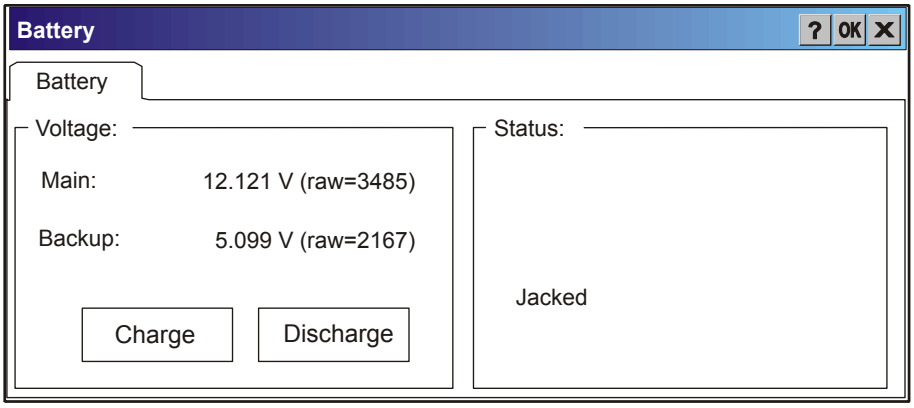


Figure 4-3 Battery

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

Tap the Charge or Discharge buttons to charge and discharge the backup battery. If the battery is Charging, tap the Discharge button to stop the Charge process. Tap Discharge a second time to begin the Discharge process. If the battery is Discharging, tap the Charge button to stop the Discharge process. Tap Charge a second time to begin the Charge process.

Bluetooth Manager

Access: **Start | Settings | Control Panel | Bluetooth Device Properties**

Set the parameters for a Bluetooth radio.

Factory Default Settings	
All Found Devices	Untrusted

Tap the Scan Device button to locate Bluetooth devices in your wireless area. Tap the "?" button and follow the instructions in the Help file to authenticate Bluetooth devices in your area.

Certificates

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

Manage digital certificates used for secure communication.

Lists the Stored certificates trusted by the mobile device user. These values may change based on the type of radio security resident in the client, access point or the host system.

 Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Date/Time

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

Set Date, Time, Time Zone, and Daylight Savings after cold boot or at anytime.

Factory Default Settings	
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Disabled

Note: Date and time is reset to the default value each time the mobile device is rebooted.

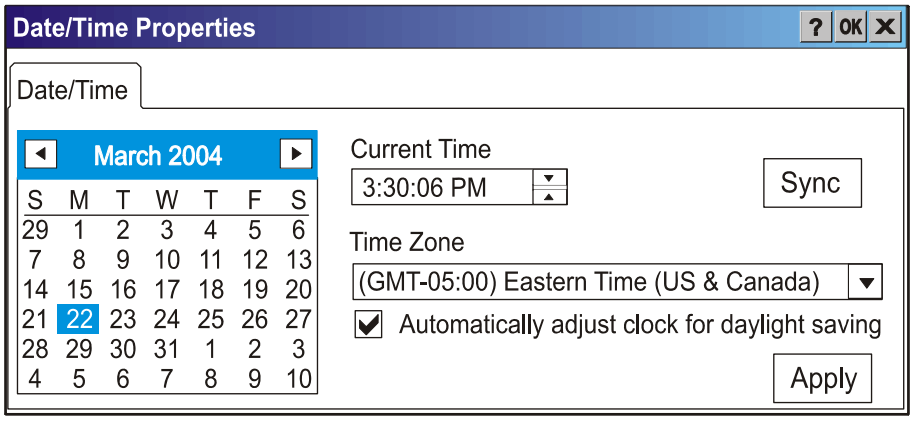


Figure 4-4 Date/Time Properties

There is no change from general desktop PC Date/Time Properties options. Adjust the settings and tap the OK box or the Apply button to save the changes. The changes take effect immediately. Double-tapping the time displayed in the Taskbar causes this display to appear.

Sync requires Internet connection. When an Internet connection is available, click the Sync button to synchronize the mobile device operating system time with an Internet time server.

Dialing

Access: **Start | Settings | Control Panel | Dialing**

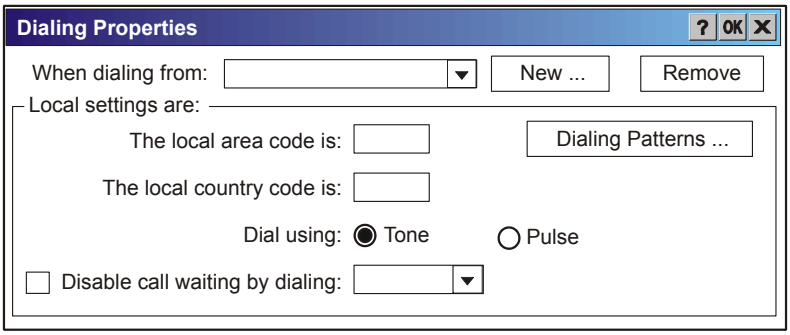


Figure 4-5 Dialing

Set dialup properties for internal modems (not supplied/supported by LXE). Tap the "?" and follow the instructions in Help.

Display

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

Set background graphic, color scheme appearance, and power scheme properties.

Factory Default Settings	
Background	Windows CE
Tile	Disable
Appearance	
Scheme: Monochrome Color	 High Contrast White Windows Standard
Backlight	
Battery Auto Turn Off	Enabled
Idle Time	30 Seconds
External Auto Turn Off	Enabled
Idle Time	2 minutes

Background

There is no change from general desktop PC Display Properties / Background options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Appearance

No change from general desktop PC Display Properties / Appearance options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. The default is High Contrast White for monochrome displays and Windows Standard for color displays.

Note: The color screens display Windows standard colors (or the color scheme selected) instead of shades of grey.

Backlight

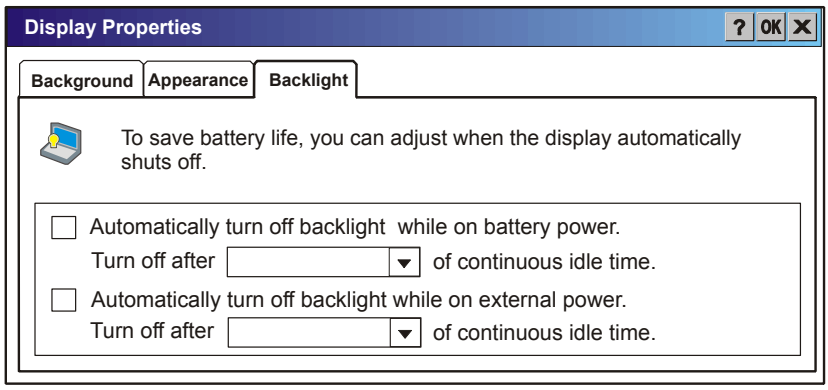


Figure 4-6 Display Properties / Backlight Tab

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. When the backlight timer expires, the monochrome screen is turned off, the color transmissive backlight is dimmed not turned off.

Input Panel

Access: **Start | Settings | Control Panel | Input Panel**

Select the current key / data input method.

Factory Default Settings	
Input Method	Keyboard
Allow applications to change input panel state	Disabled
Keys	Small keys
Use gestures	Disabled

Use this option to make the Soft Keyboard or the integrated keypad primarily available when entering data. Selecting Keyboard enables both.

Enable the input panel by checking "Allow applications to change the input panel's state". Then tap the OK button. Warmboot the device to store the changed setting.

Internet Options

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

Set General, Connection, Security and Advanced options for internet connectivity.

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Advanced	
Display web images	Enabled
Play web sounds	Enabled
Enable web scripting	Enabled
Display script error note	Disabled
Underline links	Never

Select a tab. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Keyboard

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

Set key repeat delay and key repeat rate.

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key Map	0409

There is no change from general desktop PC Keyboard Properties options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

When new key maps are added to the registry, they will appear in the Key Map dropdown list on the Keyboard Panel.

These values do not affect virtual keyboard taps.

Mixer

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

Adjust the volume, record gain, and sidetone for microphone input.

Factory Default Settings	
Master Volume	0dB
Record Gain	22.5dB
Sidetone	12.0dB
Input	None

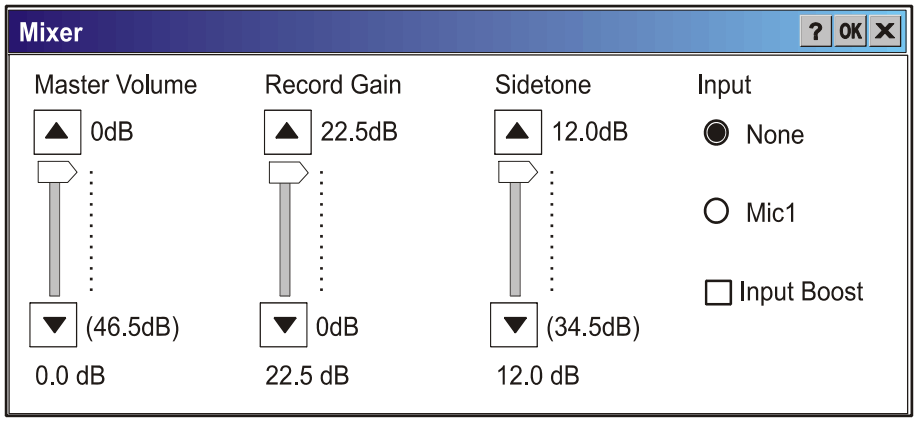


Figure 4-7 Mixer

Select the Input for the mixer. Move the sliders to adjust the decibel level. Tap OK to save the settings.

Mouse

Access: **Start | Settings | Control Panel | Mouse**

Set the double-tap sensitivity for stylus taps on the touchscreen.

Network and Dialup Connections

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

Create a dialup, direct, or VPN connection on the mobile device.

Create a Connection Option

1. On the mobile device, select **Start | 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 (IR @ 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 90 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 **Start | Settings | Control Panel | PC Connection** and tap the **Change** 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-clicking 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: **Start | Settings | Control Panel | Owner Icon**

Set mobile device owner details.

Factory Default Settings	
Identification	Blank
Notes	Blank

There is no change from general desktop PC Owner Properties display. Enter the information and tap the OK box to save the changes. The changes take effect immediately.

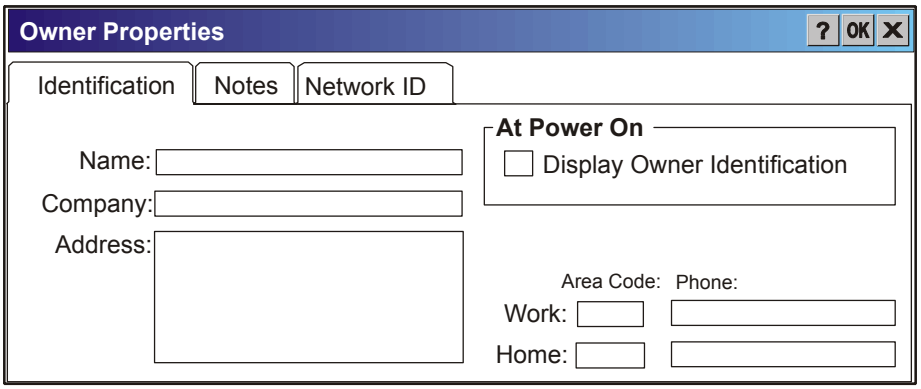


Figure 4-8 Owner Properties

Password

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

Set user access and power up password properties.

Factory Default Settings	
Password	Blank
At Power On	Disabled

Note: Once a password is assigned, each Control Panel option requires the password be entered before the Control Panel option can be accessed. If you forget the password, it cannot be restored without performing a cold boot on the unit (which erases all memory).

Enter the password, then type it again to confirm it and tap the OK box to save the changes. The password is immediately in effect.

Tap the Power On checkbox to set whether the user types a password at Power On.

Tap the Screen Saver checkbox to set whether the user types a password to clear the screensaver. If there is no screensaver chosen, this checkbox is ignored.

Note: Screensavers are not installed by LXE.

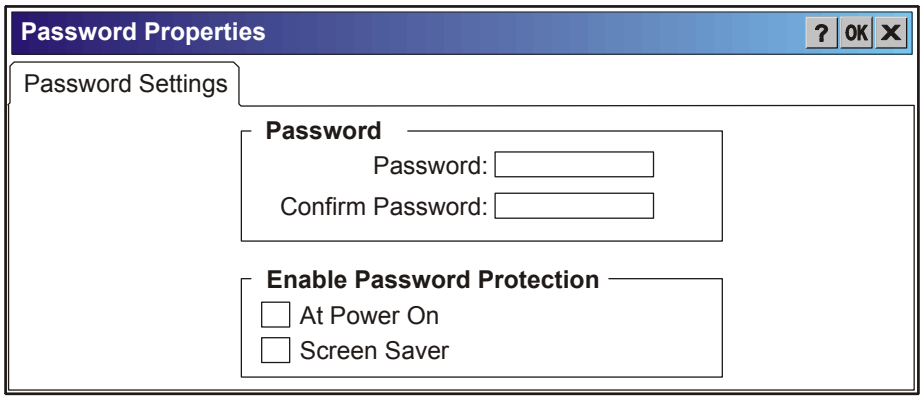


Figure 4-9 Password Properties

PC Connection

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

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

Factory Default Settings	
Allow Connection	Enabled
Connect Using	'USB Client'

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

Unchecking the "Allow connection with ….." disables ActiveSync.

Change ….

Tapping the Change button shows a list of configured ActiveSync connections. In addition, there is a checkbox for Automatic Connect. If this checkbox is checked, when the serial driver detects a cable connection on the configured port, it will automatically try to start ActiveSync on that port. Note that this interferes with processes on the configured port at the same time.

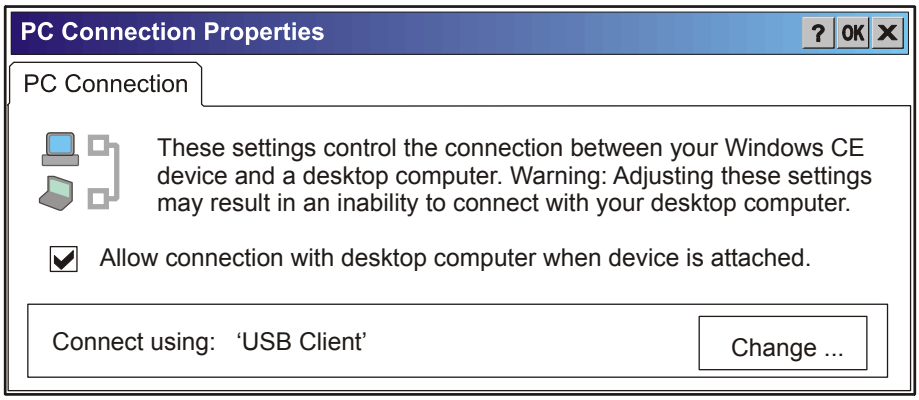


Figure 4-10 Communication / PC Connection Tab

Please refer to the "Backup Data Files using ActiveSync" section later in this chapter for parameter setting recommendations.

PCMCIA

Access: **Start | Settings | Control Panel | PCMCIA**

Note: Radio card in Slot 0, Internal ATA in Slot 2.

Factory Default Settings	
Slot 0	**PCMCIA**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off
Slot 1	**Compact Flash**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off
Slot 2	**ATA Card**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off

The name of the card (from the CIS data on the card) in the slot is displayed. This information cannot be changed by the user.

When “Power slot during sleep” is checked, the slot will stay powered up in Suspend at the cost of reduced battery life.

When “Disable slot now” is checked, the slot is powered down as soon as the Control Panel is closed and the PCMCIA driver ignores any card in the slot.

Power

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

Set Power Off, Backlight properties. Review battery status and perform backup battery charging/discharging.

Note: Control Panel parameters established in Power Properties affect the mobile device operating system. Power Management settings in the RFID Configuration utility governs power management of the RFID reader only.

Factory Default Settings	
Battery	N/A
Schemes – Battery Power	
User Idle	3 seconds
System Idle	15 seconds
Suspend	5 minutes
Schemes – AC Power	
User Idle	2 minutes
System Idle	2 minutes
Suspend	5 minutes

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

Battery

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

Schemes

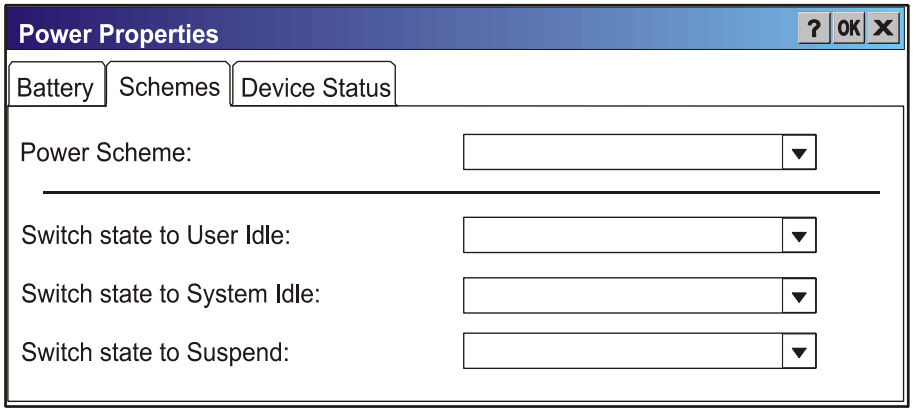


Figure 4-11 Power Schemes

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Battery Power Scheme

Use this option when the 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 device will be running on external power (e.g. AC adapter, auto outlet adapter, 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

Device Status

This option displays the power levels being used by the mobile devices.

Regional Settings

Access: **Start | Settings | Control Panel | Regional Settings**

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

No change from general desktop PC Regional Settings Properties options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Factory Default Settings	
Regional Setting	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

Remove Programs

Access: **Start | Settings | Control Panel | Remove Programs**

No change from general desktop Remove Programs options. Select a program and tap Remove. Follow the prompts on the screen to uninstall ***user-installed only*** programs. The change takes effect immediately.

Scanner

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

Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.

See Chapter 5 "MX3-RFID" for RFID Scanner applet screens.

Factory Default Settings	
Main	
Port 1	Internal
Port 2	Disabled
Power Port 1 while asleep	Disabled
Send key messages WEDGE	Enabled
Keys	
Left	Scan
Right	Enter
COM Ports (COM1- COM2 – COM3)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	8
Power on Pin 9	Off
-- With RFID Module --	
Main	
Port 1	COM1 Internal
Port 2	RFID Internal
Keys	
Left	Scan
Right	RFID
COM Ports (COM1- COM2 – COM3)	
COM1	115200bps, 8 data bits, no parity, 1 stop bit
COM2	38400bps, 8 data bits, no parity, 1 stop bit
COM3	38400bps, 8 data bits, no parity, 1 stop bit
Power on Pin 9	Enabled

Notes:

If the internal scanner has to be configured to operate at any communication settings other than 9600, N, 8, 1 and the computer either loses power or a cold boot command is entered, the Scanner applet must be reconfigured to match the scanner communication settings.

ActiveSync will not work over a COM port if that COM port is enabled in the Scanner applet as a scanner input. For example, if COM 1 is being used by the scanner, COM 1 can't be used by any other program.

When the RFID module is not installed, the RFID option is greyed out. See Chapter 5 "MX3-RFID" for instruction when using the RFID reader.

When the RFID module is installed, the barcode scanner won't function while the RFID reader is attempting to read. The RFID reader won't function until the barcode scanner completes the read / accept or reject process.

Main

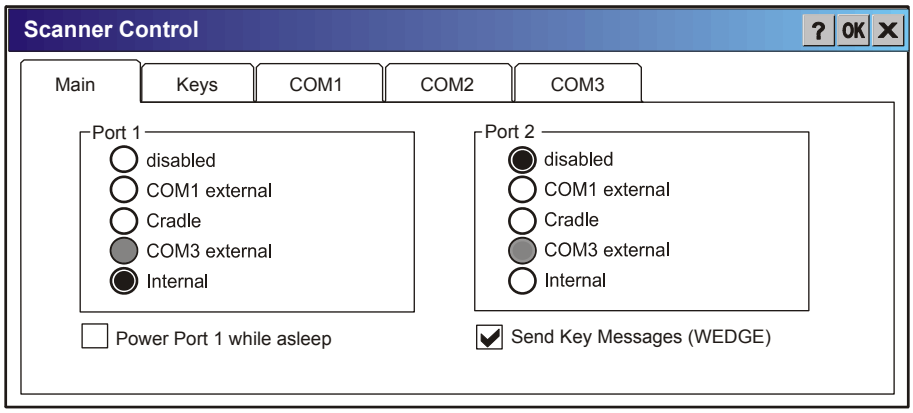


Figure 4-12 Scanner Properties / Main Tab

See Chapter 5 "MX3-RFID" when using the RFID Module.

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

If "Power Port 1 while asleep" is checked, whichever serial port is enabled as Port 1 will remain powered while the device is in Suspend, at the cost of reduced battery life. This allows a tethered scanner to wake the device by pressing the trigger on the scanner.

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".

The Scan buttons have no effect on tethered external scanners connected to the RS232 connector on the endcap.

Keys

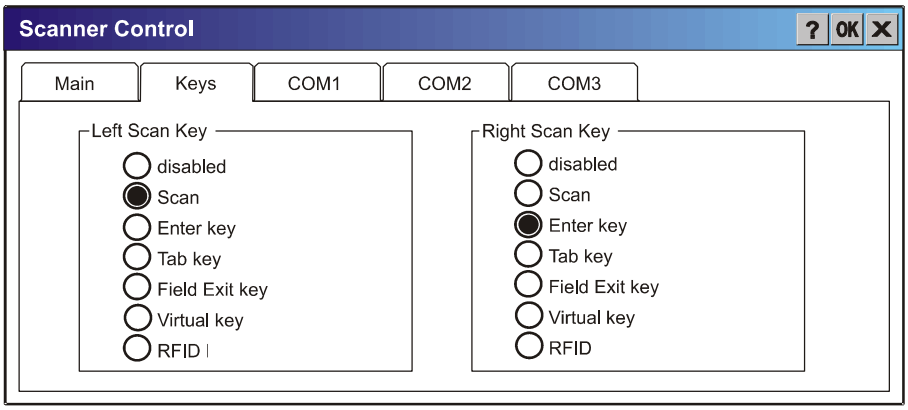


Figure 4-13 Scanner Properties / Keys Tab

See Chapter 5 "MX3-RFID" when using the RFID Module.

The Keys tab sets up what happens when one of the Scan keys are pressed. Note that the two keys can do the same or different functions.

Assigned	Function
Disabled	When either scan key is set to Disabled, it does nothing when pressed.
Scan	When set to "Scan" the integrated scanner is activated. If no integrated scanner is present, the Scan selection is greyed out. See Chapter 5 "MX3-RFID". When using the RFID module, the Scan key defaults to the Left Scan button.
Enter	When set to "Enter", both the Enter key and the (Scan button) / Enter key perform the same function.
Tab	When set to "Tab", both the Tab key and the (Scan button) / Tab key perform the same function.
Field Exit	**5250 devices only**. When a Scan key is set to "Field Exit", the key press causes the cursor to exit an input field. A field exit key press functions as a Pause key press on non-5250 devices.
Virtual	When set to "Virtual", the Virtual Left scan key produces an F20 and the Virtual Right scan key produces an F21.
RFID	When enabled, the Right Scan / Left Scan key functions as the RFID tag reader trigger. See Chapter 5 "MX3-RFID".

Change a Virtual Key (F20 or F21) Value

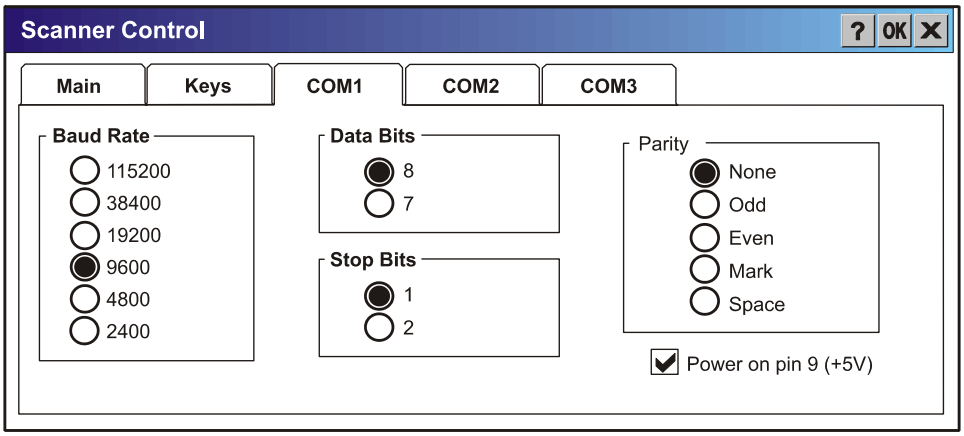
Modify the Registry using the Registry Editor (see section titled "Utilities"). LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

Set either the ScanCodeLeft or ScanCodeRight to be the scan code of the key to be used as the virtual key when the Virtual Left key (Left Scan key) or Virtual Right key (Right Scan key) is pressed. The registry requires a decimal value.

COM Ports

Do not connect a tethered scanner to the USB labelled ports:



COM1, COM2 and COM3 Panel Options are Identical.
The top baud rate when there is *no RFID module* is 38400.

Figure 4-14 Scanner Properties / COM Port Settings

See Chapter 5 "MX3-RFID" when using the RFID Module.

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

The COM 1 display contains the same parameters as the COM 2 and COM 3 Tab.

"Power on Pin 9" on the COM2 panel is disabled.

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Storage Manager

Access: **Start | Settings | Control Panel | Storage Manager**

Installed storage devices are listed by device name in the dropdown box. To view information about the disk or perform store operations, select a device from the list.

On-line help is available for this option.

- Topics available are:
  - Manage storage devices
  - Manage disk partitions
  - Creating a new partition
  - Advanced partition features

LXE recommends **caution** when formatting or dismounting storage devices and when creating new partitions or deleting partitions on the storage device.

Note: Contact LXE Customer Support prior to using management functions on the internal ATA card.

Stylus

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

Set double-tap sensitivity properties and/or calibrate the touch panel.

Double Tap

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

Calibration

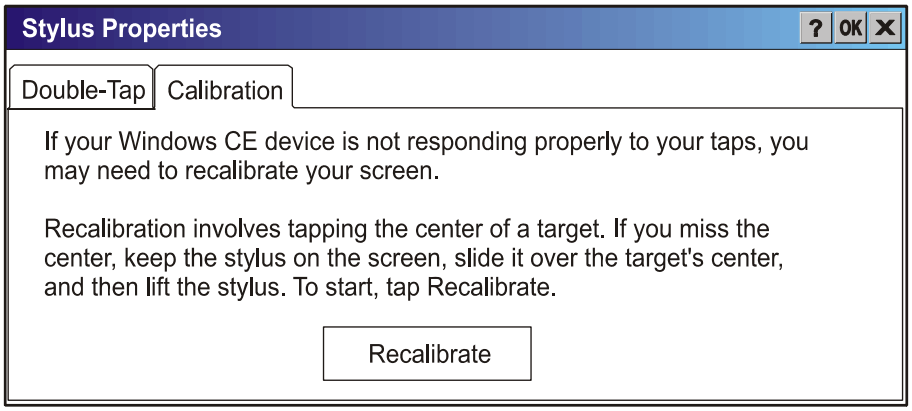


Figure 4-15 Stylus Properties / Recalibration Start

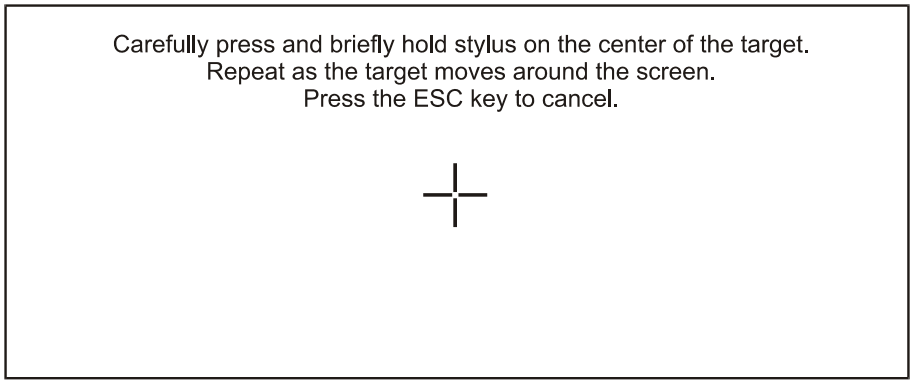


Figure 4-16 Stylus Properties / Recalibration

System

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

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

Factory Default Settings	
General	N/A
Memory	Middle of Memory Bar
Device Name	MX3X001
Device Description	LXE MX3X
Copyrights	N/A

Persist RAM Base Files

"Desktop"
"Favorites"
"Fonts"
"Help"
"Programs"

If you create a directory or directories with the above listed names in the "\System" folder (which is on the CF ATA card) and place your files in those directories, the Launch utility will automatically copy all of the files in these directories to the respective RAM base folders every time upon warm boot.

General

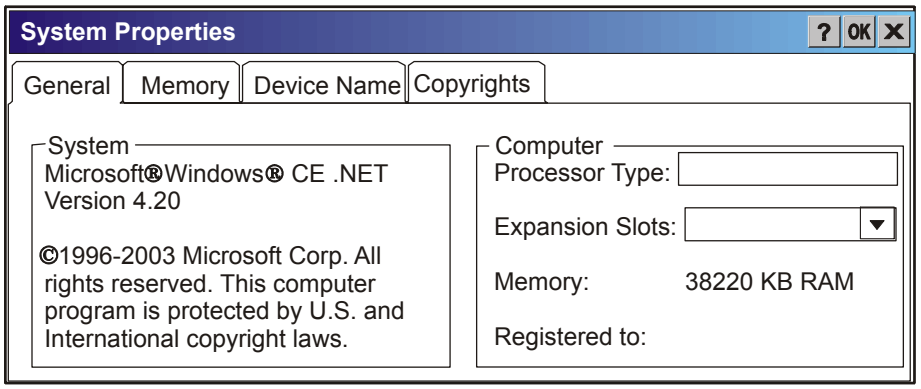


Figure 4-17 System / General tab

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. The name of the installed radio card is listed in the dropdown list. 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 64 MB may only report 35 MB memory, since 29 MB is used up by the Windows CE .NET operating system. This is actual DRAM memory, and does not include internal flash or the internal ATA card used for storage.

Memory

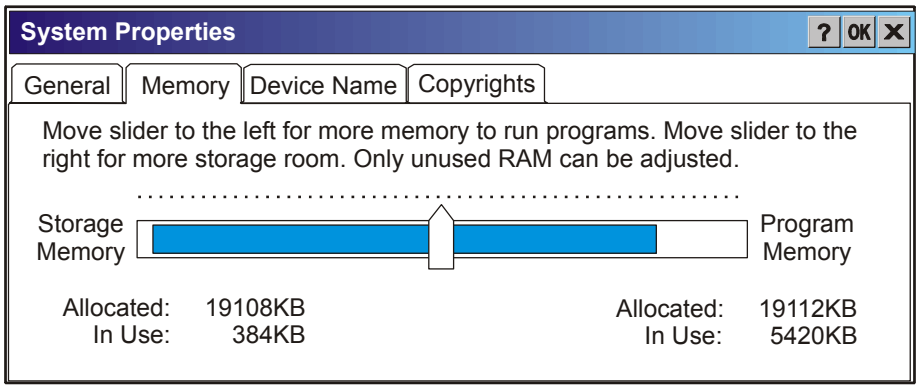


Figure 4-18 System / Memory

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 mobile device is running slowly, try increasing the amount of program memory. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Device Name

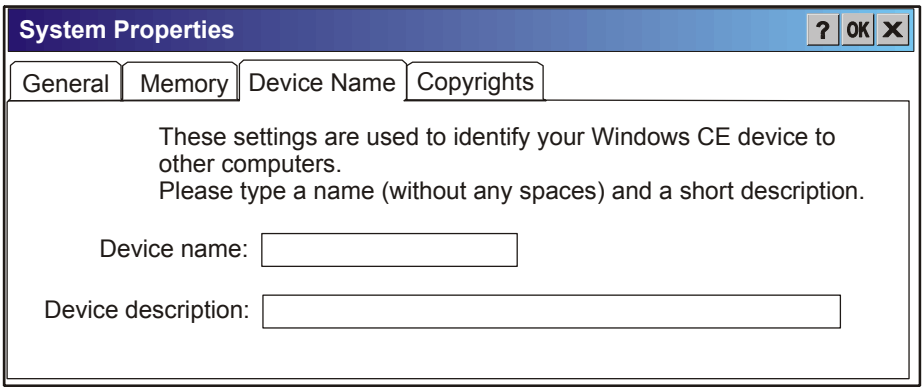


Figure 4-19 System / Device Name

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

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

Volume and Sounds

Access: **Start | Settings | Control Panel | Volume & Sounds Icon**

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

Factory Default Settings	
Volume	
Events	Enabled
Application	Enabled
Notifications	Enabled
Volume	Middle of Bar
Key click	Loud
Screen tap	Loud
Sounds	
Scheme	LOUD!

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

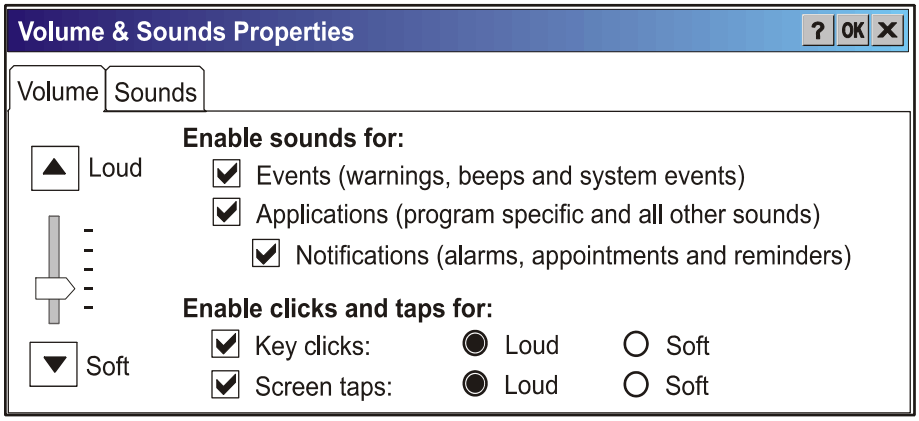


Figure 4-20 Volume and Sounds

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.

Utilities

These utilities are pre-loaded by LXE.

LAUNCH.EXE

All applications to be installed into persistent memory are normally in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and need to be copied to the mobile device using an internal ATA card or from a PC using ActiveSync. The CAB files are loaded into the folder **System**, which is the internal ATA 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.

3 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 (only on **.01D** or newer images).

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 [2]:

```
; Cisco radio
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Cisco Radio]
"FileName"="\SYSTEM\CISCO.CAB"
"FileCheck"="\WINDOWS\CISCO.DLL"
“Order”=dword:01
“PCMCIA”=dword:1

; Symbol radio
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Symbol Radio]
"FileName"="\SYSTEM\SYMBOL.CAB"
"FileCheck"="\WINDOWS\NICTT.EXE"
“Order”=dword:01
“PCMCIA”=dword:1

; this key installs RFID drivers/default values from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFID]
"FileName"="\WINDOWS\RFID.CAB"
"FileCheck"="\WINDOWS\RFID_WDG.DLL"
“Order”=dword:0C

; this key installs RFTERM from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
"FileName"="\SYSTEM\RFTERM.CAB"
"FileCheck"="\WINDOWS\LXE\RFTERM.EXE"
“Order”=dword:10

; this key installs JAVA
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Java]
"FileName"="\SYSTEM\JEODE.CAB"
"FileCheck"="\WINDOWS\EVM.EXE"
“Order”=dword:30

; this key runs RFTERM as a startup app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
"FileName"="\WINDOWS\LXE\RFTERM.EXE"
"FileCheck"="dummy"
“Order”=dword:40

; this key installs APPLOCK from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockInstall]
"FileName"="\SYSTEM\APPLOCK.CAB"
"FileCheck"="\WINDOWS\APPLOCK.EXE"
“Order”=dword:0
```

[2] 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.

```
        ; this key runs the APPLOCK prep app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockPrep]
        "FileName"="\WINDOWS\APPLOCKPREP.EXE"
        "FileCheck"="\dummy"
        “Order”=dword:1

        ; this key runs the APPLOCK main app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLock]
        "FileName"="\WINDOWS\APPLOCK.EXE"
        "FileCheck"="\dummy"
        “Order”=dword:63

        ; Autoexec
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AUTOEXEC]
        "FileName"="\SYSTEM\AUTOEXEC.BAT"
        "FileCheck"="dummy"
        “Order”=dword:50

        ; Avalanche
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
        "FileName"="\SYSTEM\LXEAVA.CAB"
        "FileCheck"="\SYSTEM\AVALANCHE\MODEL.DAT"
        "Order"=dword:4
        "Installed"=dword:0
        "PCMCIA"=dword:0
        "Delay"=dword:0

        ; Avalanche
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
        "FileName"="\SYSTEM\AVALANCHE\AVAINIT.EXE"
        "FileCheck"="dummy"
        “Order”=dword:5
        "Delay"=dword:0
        "PCMCIA"=dword:0
        "Installed"=dword:0
```

When you are installing your custom CAB file to the mobile device’s operating sytem, 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 ATA card). This is parsed by the Launch utility, and these programs are started or executed. Note that this only works on images from **.01D** and newer.

REGEDIT.EXE

Pocket Registry Editor - part of Microsoft Power Tools for Windows CE. LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

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.

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).

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

API Calls

See Also: LXE CE API Programming Guide E-SW-WINAPIPG

The LXE CE API Programming Guide documents only the LXE-specific API calls for the mobile device. It is intended as an addition to the standard Microsoft Windows CE API documentation. Details of many of the calls in the LXE guide may be found in Microsoft's documentation.

The APIs documented in the programming guide are included in the file LXEAPI.DLL, which is in the standard Windows CE image on the mobile device.

For ease of software development, the files LXEAPI.H and LXEAPI.LIB are available on the accessories CD, which are the C/C++ include files and the link library for the DLL, respectively. Note that this DLL is installed in mobile device images with a version number of 1.2 or higher (as displayed on the screen during bootup).

A full SDK is now included for Microsoft Embedded Visual C++ 4.0 (which is available free on the Microsoft website).

See Also: "RFID Driver APIs" in Chapter 5 "MX3-RFID".

Reflash the Mobile Device

Note: When reflashing, LXE recommends using a Compact Flash card that is greater than 64MB. Files to be loaded on the CF card are: NK.BIN, EBOOT.NB0, XSCALE.BIT

Requirement: A screwdriver (not supplied by LXE)

Preparation

- LXE recommends that installation of the CF card be performed on a clean, well-lit surface.
- Remove the screws on the endcap and slide the endcap to the side, being very careful not to disconnect the ribbon cables, damage the leads to the external power jack, the headphone jack or the antenna. The antenna may be taped to the endcap so great care must be taken when loosening the endcap.
- Carefully remove or loosen all cables to an existing CF card. Remove the CF card.

How To

1. Place the compact flash card with new image files on it in the right hand slot.
2. Double-tap **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Double-tap **System Folder**.
5. Select **Edit | Paste**. When asked "Overwrite ?", tap **Yes to All**.
6. When the copy process finishes, remove the CF card.
7. Select **Start | Run** and type **Coldboot**.
8. Before the splash screen appears, press and hold down the <A> key. Continue to hold it down until the displays shows "Writing to boot flash".

   Note: If you do not press and hold the <A> key quickly enough, the display shows "Loading OS Image". Remove the main battery for 2 seconds, re-insert the battery and press the Power button. Press and hold the <A> key again.
9. The mobile device will automatically reboot after flashing the bootloader. "Loading OS Image" is displayed on the screen and when the new OS finishes loading, all software upgrades are complete.
10. Replace the endcap, being careful not to pinch any leads or cables. The touchscreen will need to be re-calibrated.

Once the bootloader is loaded and the files are copied onto the internal ATA drive, you can reflash the bootloader at any time by rebooting the MX3X, and holding down the <A> key on the keypad before the splash screen appears. Wait until the splash screen displays "Writing new bootloader", and you can release the <A> key. When complete (3-5 seconds), the MX3X will reboot and startup with the new bootloader again.

Clearing Persistent Storage

Cold boot sets all registry settings back to LXE factory defaults. No other clearing is available or necessary.

Chapter 5 MX3-RFID

Introduction

Figure 5-1 MX3-RFID Device

Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify individual items. The individual items identified/read by a RFID reader contain a tag (also known as an electronic label or transponder). Unlike barcodes that must be read by a beam passing over the barcode, RFID tags do not have to be in the line-of-sight of the reader before the reader can collect the data from the tag but they do need to be within the established "read" distance from the RFID module.

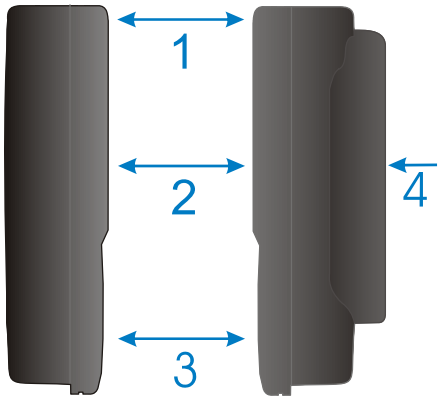
Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

When the RFID Read button is pressed, the tag reader turns on and the MX3-RFID beeps once if the tag (or tags) was located and read successfully. The reader turns off at a predetermined time limit after a good read or a failed read. The data gathered from the tag is sent to a user-specified storage area (i.e. open text file) for further handling e.g. sent to the host using wired or wireless networking. See the section titled "How To" for instruction.

There may be a buzz sound during the time the reader is "searching and reading" if the RFID reader is configured to buzz during a read cycle.

Note: The RFID Module also has a hand strap. Location and attach points are different from the standard MX3X hand strap. MX3-RFID devices are shipped with the hand strap already installed. The MX3-RFID does not fit the Hip-Flip accessory. ***The hip-flip is not to be used with the MX3-RFID device****. The MX3-RFID does not fit in the MX3 powered cradles. A passive docking cradle is available for the MX3-RFID device (see "Accessories").*

MX3X vs MX3-RFID Chart



MX3X MX3-RFID

1 Endcap

2 Touchscreen

3 Keypad

4 RFID Module

MX3-RFID Capability/Function	MX3-RFID
Integrated Scanner port (SE923 short range)	x
RFID Reader	x
USB Client RS232 port	x
Cisco 802.11b Radio and RFID	x
Passive Cradle	x
Intel XScaleTM PXA255 400MHz CPU	x
128M Flash / 128M RAM or greater	x
Windows CE .NET 4.2	x
AppLock / RFTerm / Barcode Wedge	x
JAVA support	x
63 Key QWERTY Keypad, two large user mappable scan keys	x
640 x 240 1/2 VGA LCD 6" diagonal - color	x
Touchscreen and stylus	x
10.8V, 2200mAh Li-Ion battery pack	x
IR Port	x
Handstrap	x
Holster	x
IP55	x
Available in US and Canada	x

MX3-RFID Endcap Options

Left Port	Right Port
Laser Scanner	USB Client

Specifically the assignment of the serial ports is as follows:

- COM1 for the RFID module.
- COM3 for either the integrated barcode scanner or an RS232 port.

RFID Reader Scan Range

Type of Tag	Scan Range
Class 0 Tag	2 feet / .7 meters
Class 1 Tag	3 feet / .9 meters

Figure 5-2 RFID Tag Reading Ranges

Unlike barcode scanners that require line-of-sight before successfully reading a barcode, the RFID reader does not require line-of-sight when searching for and reading tags. Pressing the RFID Read button on the MX3-RFID starts a 360 degree search “beam” that stops at the limits of the scan range of the RFID reader. The “beam” stops searching when the read timer expires.

RFID Device and LXE Cradles

The MX3-RFID module is too bulky to fit in the standard MX3 powered cradles. There is a passive vehicle cradle available for the MX3-RFID device that secures the device to the cradle only. See section titled “Accessories”.

Main battery charging and host communication is not available through the passive vehicle cradle. The passive vehicle cradle does not have LEDs or indicators. It does not accept DC power connection.

The MX3-RFID can be connected to DC Power while secured in the passive vehicle cradle. It can also communicate wirelessly with the host while in the passive vehicle cradle.

How To …

1. Set RFID tag read parameters using **Start | Settings | Control Panel | RFID**.
2. Set Scanner properties using **Start | Settings | Control Panel | Scanner**.
3. Open the application or text file that is to gather the data read from tags.
4. Place the MX3-RFID within the boundary parameters of the tag to be read. See “RFID Reader Scan Range”.
5. Press the RFID Read button.
6. The data gathered from the tag is sent to the open file.
7. Save the file. The tag read data is ready for further processing.

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

Note: Any tag data retrieved and not saved is lost during a reboot or reset.

Scanner Properties Settings

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

When the mobile device with an installed RFID module powers up, the following scanner and RFID parameters are automatically set:

Factory Default Settings	
--- With RFID Module ---	
Main	
Port 1	Internal
Port 2	RFID Internal
Power Port 1	Disabled
Wedge	Enabled
Keys	
Left	Scan
Right	RFID
COM Ports (COM1- COM2 – COM3)	
COM1	115200bps, 8 data bits, no parity, 1 stop bit
COM2	38400bps, 8 data bits, no parity, 1 stop bit
COM3	38400bps, 8 data bits, no parity, 1 stop bit
Power on Pin 9	Enabled on COM1 only

Power on Pin 9 is automatically enabled and greyed out to keep it enabled.

When the RFID module is installed, the laser barcode scanner won't activate while the RFID reader is attempting to read. The laser scan key can be pressed after the RFID reader has completed the read function.

The RFID reader won't function until the barcode scanner completes the barcode read / accept or reject process. The RFID read key can be pressed after the laser reader has completed the barcode read / accept or reject process.

Main

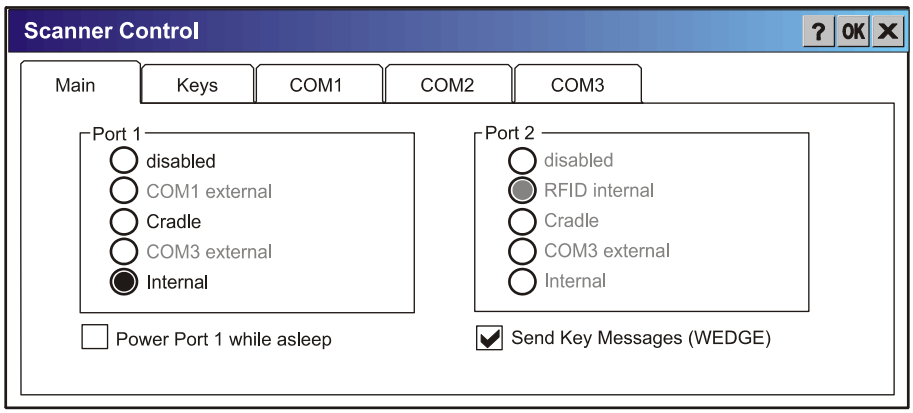


Figure 5-3 Scanner Properties / Main Tab

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Keys

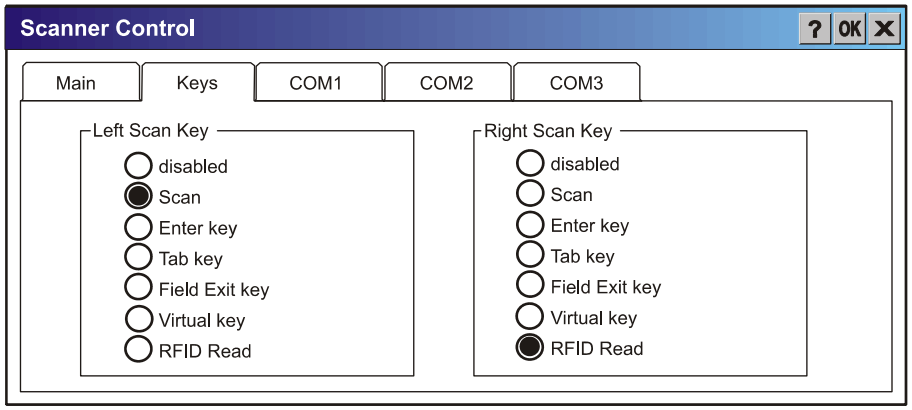
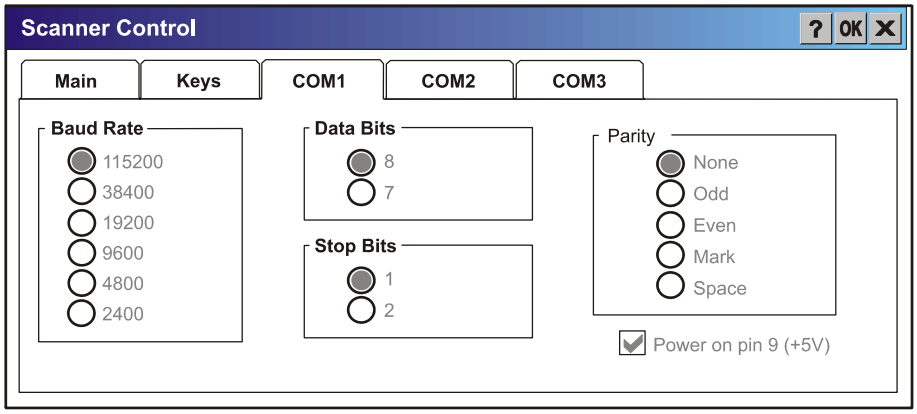


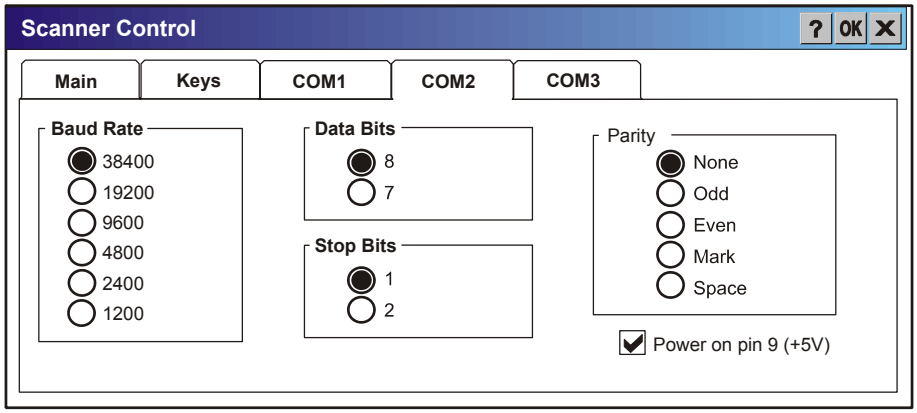
Figure 5-4 Scanner Properties / Keys Tab

The Keys tab sets up what happens when one of the Scan keys are pressed. Note that the two keys can do the same or different functions.

Assigned	Function
Disabled	When either scan key is set to Disabled, it does nothing when pressed.
Scan	When set to “Scan” the integrated scanner is activated. If no integrated scanner is present, the Scan selection is greyed out.
Enter	When set to “Enter”, both the Enter key and the (Scan button) / Enter key perform the same function.
Tab	When set to “Tab”, both the Tab key and the (Scan button) / Tab key perform the same function.
Field Exit	**5250 devices only**. When a Scan key is set to “Field Exit”, the key press causes the cursor to exit an input field. A field exit key press functions as a Pause key press on non-5250 devices.
Virtual	When set to “Virtual”, the Virtual Left scan key produces an F20 and the Virtual Right scan key produces an F21.
RFID	When selected, the Left Scan or Right Scan keys function as RFID module read triggers.

COM Ports





COM2 and COM3 Panel Default Settings are Identical

Figure 5-5 Scanner Properties / COM Port Settings

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

The COM 1 figure above displays the default settings for the MX3-RFID device.

COM 2 and COM 3 default settings are identical. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

RFID Configuration Utility

Access: **Start | Settings | Control Panel | RFID**

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

Note: Any tag data retrieved and not saved is lost during a reboot or reset.

There are two versions of the RFID Configuration Utility. The version presented in this chapter supersedes the version described in earlier revisions of this reference guide. Contact your LXE representative for availability of the RFID CAB file.

Factory Default Settings	
Tags	
Tag Types to Read – Class 0	Enabled
Class 0 Tag Read Attempts	4
Tag Types to Read – Class 1	Enabled
Class 1 Tag Read Attempts	1
Class 0 Singulation	ID 2
Preamble	Blank
Postamble	Blank
Separator	^M^J
Filters	
Select	Blank
Field Name	Blank
Offset	Blank
Mask Value	Blank
Read	
Read Once on Key Press	Enabled
Read Continuous on Key Press	Disabled
Toggle On/Off with Key Press	Disabled
Beep Once on Tag Read	Enabled
Buzz during Read Cycle	Enabled
Send Key Messages (Wedge)	Enabled
Power	
Output Power	+30 dBm
Modulation	95%
Power Management	3 sec
Disable	Disabled
Firmware	
File	Blank
Format	
HEX	Enabled
EPC	Disabled
Field Separator	Blank

See Also: “Set the Display Backlight Timer”, “Set the Power Schemes Timers”, and “Set the Audio Speaker Volume”.

Tags

Access: **Start | Settings | Control Panel | RFID | Tags tab**

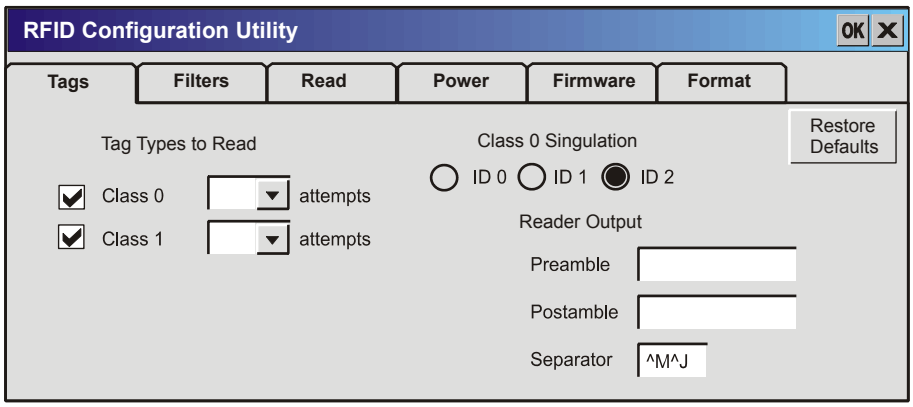


Figure 5-6 RFID Configuration Utility – Tags tab

Note: MX3-RFID is restricted to 95% for Modulation. LXE recommends using the default setting of ID2 for Class 0 Singulation.

Data output from tags read is sent in character mode to the keyboard buffer. A pop up option box is displayed if the user attempts to deselect both Class 0 and Class 1 tags. At least one class must be selected before the user can continue.

Tap the Restore Defaults button to set the parameters in the RFID Configuration Utility menu panels to their factory default settings.

Tag Types to Read

Specify which class of tags are to be read and reported during tag reading operations. Duplicate tags are not reported.

- Class 0 (Class 0 Read attempts)
- Class 1 (Class 1 Read attempts)

Class 0 and Instant tags are more difficult to read. For this reason, a read operation can contain a user-defined number of read attempts. The default for Class 0 tags is 4 read attempts. This means that when a read operation is performed by pressing the RFID Read button, 4 reads will be performed internally; the results merged, duplicate tags removed, and the result is then made available to the application.

Default number of reads for collecting Class 0 tags is 4. Valid values are between 1 and 10.

Default number of reads for collecting Class 1 tags is 1. Valid values are between 1 and 10.

Change the attempts value by tapping the drop down list box and selecting a number from the list. Tap OK to save the change or X to ignore the change and return to the Control Panel.

Class 0 Singulation

Tap the radio button to specify which singulation method to use during Class 0 read operations. Selection is grayed out if the Class 0 Tag Type is unchecked. Tap OK to save the change or X to ignore the change and return to the Control Panel.

Reader Output

Preamble	A preamble is a lead-in character for tags transmitted to the host device. The lead-in characters are considered part of the tag. The Preamble field will accept up to 5 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters.
Postamble	A postamble is a follow-on character for tags transmitted to the host device. The follow-on characters are considered part of the tag. The Postamble field will accept up to 5 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters.
TAG data separators	Use data separators to add spacing between read tags. Up to 2 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters. For example, ^M^J places a carriage return (^M) and line feed (^J) after each tag is successfully read.

When the maximum number of characters is exceeded, the mobile device beeps and will not allow more characters to be entered. However, “hat” encoded characters count as a single character in determining the number of characters entered into the field. Tap OK to save the change or X to ignore the change and return to the Control Panel.

See Also: “Hat Encoding”.

Filters

Access: **Start | Settings| Control Panel | RFID | Filters tab**

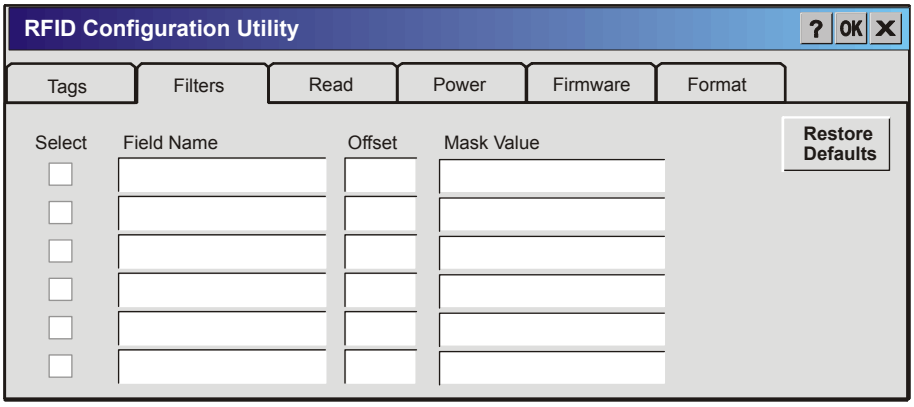


Figure 5-7 RFID Configuration Utility – Filters tab

Tap the Restore Defaults button to set the parameters in the Filters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Parameters

Default value for all parameters is blank. Tags read and reported are filtered through a logical OR of the selected mask values.

Select	Toggles between a blank and a checkmark. A checkmark in this field allows the filter on that line to be active at the next and subsequent tag read action.
Field Name	The user-friendly name for the filter. Accepts up to 40 alphanumeric characters. Field is not case sensitive. Duplicate field names are allowed between filters.
Offset	The number of characters that offset the mask value from the beginning of the tag. The range is from 0 to 23 (characters).
Mask Value	Accepts up to 24 hexadecimal characters. Field is not case sensitive. Duplicate mask values are allowed between filters. When filtering EPC decoded tags, the filter is applied before the tag is converted to EPC.

When the maximum number of characters is exceeded, the mobile device beeps and will not allow more characters to be entered.

See Also: “Decimal-Hexadecimal Chart”.

How to Set a Filter

Occasionally, it is desirable to see only a subset of tags; for example, when inventorying items from a specific company. In cases like this, filtering can be used to select only the desired tags.

1. To set up a filter, first enter a Field Name for the filter. The Field Name is simply a descriptive name that is used to distinguish the filter from other filters. In the example described previously, the Field Name could be the company name of the tags to be identified.
2. Next, enter the offset that the mask will be applied to in the Offset field. A mask value may be blank. When a blank mask value is selected as a filter it will return all tags read.
3. Then, enter the hexadecimal characters to search for in the Mask Value field.
4. Enable the filter by checking the Select field.

When the format of the tag data sent to the application is set to EPC, the filter is applied to the tag data before the conversion from hexadecimal notation to EPC format.

For example, suppose the following three tags exist:

- c80507a000819530
- c80507a00081a1df
- c80507a00081a985

Only the tags that end in “81a” are wanted.

Two filter examples to identify the “81a” tags might be:

Field Name	Offset	Mask Value
Filter 1	0	c80507a00081a
Filter 2	10	81a

Read

Access: **Start | Settings | Control Panel | RFID | Read tab**

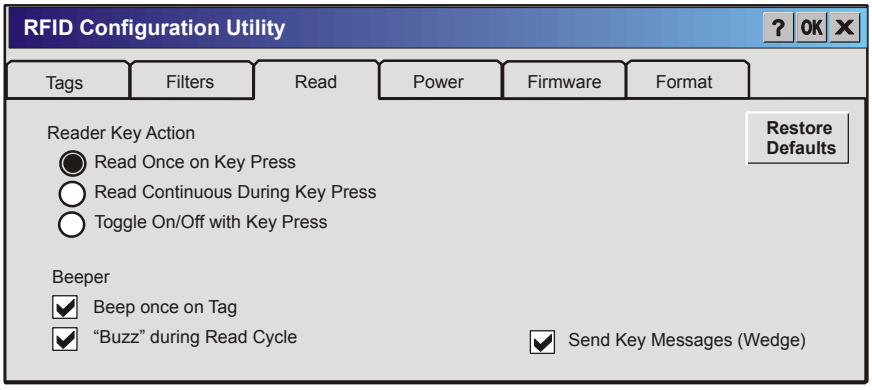


Figure 5-8 RFID Configuration Utility – Read tab

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Reader Key Action

When the "Toggle On/Off with key press" is enabled, the "'Buzz' during Read Cycle" check box is automatically enabled.

Read Once on Key Press

When the RFID Read button is pressed a single read operation is performed and the RFID reader waits for another key press. The operation reads class 0 tags and/or class 1 tags depending on whether the class was selected on the Tags tab. The read for each tag class consists of 1 or more internal read attempts as specified on the Tags tab.

Read Continuous During Key Press

When the RFID Read button is pressed, the MX3-RFID reads class 0 and/or class 1 tags repeatedly until the Read button is released. The operation continuously reads class 0 tags and/or class 1 tags depending on whether the class was selected on the Tags tab. The read for each tag class consists of continuous internal read attempts as specified on the Tags tab.

Toggle On/Off with Key Press

When the RFID Read button is pressed, the MX3-RFID reads class 0 and/or class 1 tags repeatedly. It continues to perform read operations after the Read button is released and does not stop reading until the Read button is pressed again. The Read operation is cancelled. The operation continuously reads class 0 tags and/or class 1 tags depending on whether the class was selected on the Tags tab.

Beeper

- Beep once on any successful read cycle (one or more Tags read)
- “Buzz” (continuous beeps) during Read Cycle.

Settings	Read Result	
	Tag(s) Read	No Tags Read
Beep On / Buzz On	Beep	Buzz
Beep On / Buzz Off	Beep	No sound
Beep Off / Buzz On	Buzz	Buzz
Beep Off / Buzz Off	No sound	No sound

Power

Access: **Start | Settings | Control Panel | RFID | Power tab**

Note: Control Panel parameters established in Power Properties affect the mobile device operating system. Power Management set using RFID Configuration governs power management of the RFID module only.

See Also: “Set the Power Schemes Timers”.

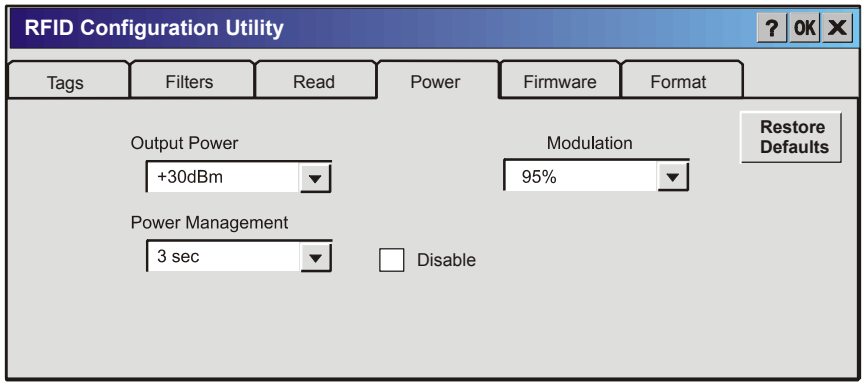


Figure 5-9 RFID Configuration Utility – Power tab

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Note: MX3-RFID is restricted to 95% for Modulation. LXE recommends using the default setting of ID2 for Class 0 Singulation.

Output Power

Provides configuration for the output power applied during Read (or Write) operations. The range is 16 settings from +15dBm to +30dBm.

Modulation

Provides configuration carrier modulation during Read (or Write) operations. The range is from 20% to 95% in 2.42% steps.

Power Management

The time out period sets the time that the software will change the RFID module state from Standby to Disable in order to reduce battery current consumption.

This timer expires if no reads have been requested for the specified period of time. The increments of the timer are 3 sec., 4 sec., 5 sec., 10 sec., 15 sec., 20 sec., 30 sec., 45 sec., 1 min., 2 min., 3 min., 4 min., 5 min., 6 min., 7 min., 8 min., 9 min., 10 min., 11 min., 12 min., 13 min., 14 min., and 15 minutes.

When the “Disable” check box is checked, then Power Management is disabled and the RFID module remains in the “Standby” state.

Firmware

Access: **Start | Settings | Control Panel | RFID | Firmware tab**

Select and install RFID firmware upgrades to the RFID module. The upgrade file is selected using standard Windows functions.

The currently loaded RFID firmware version is displayed. This value cannot be edited by the user.

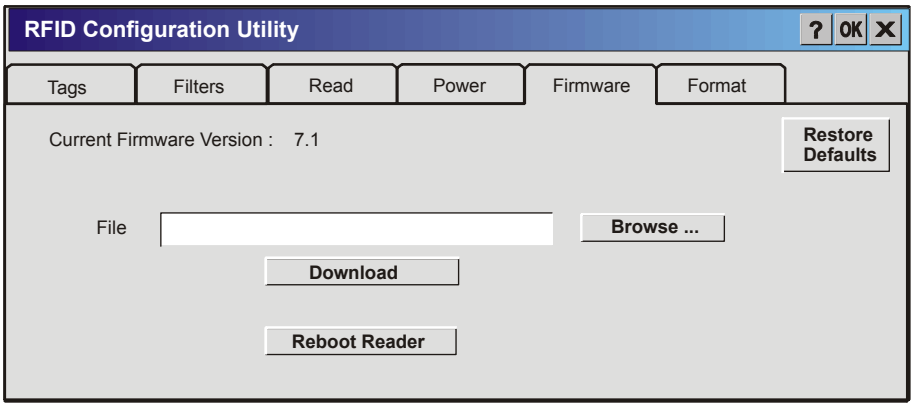


Figure 5-10 RFID Configuration Utility – Firmware tab

Note: RFID firmware upgrades and subsequent rebooting does not directly cause changes to any other MX3X firmware.

Tap the Restore Defaults button to set the parameters to their last saved default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Firmware Upgrade

Tap the Browse button to locate the Firmware Upgrade File on the mobile device to download to the RFID module. Tap OK in the File Open box to select the file.

Once selected, tap the Download button on the Firmware panel. The upgrade is installed.

When the upgrade process is complete, a pop up dialog box appears indicating a successful or unsuccessful upgrade.

Tap OK in the pop up dialog box to close the dialog box.

Reboot Reader

Tap the Reboot Reader button. The RFID Reader module reboots. The MX3X is not rebooted, only the RFID Reader is rebooted.

A pop up dialog box appears indicating a successful or unsuccessful reboot. The mobile device does not reboot.

Tap OK in the pop up dialog box to close the dialog box.

Format

Access: **Start | Settings | Control Panel | RFID | Format tab**

Use this option to select the output format that is sent to the open file from RFID read actions.

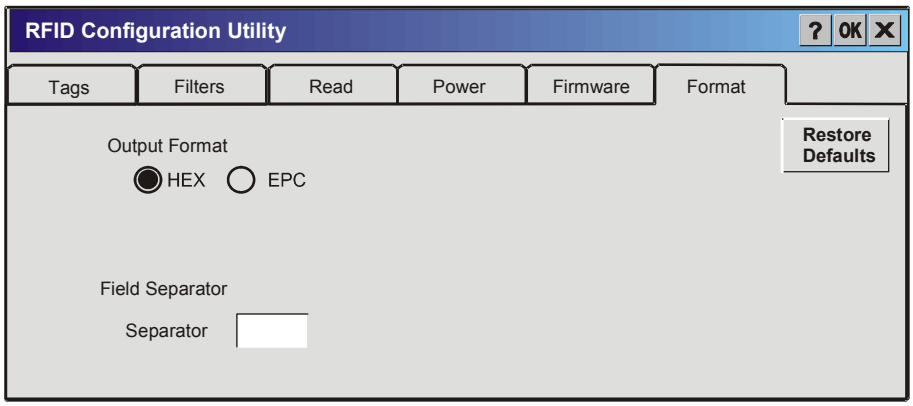


Figure 5-11 RFID Configuration Utility – Format tab

The default output format is HEX. When HEX is selected, the Separator text box is greyed out.

When EPC is selected, the user can enter a field separator to use between RFID tag read actions.

There are four EPC encoding schemes available:

- SGTIN-96
- SGTIN-64
- SSCC-64
- SSCC-96

Invalid or non-supported formats are represented in HEX digits that represent the bits of encoded data read from a tag. Select EPC to decode the HEX digits into EPC tag data standards.

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

RFID Driver APIs

For the development of applications to execute locally on the MX3-RFID device, API support for the functions described supplement the current MX3X APIs documented in the "LXE CE API Programming Guide" (available on the LXE Manuals CD or the LXE ServicePass website).

For ease of software development, the library file, RFIDAPI.LIB, and two header files, RFIDAPI.H and LXERFID.H, are available on the MX3X SDK CD (see "Accessories").

The following operations take place when a user presses a scan button mapped to an RFID Read command.

1. Scanner Wedge catches a Keyboard Event and determines that the key pressed is mapped to an "RFID Read" operation.
2. RFID Driver executes the READ command. Based on the "Tag Types to Read" setting (set through the LXE RFID Configuration Utility), the command calls either of the following: TAG_0_READ, TAG_1_READ, or both TAG_0_READ and TAG_1_READ.
3. The Reader receives an API call, performs an appropriate read, and returns tag data to the RFID Driver.
4. Based on the "Reader Output" settings (set through the LXE RFID Configuration Utility), the RFID Driver formats the tag data with a preamble, postamble, and separators.
5. RFID Driver populates the Keyboard Buffer with the formatted data output.

Formatted data is displayed in the foreground application window.

System Commands

NO_CHG	No Commands, RFIDchange (the system mode is not changed). Used to retrieve firmware version.

Class 0 Commands

KILL	*Kill Class 0 tag*
SET	Set read parameters (RF power level and Modulation depth)
READ	Read Class 0 tag IDs using parameters set by TAG_0_SET

Class 1 Commands

KILL	*Kill Class 1 tag*
SET	Set read parameters (RF power level and Modulation depth)
READ	Read Class 1 tag IDs using parameters set by TAG_1_SET
PROGRAM_ID	All Class 1 tags receiving this command will program the specified tag ID in memory

VERIFY_ID	All tags receiving this command will reply with their CRC, followed by their entire ID code, followed by their Password. A tag that has successfully executed the LOCK_ID command ignores the VERIFY_ID command.
LOCK_ID	This command prevents any further modification of the tag ID, CRC, and Password.
ERASE_ID	This command sets all bits of the tag ID, CRC, and Password to '0'. A tag that has successfully executed the LOCK_ID command ignores the ERASE_ID command
WRITE	Performs/combines Program_ID and Lock_ID

Data Format Commands

MASK_DEFINE	Allows definition of a set of six masks, each containing a Field Name, Offset, and Mask Value. Updates registry values.
MASK_READ	Reads Class 0 tags or Class 1 tags depending on the value passed in for TAG_TYPE parameter. Allows a maximum of six masks as an Input.
SET_PREAMBLE	Sets preamble for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)
SET_POSTAMBLE	Sets postamble for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)
SET_SEPARATOR	Sets tag separator for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)

Power Commands

READER_POWER_TIMEOUT	Sets the timeout for the Reader Power Management to kick in. When the driver is inactive for the specified time, it puts the reader into "Disabled" mode to conserve power.

Reader Feedback Commands

NOTIFY_READ_SUCCESS	Turn ON/OFF beep on a read operation that results in one or more tags read. See table below.
NOTIFY_READER_ON	Turn ON/OFF buzz on a read operation that does not produce a beep. See table below.

Settings	Read Result	
	Tag(s) Read	No Tags Read
Beep On / Buzz On	Beep	Buzz
Beep On / Buzz Off	Beep	No sound
Beep Off / Buzz On	Buzz	Buzz
Beep Off / Buzz Off	No sound	No sound

LXE RFID Get Data Commands

Get_Data	Returns the tag data acquired in the last RFID Read. WM_LXE_RFIDFULL message indicates that RFID Read is complete.
WM_LXE_RFIDFULL	Indicates that the RFID Read is complete.

Hat Encoding

The MX3-RFID supports only 7-bit hat encoding which means only ^@ through ^_ (underscore) are supported.

Desired ASCII	Hex Value	Hat Encoded
NUL	**00**	**^@**
SOH	**01**	**^A**
STX	**02**	**^B**
ETX	**03**	**^C**
EOT	**04**	**^D**
ENQ	**05**	**^E**
ACK	**06**	**^F**
BEL	**07**	**^G**
BS	**08**	**^H**
HT	**09**	**^I**
LF	**0A**	**^J**
VT	**0B**	**^K**
FF	**0C**	**^L**
CR	**0D**	**^M**
SO	**0E**	**^N**
SI	**0F**	**^O**
DLE	**10**	**^P**
DC1 (XON)	**11**	**^Q**
DC2	**12**	**^R**
DC3 (XOFF)	**13**	**^S**
DC4	**14**	**^T**
NAK	**15**	**^U**
SYN	**16**	**^V**
ETB	**17**	**^W**
CAN	**18**	**^X**
EM	**19**	**^Y**
SUB	**1A**	**^Z**
ESC	**1B**	**^[**
FS	**1C**	**^**
GS	**1D**	**^]**
RS	**1E**	**^^**
US	**1F**	**^_ (Underscore)**
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~”
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~’
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)

Figure 5-12 Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Figure 5-13 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	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

Figure 5-14 Decimal - Hexadecimal Chart (0 to 159 Decimal)

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		

Figure 5-15 Decimal - Hexadecimal Chart (160 to 255 Decimal)

Chapter 6 AppLock

Introduction

LXE's AppLock is designed to be run on LXE certified Windows CE. NET based devices only. LXE installs the program as part of the factory-installation process.

A mobile device running AppLock becomes a dedicated, single application device. In other words, only the application or feature specified in the AppLock configuration by the Administrator is available to the user.

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

When the mobile device is reset to factory default values, the Administrator may need to reconfigure the AppLock application.

Note: To reset the device to factory default values, please refer to Chapter 4 "System Configuration" section titled "Utilities" and the RegClear, PSMFormat and ColdBoot executable files.

Setup a New Device

LXE 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. Connect an external power source to the device (if required).
3. Adjust screen display, audio volume and other parameters if desired. Install accessories (e.g. handstrap, stylus).
4. Tap **Settings | Control Panel | Administration** icon.
5. Assign an application on the Control tab screen.
6. Assign a password on the Security tab screen.
7. Select a view level on the Status tab screen, if desired.
8. Tap OK
9. Press the hotkey sequence to launch AppLock and lock the configured application.
10. The device is now in end-user mode.

Note: LXE has made the assumption, in this chapter, that the first user to power up a new mobile device is the system administrator.

Administration Mode

Administration mode gives full access to the 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:

1. Create/change the keystroke sequence to activate administrator access.
2. Create/change the password for administrator access.
3. Assign the name of the application to lock.
4. Select the command line of the application 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

End User Mode

End-user mode locks the end-user into the configured application. The end user can still reboot and respond to dialog boxes. The single application is automatically launched, and runs in full screen mode, when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE .NET key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE .NET desktop icons, menu bars, task bar and system trays are not visible or accessible. 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 clicks on the Close icon on the application's title bar and the application remains active.

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.

Windows accelerator keys such as Alt-F4 are disabled.

Administration and Configuration

The default Administrator Hotkey sequence is **Shift+Ctrl+A.**

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

Configuration

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

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Control Panel

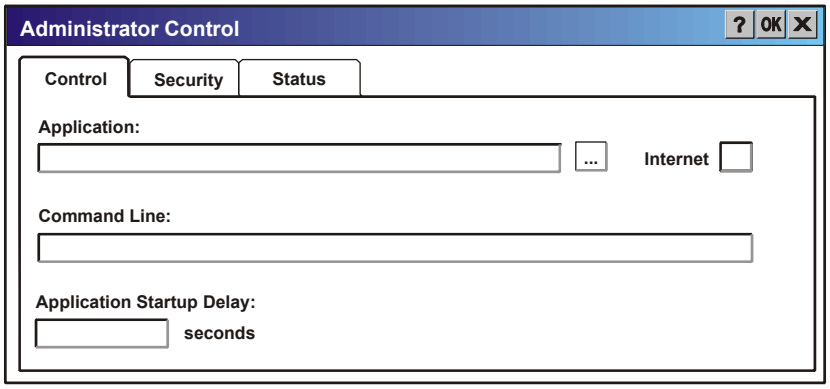


Figure 6-1 Administrator Control Panel

Use the Control tab options to select the application to launch when the device boots up.

Move the cursor to the Application text box and either type the application path or click the Browse button (the … button). The standard Windows CE .NET Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.

Enter the command line parameters for the application in the Command Line text box.

Enter the number of seconds the selected Application must wait before starting to run upon reboot.

If no application is specified when the Administrator Control panel is closed, the device reboots into Administrator mode. If a password has been set, but the 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.

End User Internet Explorer

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.

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). 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 simply checking the "Internet" checkbox in the Control tab of the Administrator applet. The internet application should then be entered in the "Application" text box. If the standard Internet Explorer that is shipped with the 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

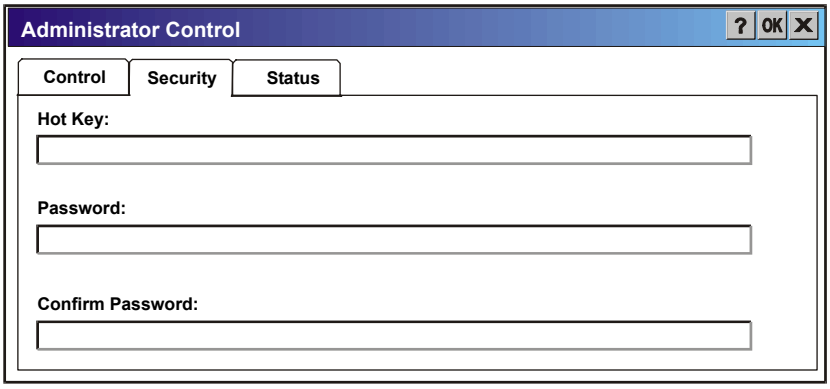


Figure 6-2 Administrator Security Panel

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Note: Some key combinations cannot be specified because they conflict with the key combinations used by other LXE applications. The message "Selected hotkey is not allowed, Please re-enter" is displayed. A different Hotkey must be entered.

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.

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", "Alt", and "Ctrl" text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence.

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 unlike pressing the normal key during a mode switch; this key can be entered from the SIP 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 SIP.

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

Status Panel

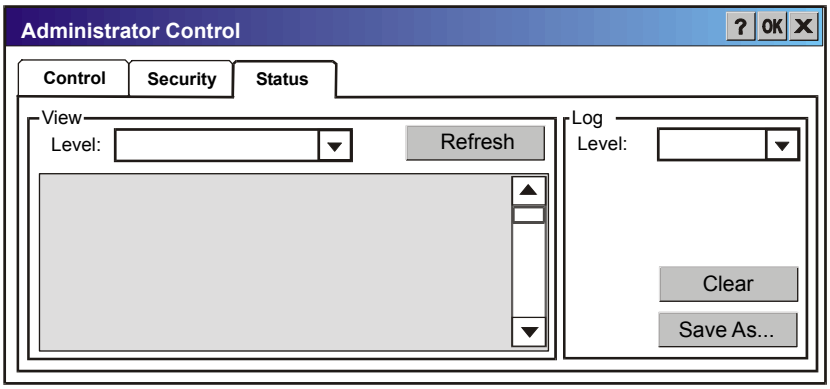


Figure 6-3 Administrator Status Panel

Use the Status panel to view the log of previous AppLock operation and to configure which messages are to be recorded during AppLock operation.

As the status information is stored in the registry and accumulates during AppLock configuration and operation, it is very important that the administrator periodically clear the status information to reduce the amount of registry space used. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

View

Error	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	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	Extended status provides more detailed information than that logged by Process Logging.
All	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.

Levels

Note: ***If a level higher than Error is selected, the status should be cleared frequently by the administrator.***

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is Error Logging; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, 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.

See Also: Error Messages

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 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 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

Forgotten the password that has been set? Enter this LXE back door key sequence:

Ctrl+L Ctrl+X Ctrl+E

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; 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 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
Alt	Processing the hotkey and backdoor entry	LOG_EX

Message	Explanation and/or corrective action	Level
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
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR

Message	Explanation and/or corrective action	Level
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
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
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 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 Adminstration 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
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR

Message	Explanation and/or corrective action	Level
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
Term process restart –window not found	The locked application has been closed using a method that cannot be detected by AppLock. AppLock will restart the application.	LOG_ERROR

AppLock Registry Settings

This system application runs at startup via the "launch" feature of LXE Windows CE .NET devices. When the launch feature is installed on the 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=
```

Chapter 7 Wireless Network Configuration

Introduction

The MX3X computer offers a choice of Cisco and Symbol radios. The radios can be configured for no encryption, WEP encryption or WPA security (Cisco only).

Configuring an MX3X Radio without WPA

Cisco – Aironet Client Utility (ACU)

Access: **Start | Aironet Client Utility *or* ACU Icon on Desktop**

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards. Cisco options are available on the MX3X and MX3-RFID devices.

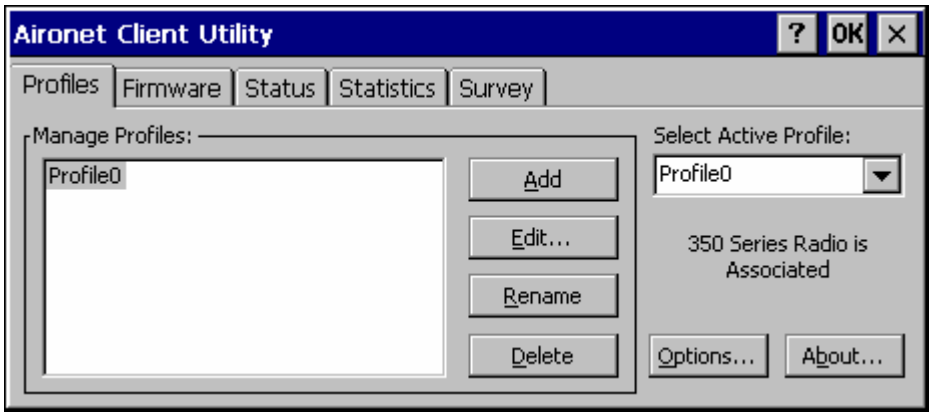


Figure 7-1 Cisco Aironet Client Utility

Note: To configure WPA, please see "WPA for the MX3X", later in this chapter.

Profiles Tab

Use this option to manage profiles and review firmware information, status, statistics and wireless radio survey data.

Profile Parameter	Default
SSID	Blank
Client Name	Blank
Infrastructure Mode	Yes
Power Save Mode	Fast PSP
Network Security Type	None
WEP	No WEP
Authentication Types	Open
LEAP	Disabled
Mixed Mode	Disabled
World Mode	Disabled
Data Rates	Auto
Transmit Power	MAX
Offline Channel Scan	Enabled

Select an active profile to manage.

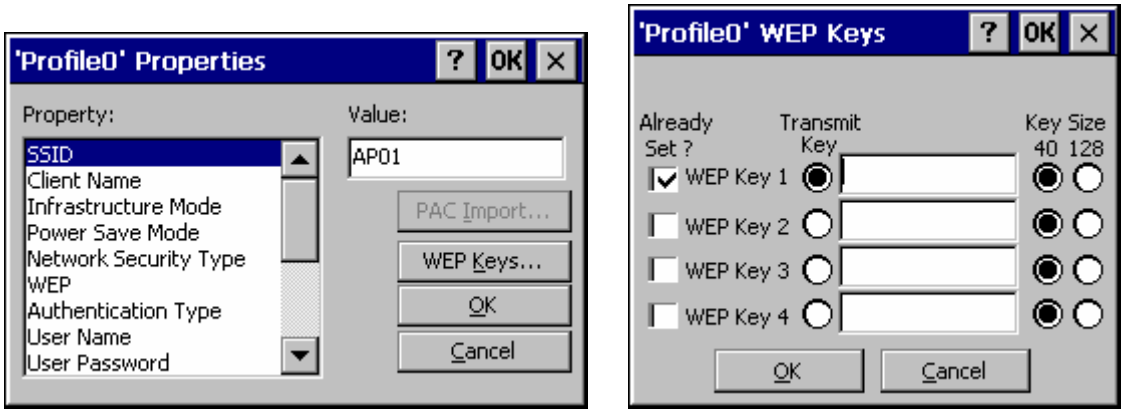


Figure 7-2 Cisco Profile Properties Screen

Tap the **WEP Keys** button to enter WEP information. If a key is already entered, the "Already set?" checkbox is checked. The previously entered key value is not displayed for security.

Firmware Tab

Displays the current firmware version and allows you to load new firmware. Tap the Browse button to locate the new firmware file.

Status Tab

Immediately runs status on : signal strength and signal quality.

Statistics Tab

Select the Receive Stats or Transmit Stats. The data is displayed on the screen.

Survey Tab

Immediately runs signal strength and quality and link speed. An option is available to Setup parameters for Active Mode reporting.

Symbol

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards unless noted otherwise. Symbol options are available on an MX3X device only.

Access: Tap the Network Connected Icon in the Status Bar

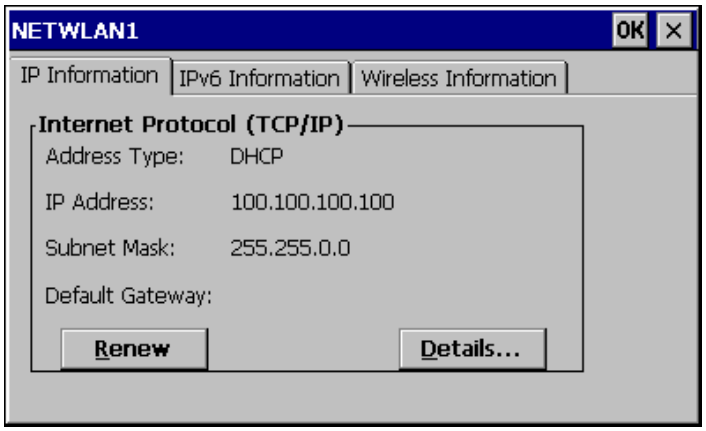


Figure 7-3 Symbol NETWLAN Screen

IP Information Tab

After the IP Address has been assigned to the mobile device, tap the Renew button to renew the IP address if necessary. Tap the Details button to view the Network Connection details.

IPv6 Information Tab

This is the TCP/IPv6 information screen. The contents cannot be edited by the user.

Configuring IPv6

By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up. To disable IPv6, run \Windows\ipv6Disable.reg and perform a warmboot. To enable IPv6, run \Windows\ipv6Enable.reg and perform a warmboot.

Note: These utilities affect the behavior of the IPv6 on warmboot. After a coldboot, IPv6 is enabled.

Wireless Information Tab

Factory Default Settings	
Wireless Information tab	
Notify when new networks available	Enabled
Advanced Button	
Use Windows to configure wireless settings	Enabled
Automatically connect to non-preferred networks	Disabled
Networks to access (Only APs, Only comp-to-comp)	All available
Encryption (WEP, TKIP)	WEP
Authentication (WPA, Open, Shared, WPA-PSK)	WPA
Ad hoc network	Disabled
Key provided automatically	Enabled
Enable 802.1X authentication	Enabled
EAP Type (MDF-Challenge, PEAP, TLS)	TLS

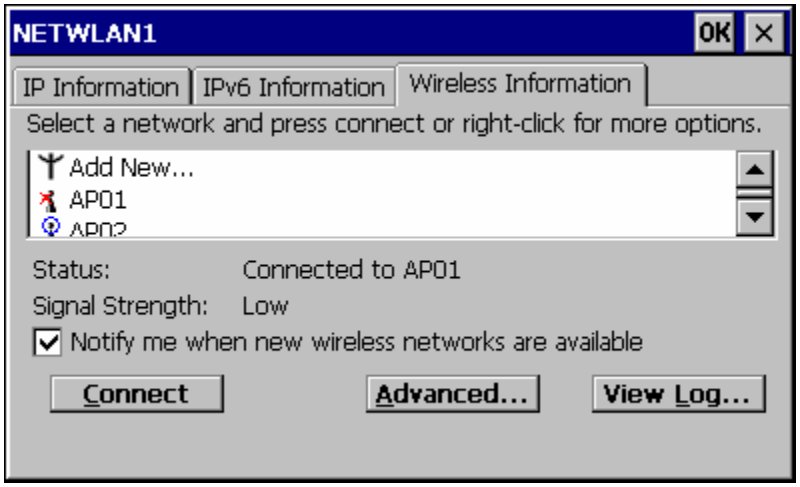


Figure 7-4 Symbol Wireless Information Tab

View Log

Displays the logon/connection data for the current network connection.

Add a new connection

Select **Add New**. Enter the ESSID in the **Network Name** text box.

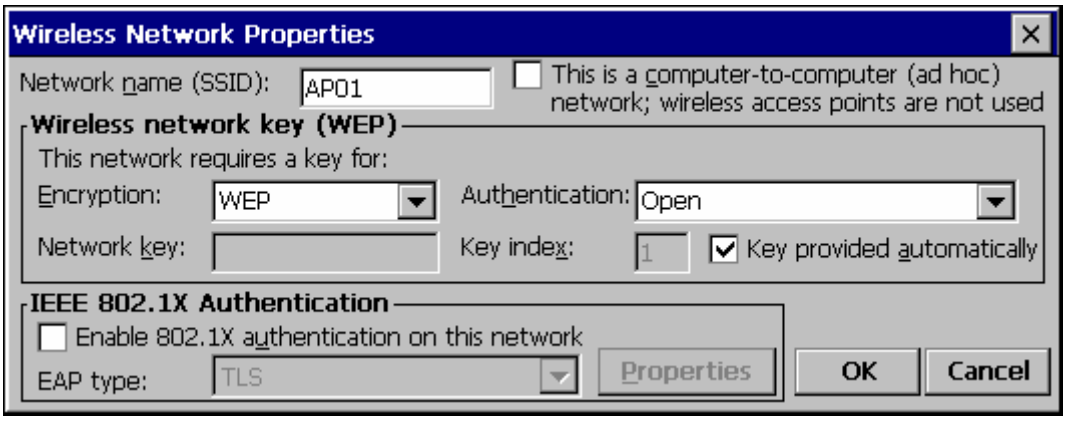


Figure 7-5 Symbol Wireless Network Properties

Disable WEP

- If WEP is to be disabled, tap the down arrow in the **Authentication** drop down box. Select **Open**.
- Tap the down arrow in the **Encryption** drop down box. Tap **Disabled** and WEP is disabled.
- Tap the **OK** button to return to the **Wireless Information** tab.

Enable WEP

- Tap the down arrow in the **Authentication** drop down box.
- Tap the **WEP Authentication** protocol.
- If the key is provided automatically by your network, check the "**Key provided automatically**" checkbox.
- If you wish to enter your Authentication key, uncheck the "**Key provided automatically**" checkbox and enter the Network Key in the **Network Key** text box.
- Tap the **OK** button to return to the **Wireless Information** tab.

Continue

Tap the **Advanced** … button. Make sure there is a checkmark in the "**Use Windows to configure my wireless settings**" checkbox. Make sure there is ***no*** checkmark in the "**Automatically connect to non-preferred networks**" checkbox. Tap the **Connect** button.

Tap **OK** to return to the **Wireless Information** tab.

Tap the **Connect** button.

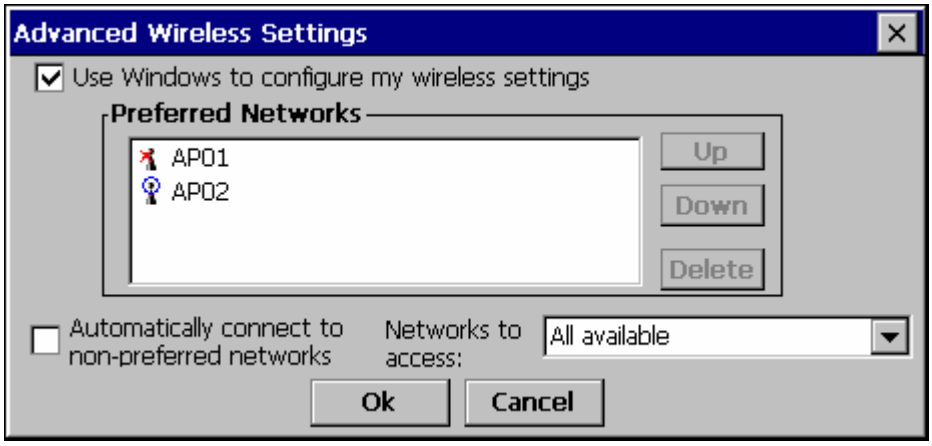


Figure 7-6 Symbol Advanced Wireless Settings

To access NETWLAN1 Properties again, tap the **Network Connected icon** in the Toolbar.

Select a User Certificate

1. Select **Wireless Information** Tab
2. Select a network by doubletapping the network name.
3. In the IEEE 802.1X Authentication box, enable **802.1X** authentication
4. Select an **EAP type.**
5. Tap the **Properties** button. Validate Server is enabled by default.
6. At the Authentication Settings display, tap the **Select** button to choose a User Certificate.

WPA for the MX3X and MX3-RFID

	Wi-Fi Protected Access (WPA) is only available on mobile device's equipped with the updated Cisco radio driver (**release 2.60 or later**).
	WPA requires software **revision 1ED** or greater. To identify the software revision, please click on the "About" icon in the CE .NET Control Panel.
	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for MX3X communication.
 Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

System Requirements

To support Wi-Fi Protected Access (WPA), the mobile device must be equipped as follows:

- Cisco 350 radio card with driver release 2.60 (or later).

The LXE MX3X supports WPA and all authentications. The Microsoft supplicant and Cisco supplicants are used separately or together to provide support for the different authentications.

Most of the configuration is done with the Microsoft Wireless Configuration tool.

WPA/LEAP requires the Cisco supplicant and Cisco ACU configuration tool.

Installing Radio drivers

Which version of the Cisco driver should be installed depends on which authentication protocol is to be configured.

- Cisco PEAP should not be installed if using PEAP/MSCHAP.
- Cisco PEAP must be installed if using PEAP/GTC.
- For all other authentications (LEAP, EAP-TLS, WPA-PSK) it does not matter if Cisco PEAP is installed or not.

To determine if Cisco PEAP is installed or to change the installation, refer to the instructions in the following sections.

Checking for the Cisco PEAP Supplicant

With a Cisco radio installed, open the Wireless network properties as described in "Wireless Network Configuration", later in this chapter. With the Authentication tab selected check the text in the EAP type drop down box. Refer to the following figures to determine if Cisco PEAP is installed.

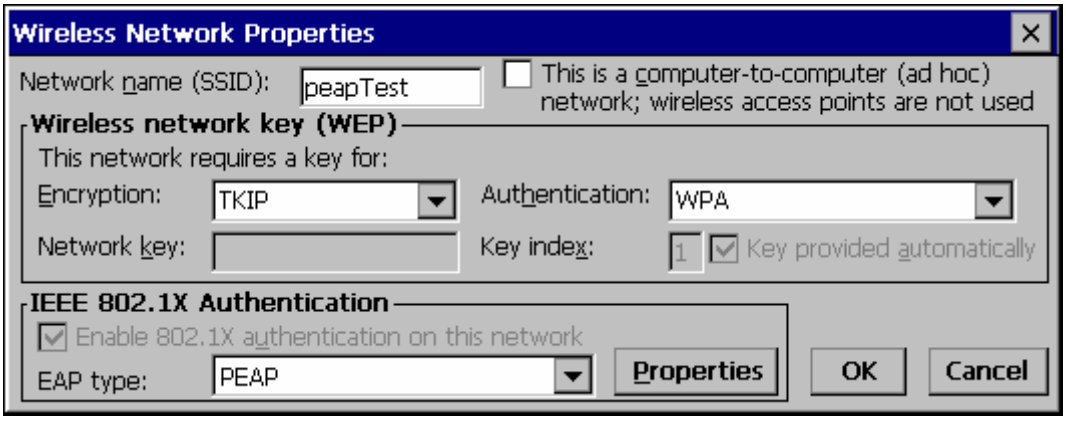


Figure 7-7 No Cisco PEAP

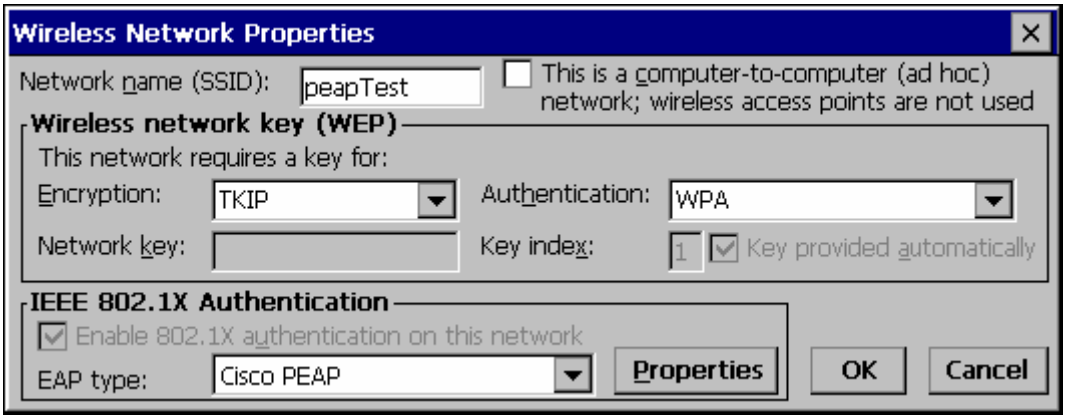


Figure 7-8 Cisco PEAP Installed

If the Cisco installation is correct, continue with the configuration. If it is not correct, follow the procedures below.

Note: Instructions are also included in the README file located in the \SYSTEM folder.

There are two Cisco CAB files in the \SYSTEM folder of the MX3X. The default files are:

- CISCO.CAB
- CISCOPEAP.CAB

The default CISCO.CAB file provides for all authentications except Cisco PEAP. When the default CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the figure labeled “No Cisco PEAP”, above.

If Cisco PEAP is desired:

1. Rename the CISCO.CAB file to CISCOMSCHAP.CAB.
2. Rename the CISCOPEAP.CAB file to CISCO.CAB.
3. Coldboot the mobile device to install the new driver with the registry.

The renamed CISCO.CAB file provides for Cisco PEAP and PEAP/GTC authentications. When the renamed CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the previous figure labeled “Cisco PEAP Installed”.

If it becomes necessary to switch to a different authentication than Cisco PEAP or PEAP/GTC,

1. Rename the CISCO.CAB file to CISCOPEAP.CAB.
2. Rename the CISCOMSCHAP.CAB file to CISCO.CAB
3. Coldboot the mobile device to install the new driver with the registry.

Root Certificates

Generating a Root CA Certificate

	Please refer to the "LXE Security Primer" for more information on obtaining and installing root certificates.

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.

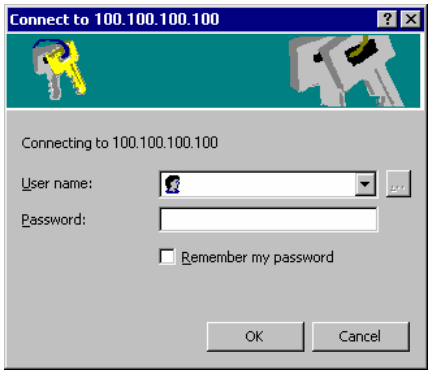


Figure 7-9 Logon to Certificate Authority

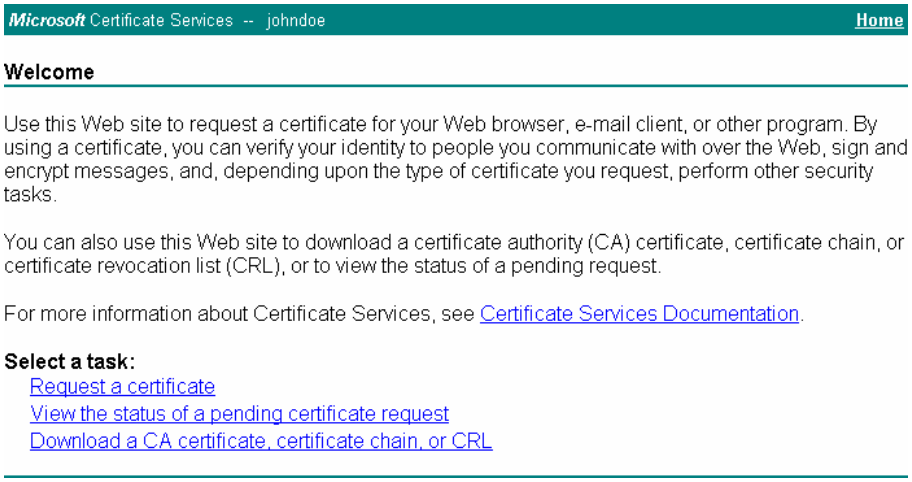


Figure 7-10 Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** task link.

Make sure the correct root **CA certificate** is selected in the list box.

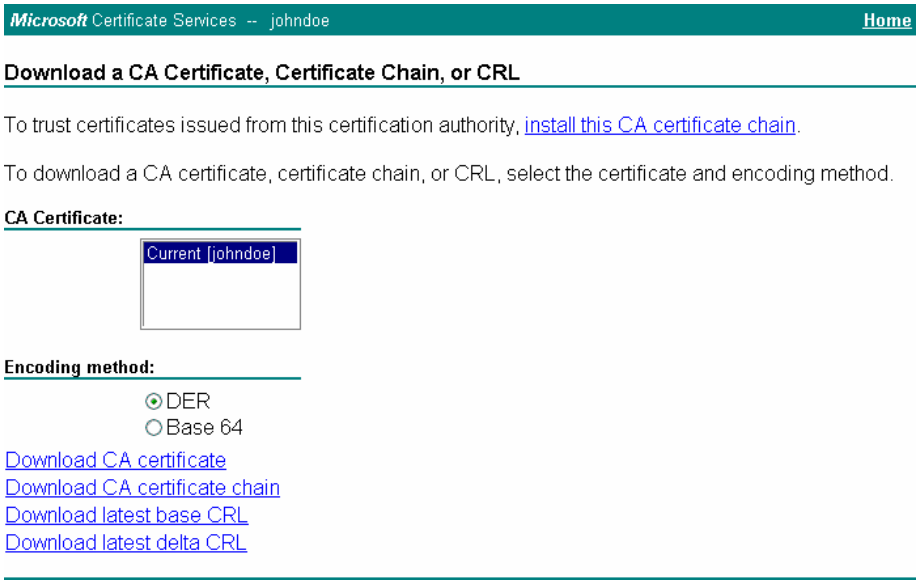


Figure 7-11 Download CA Certificate Screen

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.

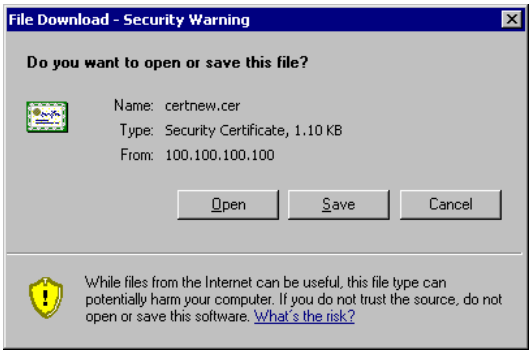


Figure 7-12 Download CA Certificate Screen

Click 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**.

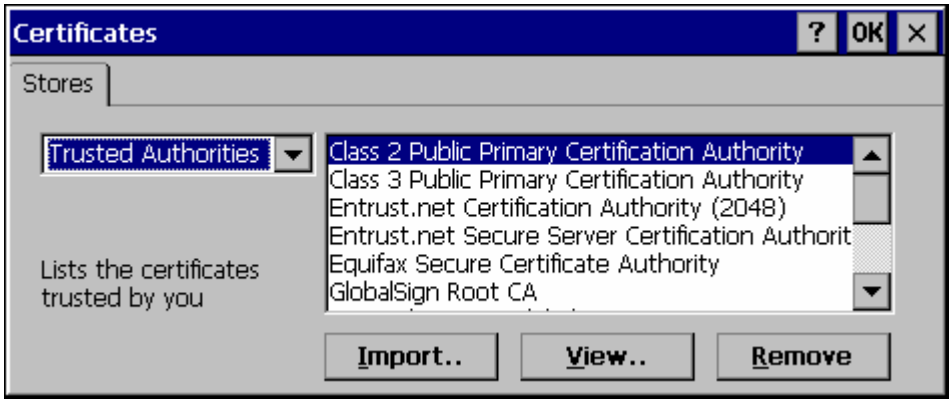


Figure 7-13 Certificates

Click the "**Import**" button.

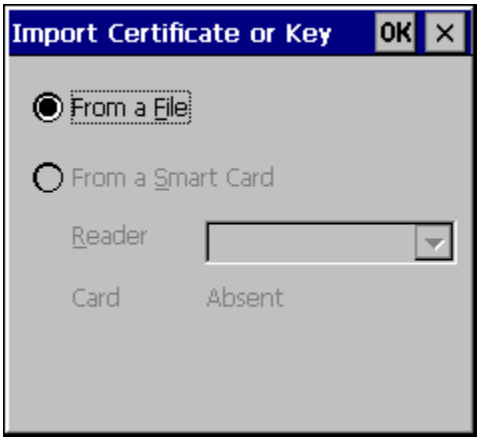


Figure 7-14 Import Certificate

Make sure "**From a File**" is selected and click OK.

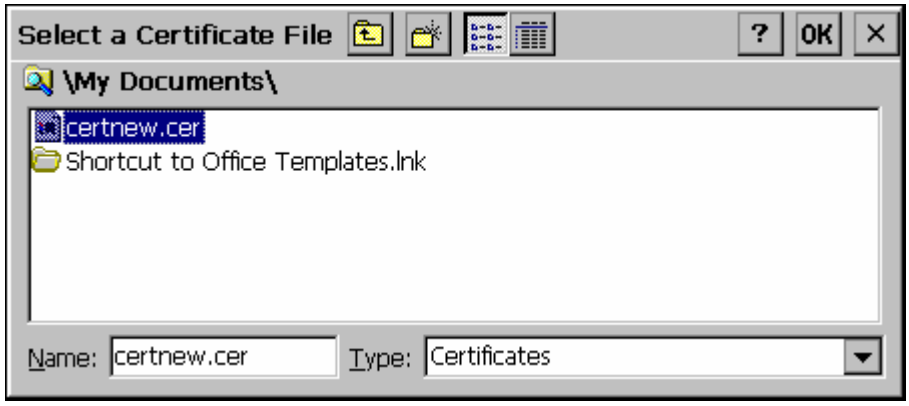


Figure 7-15 Browsing to Certificate Location

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and click OK.

Figure 7-16 Certificate Import Confirmation

Click **Yes** 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 MX3X

	Please refer to the "LXE Security Primer" for more information on obtaining and installing user certificates.

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 and password of the person who will be logging into the mobile device.

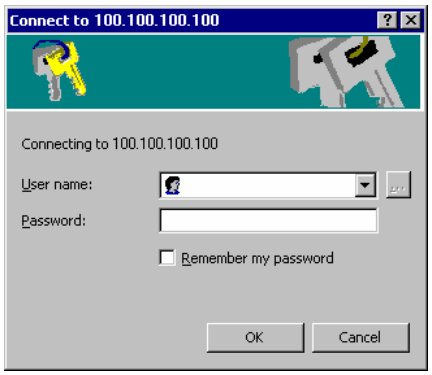


Figure 7-17 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. CE .NET devices such as the MX3X require the private key to be saved as a separate file rather than including the private key in the user certificate.

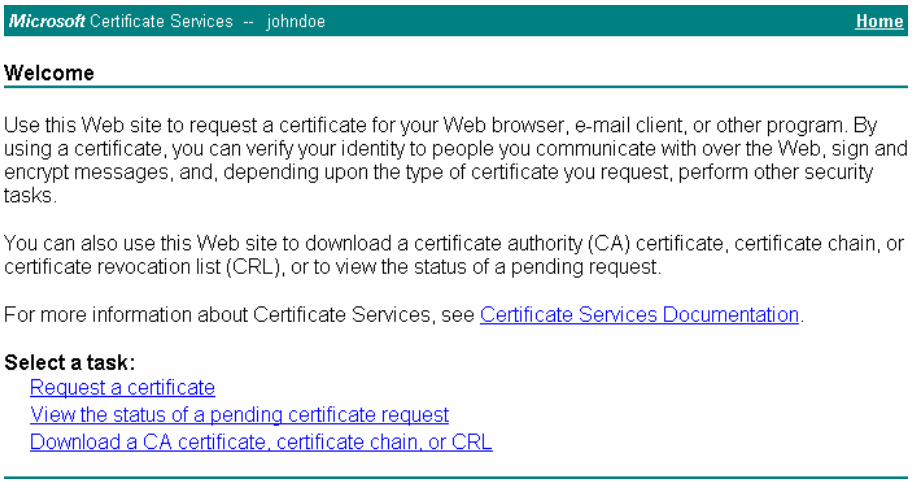


Figure 7-18 Certificate Services Welcome Screen

Click the "**Request a certificate"** task link.

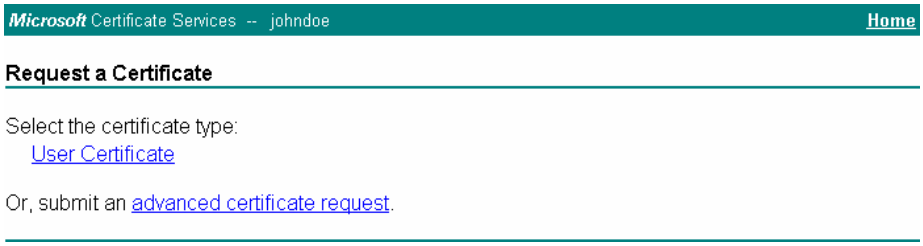


Figure 7-19 Request a Certificate Screen

Click on the "**advanced certificate request"** link.

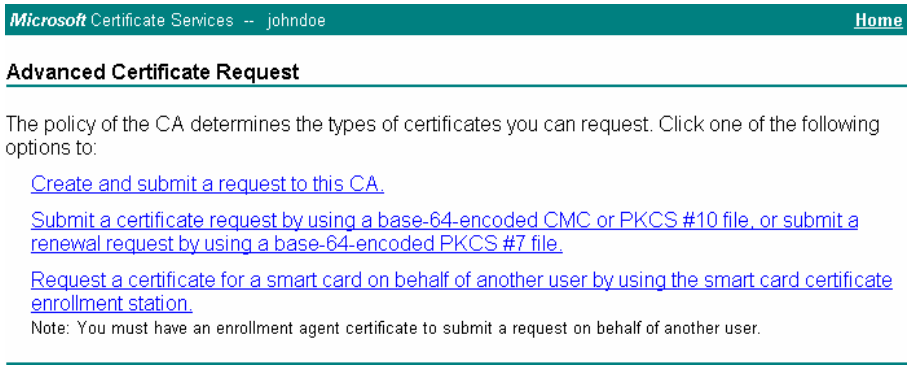


Figure 7-20 Advanced Certificate Request Screen

Click on the "**Create and submit a request to this CA"** link.

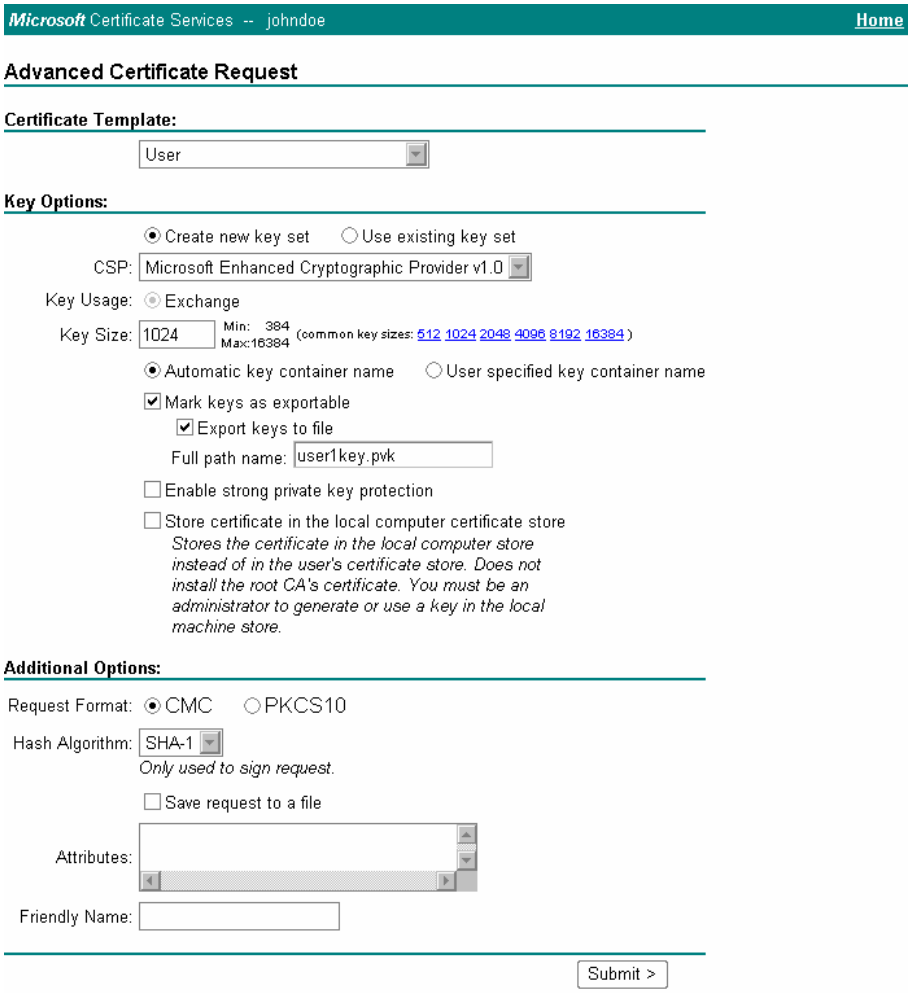


Figure 7-21 Advanced Certificate Details

For the Certificate Template, select “User”.

Check the “Mark keys as exportable” 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 MX3XUSER.PVK. The certificate file created later in this process must be given the same name, for example, MX3XUSER.CER.

DO NOT check “Enable strong private key protection”.

Make any other desired changes and click the “Submit” button.

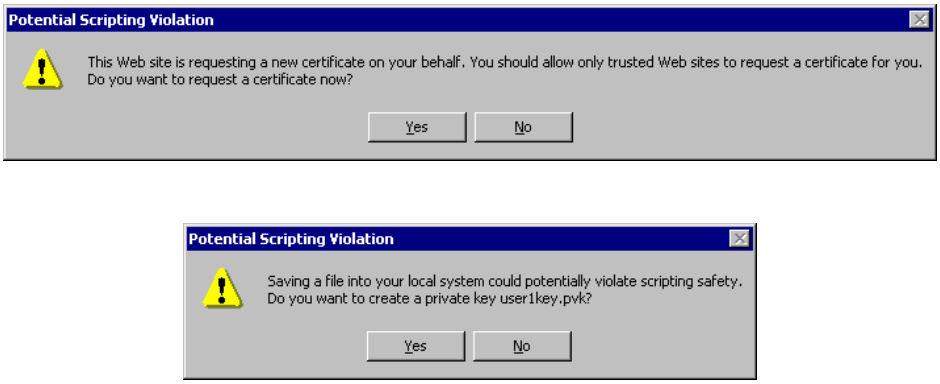


Figure 7-22 Script Warnings

If any script notifications occur, click the "Yes" button to continue the certificate request.

Figure 7-23 Script Warnings

When prompted for the private key password:

- Click "None" if you do not wish to use a password, *or*
- Enter and confirm your desired password then click "OK".

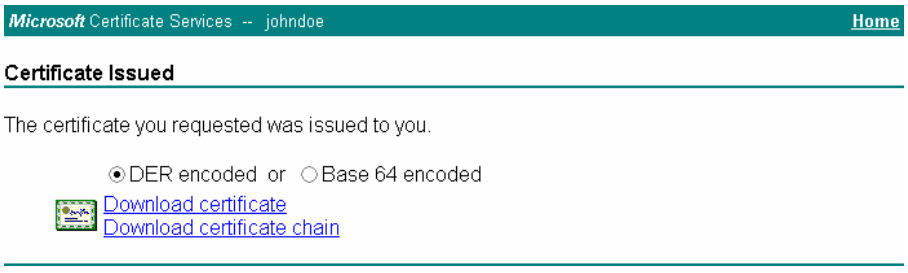


Figure 7-24 Certificate Issued

Click the **Download certificate** link.

Figure 7-25 Download Security Warning

Click **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 MX3XUSER.PVK then the certificate file created must be given the same name, for example, MX3XUSER.CER.

Installing a User Certificate on the MX3X (WPA-TLS Only)

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.

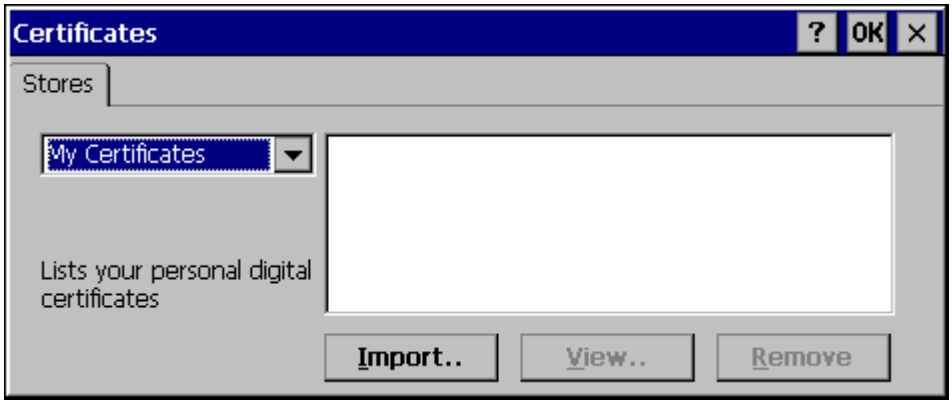


Figure 7-26 Certificates

Click the “Import” button.

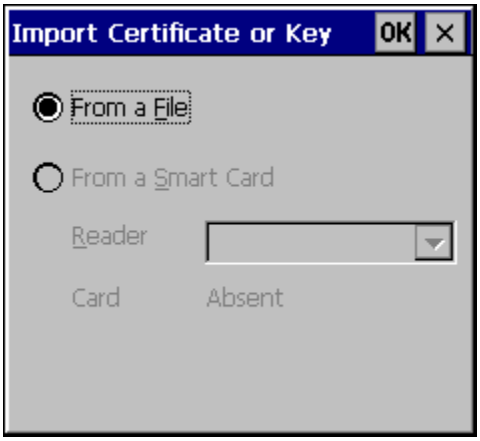


Figure 7-27 Import Certificate

Make sure “From a File” is selected and click OK.

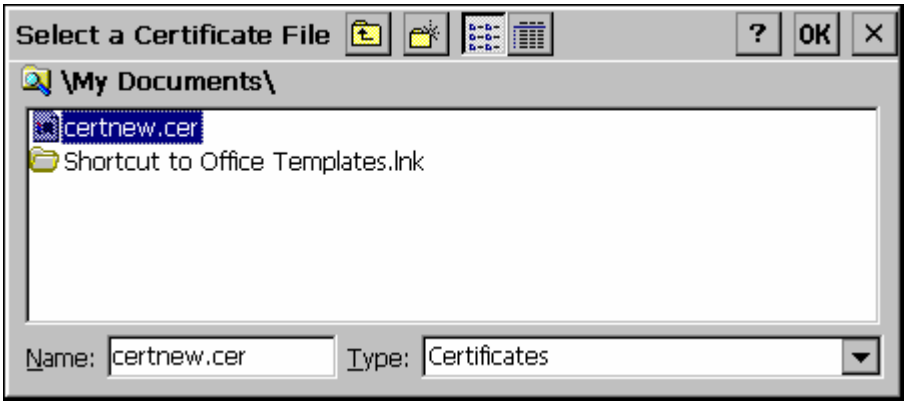


Figure 7-28 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and click OK.

The certificate is now shown in the list.

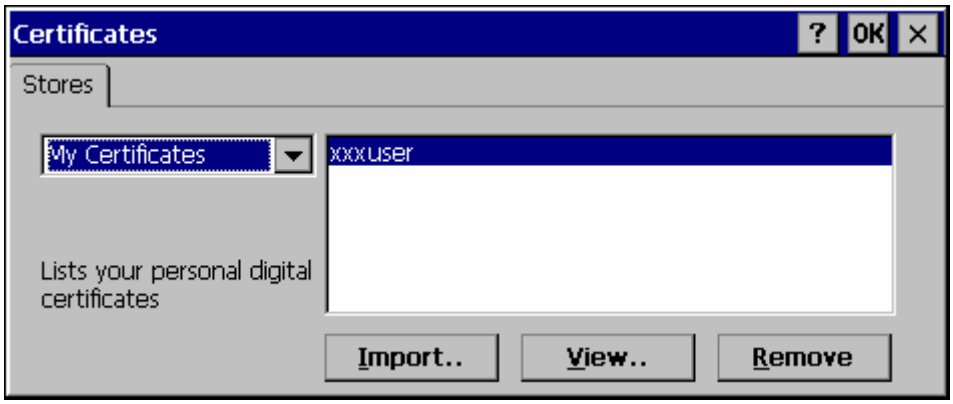


Figure 7-29 Certificate Listing

Highlight the certificate you just imported and click the View. . button.

From the Field pull down menu, select “Private Key.

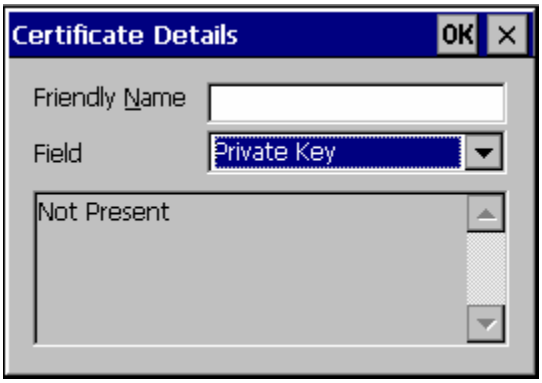


Figure 7-30 Private Key Not Present

- 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, click OK to return to the Certificates screen.

Click import.

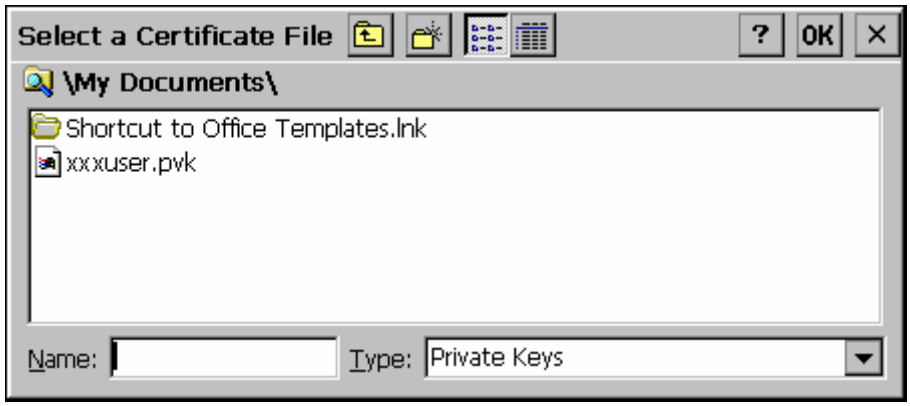


Figure 7-31 Browsing to Private Key Location

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 click OK. Enter the password for the certificate if appropriate.

Click on View to see the certificate details again.

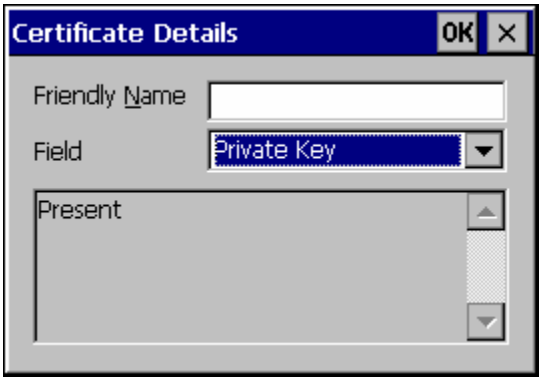


Figure 7-32 Private Key Present

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 mx3xuser.cer for the certificate and mx3xuser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Wireless Network Configuration

Use the following instructions for all authentication protocols to configure the Microsoft Wireless Network configuration utility unless WPA/LEAP is used.

WPA/LEAP is configured with the Cisco ACU (see Section titled "WPA/LEAP Authentication Configuration").

Click the ACU icon on the desktop.

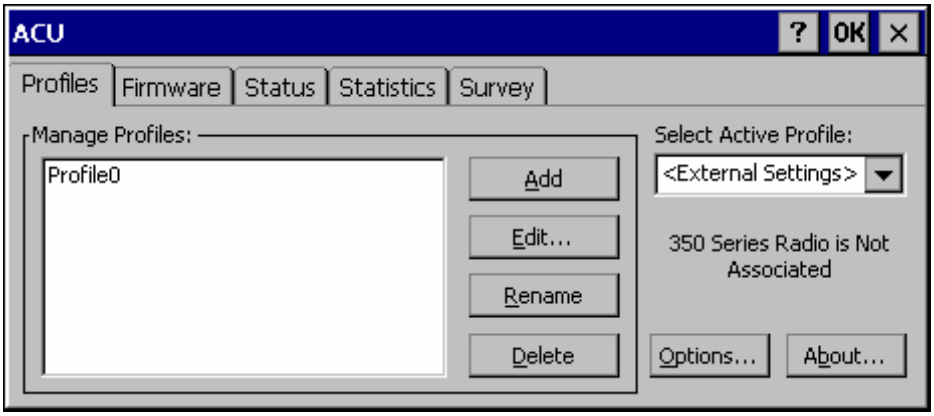


Figure 7-33 Cisco ACU Profile Selection

From the "Select Active Profile" pull down list, select <External Settings>.

Click OK and warmboot.

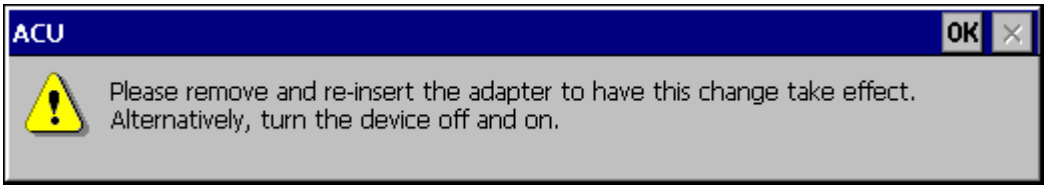


Figure 7-34 Cisco ACU Reboot Message

After booting up, the Microsoft Zero Config tool should start. If it does not, start configuring the wireless connection by clicking on the icon on the task bar shown in below.

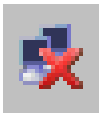


Figure 7-35 Microsoft Wireless Connection Icon

The Wireless Network Connection screen appears.

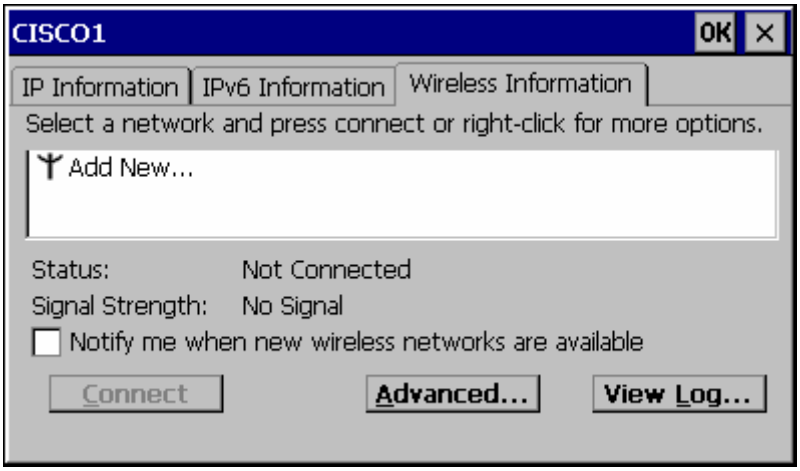


Figure 7-36 Wireless Information Screen

Make sure the “Notify me when new wireless networks are available” box is *not* checked..

Click the “Advanced…” button.

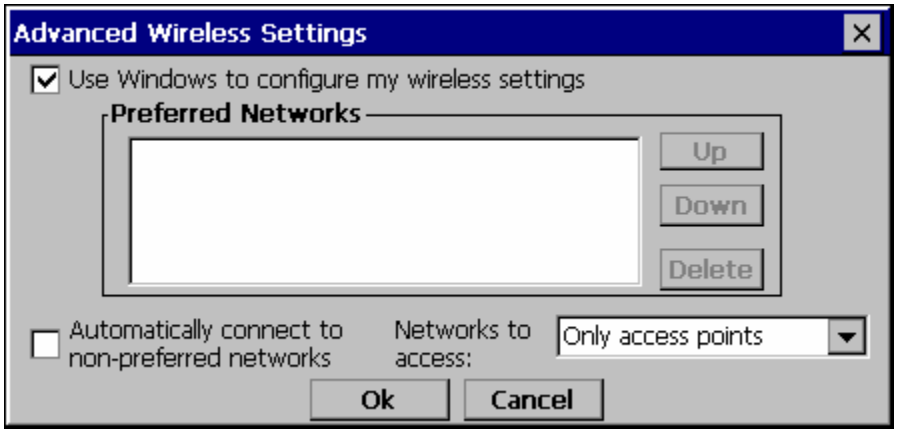


Figure 7-37 Advanced Wireless Settings

Make sure the “Use Windows to configure my wireless settings” box is checked.

Set the “Networks to access” drop down box to “Only access points”.

Click the OK button on the Advanced Wireless Settings screen and the Wireless Information Screen is displayed.

On the Wireless Information screen click the “Add New …” line.

The Wireless Network Properties screen is displayed.

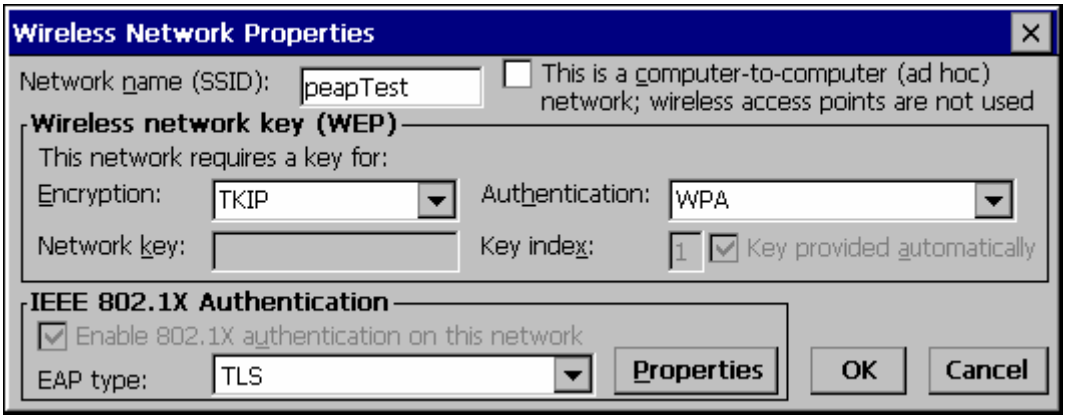


Figure 7-38 Wireless Network Properties

Enter the Network name (SSID) into the text field.

For PEAP/MSCHAP and EAP/TLS, set Encryption to TKIP and Authentication to WPA.

For WPA/PSK see “WPA/PSK Authentication Configuration”.

To configure the IEEE 802.1X Authentication box see the following sections for configuration of each authentication protocol.

PEAP/MS-CHAP Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/MS-CHAP protocol. The Cisco CAB file without Cisco PEAP must be used with PEAP/MS-CHAP. See “Installing Radio Drivers”, earlier in this chapter, for more information.

Configuring the PEAP/MS-CHAP Supplicant

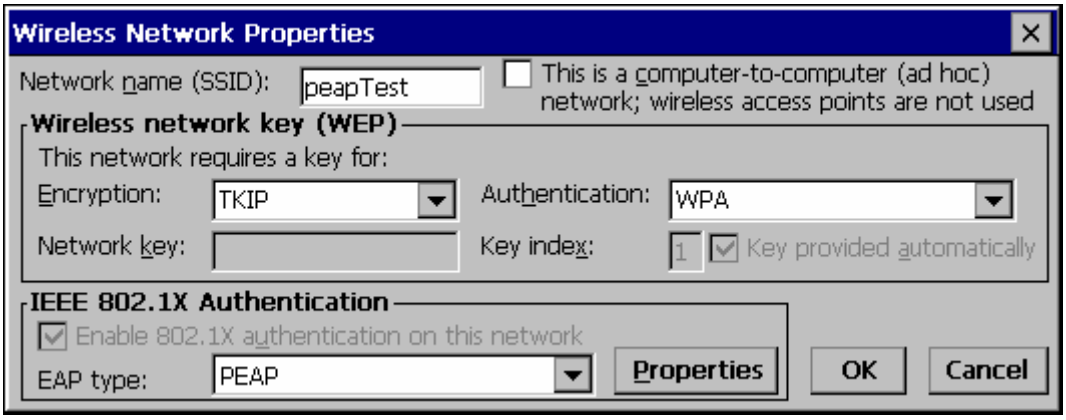


Figure 7-39 PEAP/MSCHAP Wireless Network Properties

With the radio parameters configured (see “Wireless Network Configuration” earlier in this chapter) set the **EAP type** to PEAP as shown above.

If the EAP type box text is not exactly as shown see “Installing Radio Drivers” earlier in this chapter, to change the radio CAB file.

Click the **Properties** button.

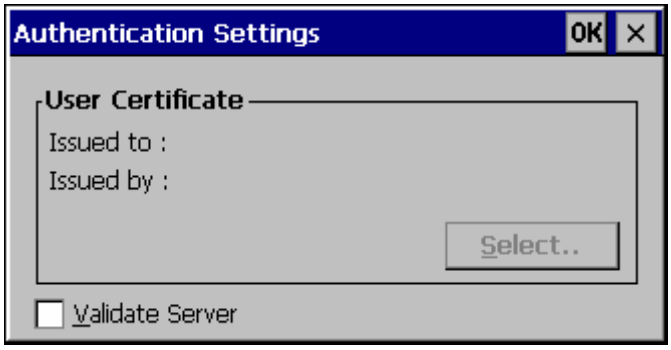


Figure 7-40 Authentication Settings

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, come back to this screen and validate the server certificate.

The login screen appears for logging into the wireless network.

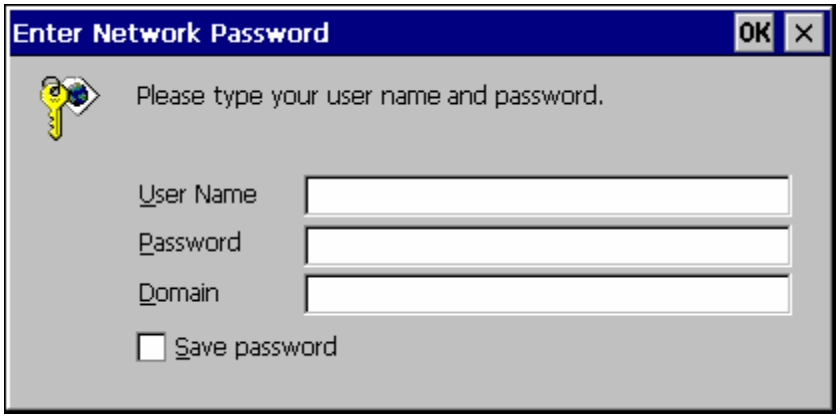


Figure 7-41 Wireless Network Login

Once authenticated, click the IP Information tab.

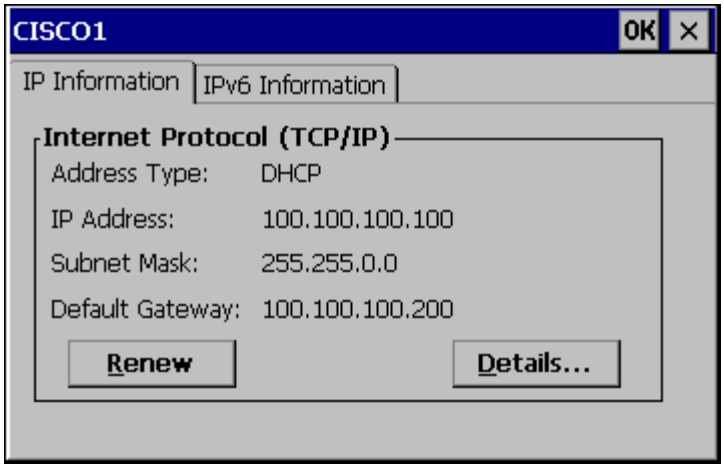


Figure 7-42 IP Information Tab

If the network is set to use DHCP, the mobile device displays the IP address assigned by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see "Root Certificates", earlier in this chapter.

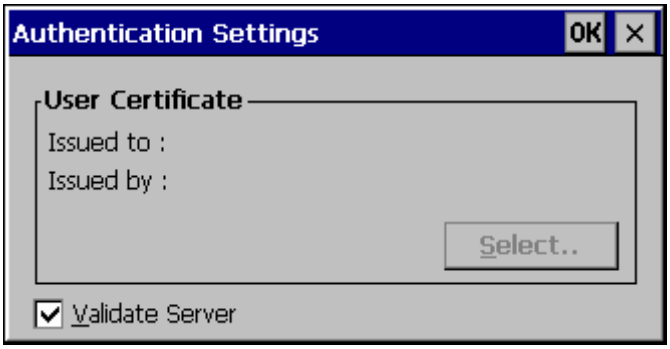


Figure 7-43 Authentication Settings, Validate Server

Navigate to the Wireless Network Properties configuration screen.

Click the Properties button.

Check "Validate server" .

Click OK to dismiss the configuration boxes.

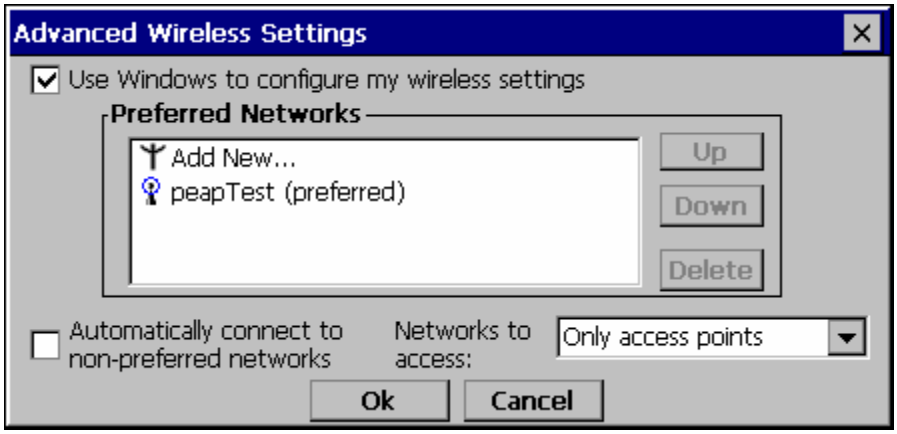


Figure 7-44 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Click on the IP Information tab and make sure there is a valid IP address as shown in the figure labeled "IP Information Tab", earlier in this chapter.

PEAP/GTC Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/GTC protocol.

Configuring the PEAP/GTC Supplicant

With the radio parameters configured set the EAP type to Cisco PEAP as shown below.

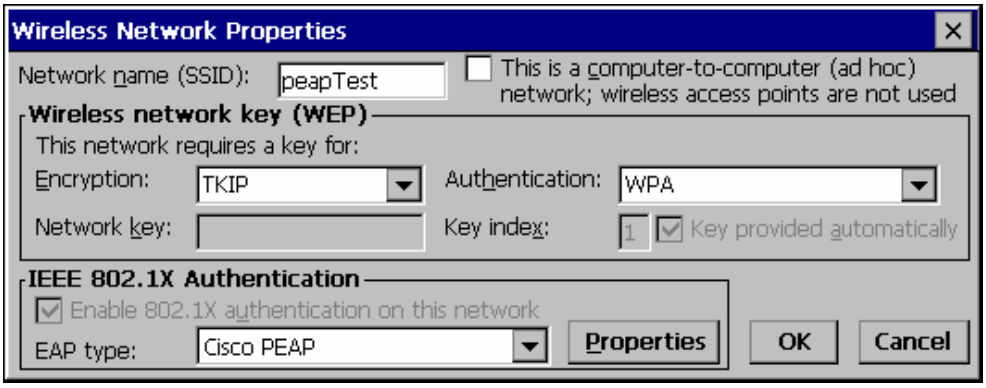


Figure 7-45 PEAP/GTC Wireless Network Properties

If the EAP type box text is not exactly as shown see "Installing Radio Drivers", earlier in this chapter, to change the radio cab file.

Click the **Properties** button.

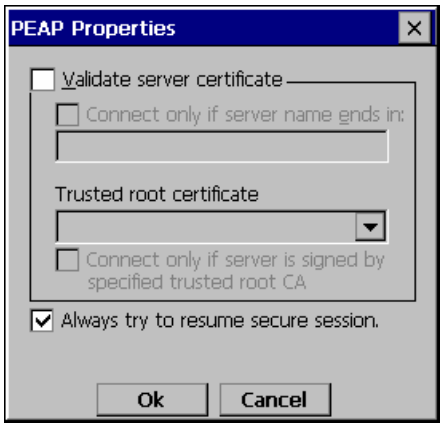


Figure 7-46 PEAP Properties

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, return to this screen and validate the server certificate as shown later in this section.

Check the **Always try to resume secure session** box.

Note: This box must be checked for the LXE device to roam from one AP to another AP.

Click the **OK** button.

The login screen appears for logging into the wireless network.

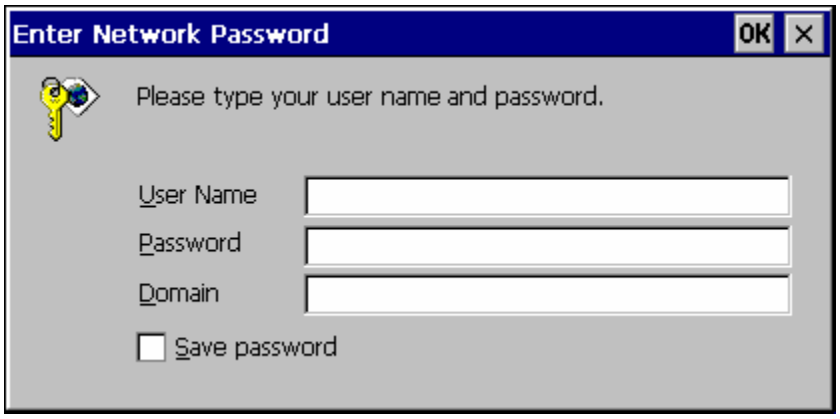


Figure 7-47 Login Screen

Enter valid user credentials.

Once authenticated click the **IP Information** tab

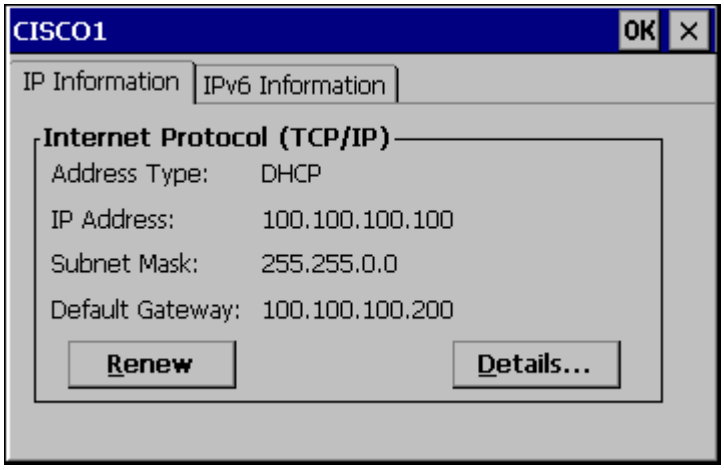


Figure 7-48 IP Information Tab

The .NET device displays the IP address given by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see "Root Certificates", earlier in this chapter.

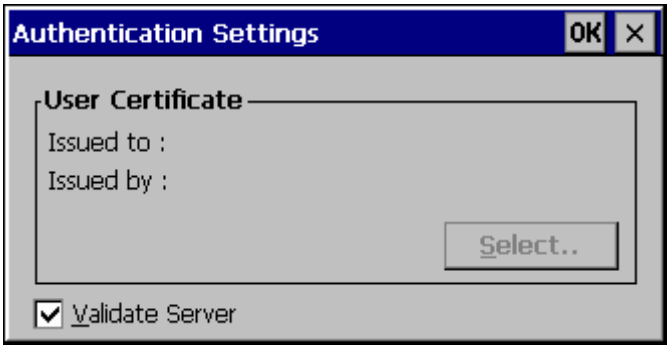


Figure 7-49 Authentication Settings, Validate Server

Navigate to the **Wireless Network Properties** configuration screen.

Click the **Properties** button.

Check **Validate server** .

Click **OK** to dismiss the configuration boxes.

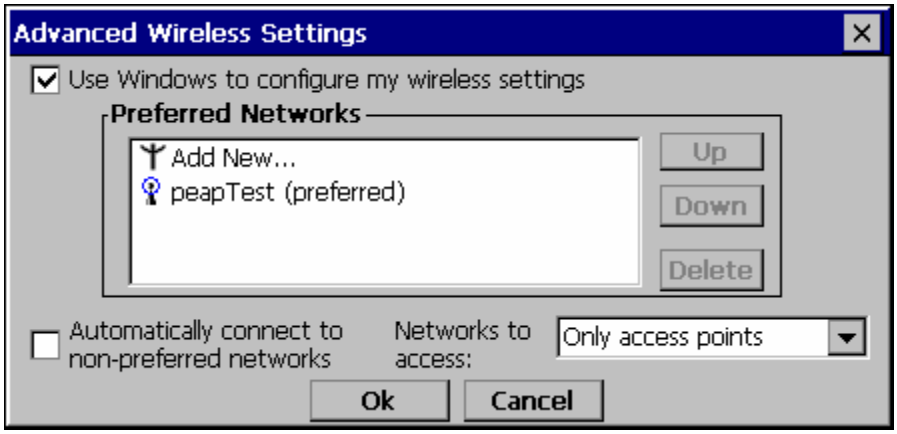


Figure 7-50 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Click on the IP Information tab and make sure there is a valid IP address as shown in the figure labeled "IP Information Tab", earlier in this chapter.

WPA/LEAP

LEAP is a Cisco proprietary authentication protocol and is not supported by the Microsoft supplicant. To configure the mobile device for WPA/LEAP, use the Cisco ACU installed during normal installation of the Cisco radio driver.

Cisco ACU

Start the Cisco ACU by clicking the icon on the desktop or navigate to **Start** | **Programs** | **Cisco** | **ACU**.

Click on the Profile tab.

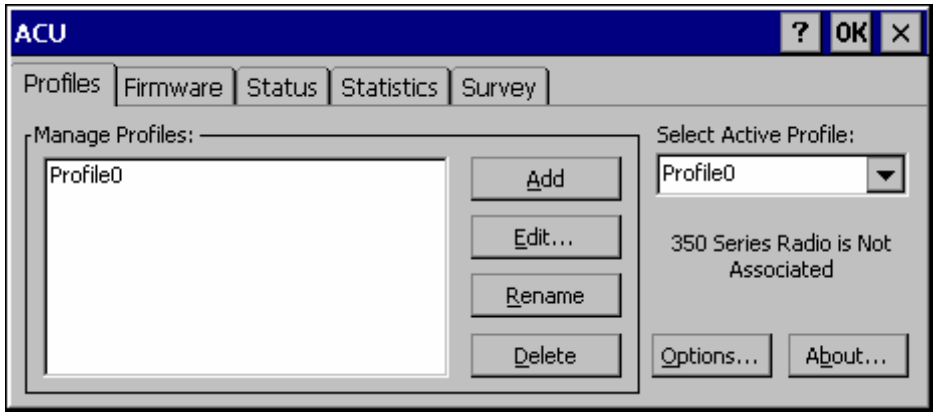


Figure 7-51 ACU Profile Tab

Click the Rename button.

Name the profile.

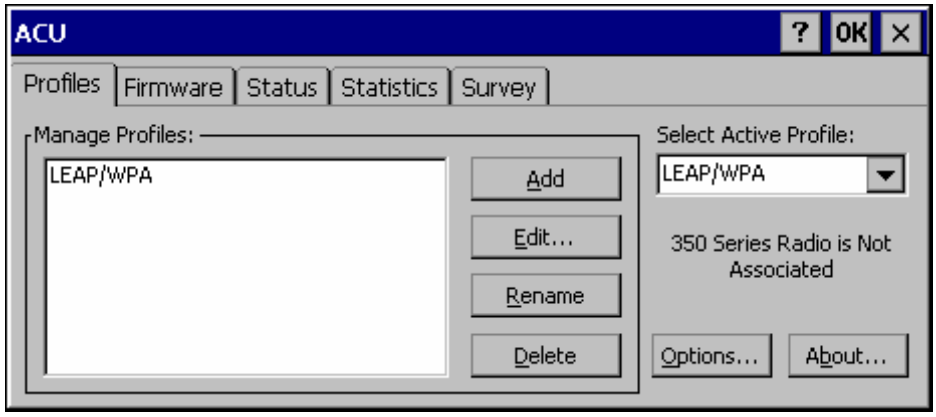


Figure 7-52 Renaming Profile

Click the Edit . . . button.

The profile properties screen is displayed.

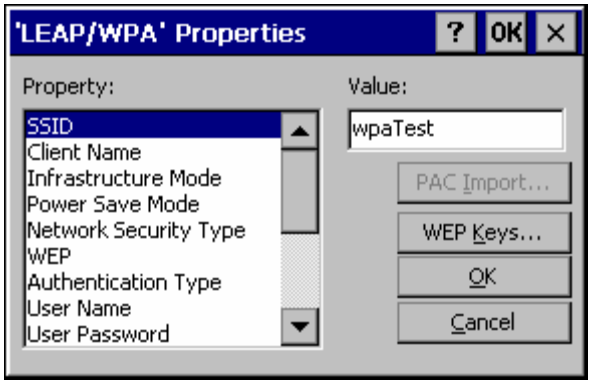


Figure 7-53 Profile Properties Screen

Enter the SSID and Client Name in the correct fields.

Set the Network Security Type to LEAP(WPA).

Click the OK button.

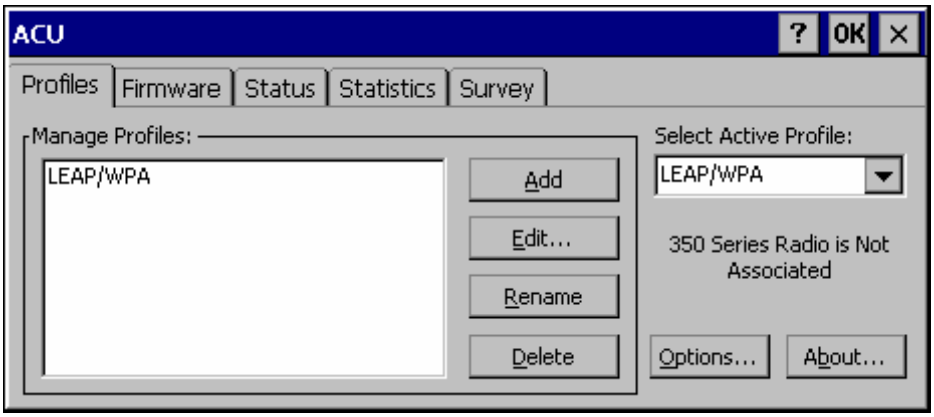


Figure 7-54 Select Profile

Use the drop down box to choose the profile just configured.

Click OK.

The mobile device associates and displays the sign on screen.

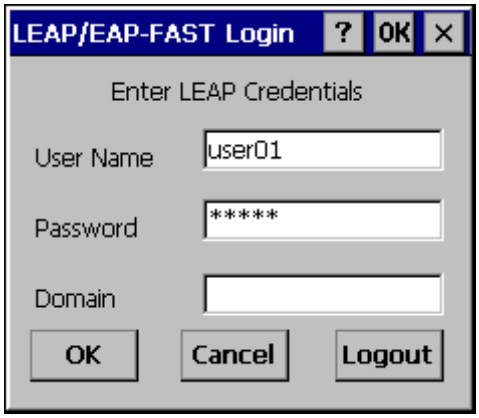


Figure 7-55 Login Screen

Click the Status tab to display status.

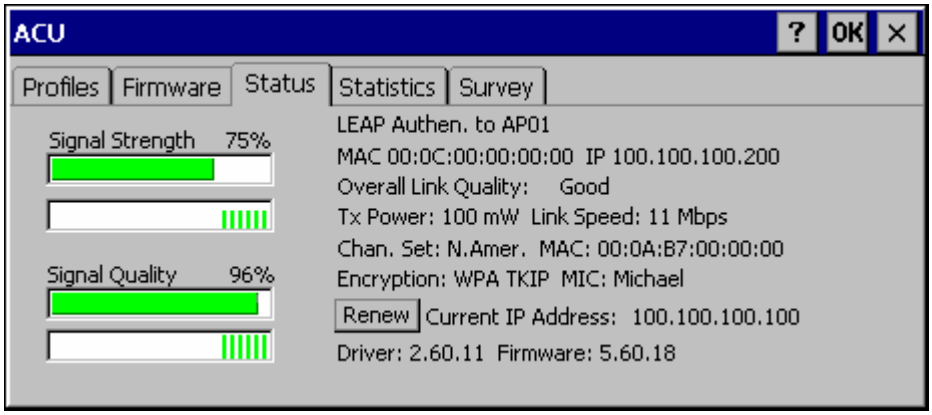


Figure 7-56 ACU Status Tab

EAP-TLS Authentication Configuration

To authenticate using the EAP-TLS protocol you need a user certificate file and a private key file. Once you have the user certificate files run the certificate installer from the Microsoft control panel. For EAP-TLS it does not matter which Cisco cab file is installed.

Note: It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificate

To check if a user certificate is installed navigate to **Start | Control Panel | Certificates**.

Set the drop down box to “My Certificates” as shown below.

The correct user certificate should be shown in the right pane.

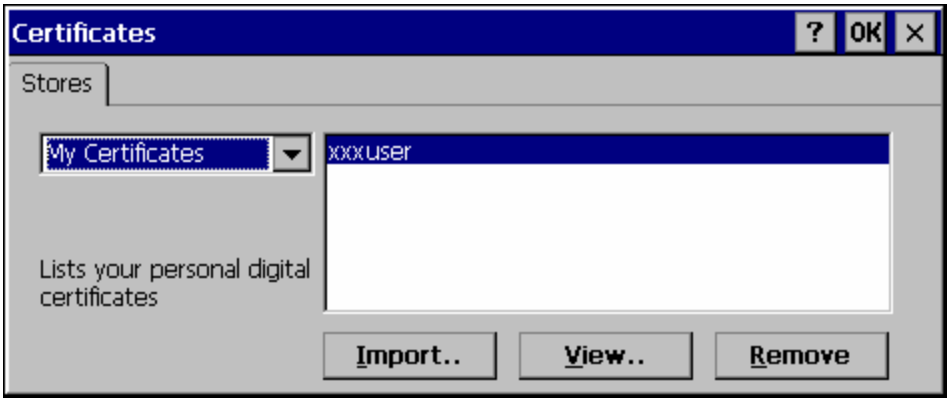


Figure 7-57 Certificate Stores

Click the View . . . button.

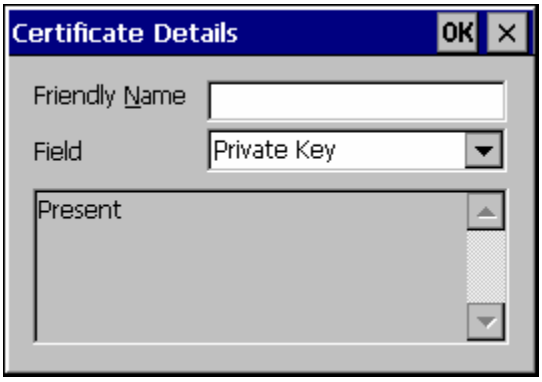


Figure 7-58 View Certificate Details

Set the **Field** to Private Key.

Make sure the private key is Present.

If it is not present, install the private key file.

If there is no user certificate refer to “User Certificates”, earlier in this chapter, to acquire a user certificate and private key file.

Setting EAP/TLS Parameters

With the radio parameters configured (see “Wireless Network Configuration”) set the EAP type to TLS as shown.

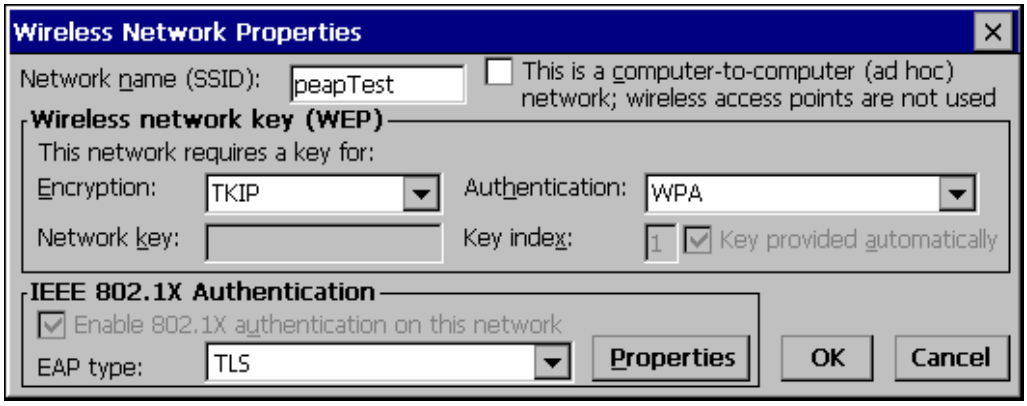


Figure 7-59 EAP/TLS Configuration

Click the **Properties** button.

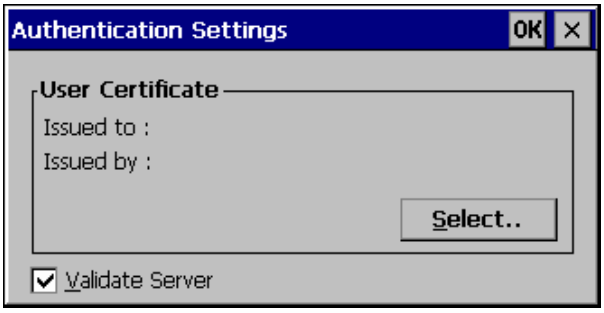


Figure 7-60 Authentication Settings

Click the **Select** button to choose the user certificate.

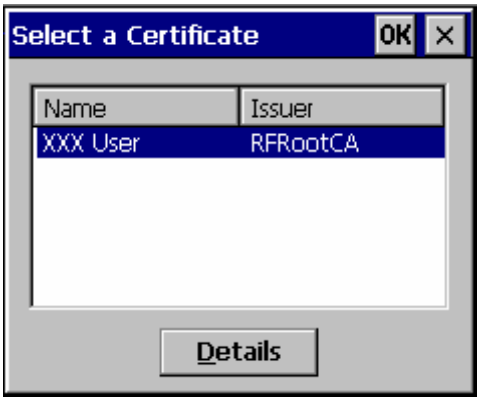


Figure 7-61 Select Certificate

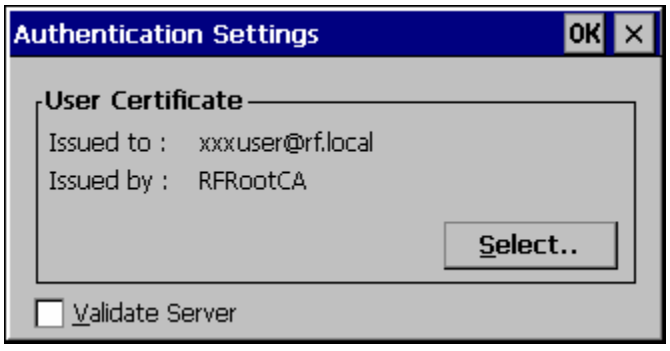


Figure 7-62 Authentication Settings, Certificate Details

Do *not* check the Validate server certificate box. This allows the user to be authenticated as the first step.

When the user certificate successfully authenticates, come back to this screen and validate the server certificate as described in the next section.

Click the OK button to dismiss the configuration screens.

When the radio re-connects the user is authenticated with the user certificate.

If the user does not authenticate, recheck the user certificate and the date on the computer.

Validating the Server Certificate

Before validating the server certificate, make sure the Root CA certificate is installed on the mobile device.

Navigate to the Wireless Network Properties configuration screen.

Click the **Properties** button.

Check the **Validate server** box as shown below.

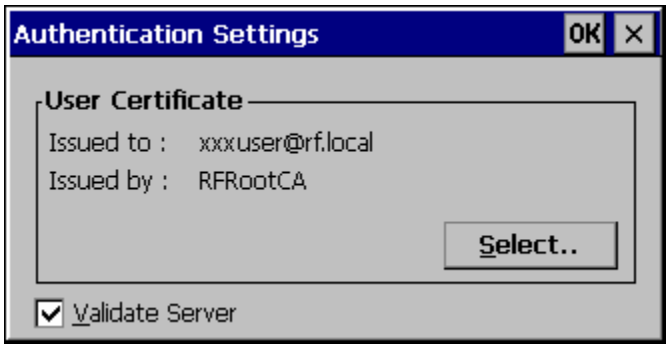


Figure 7-63 Validate Server

Click OK to dismiss the configuration boxes.

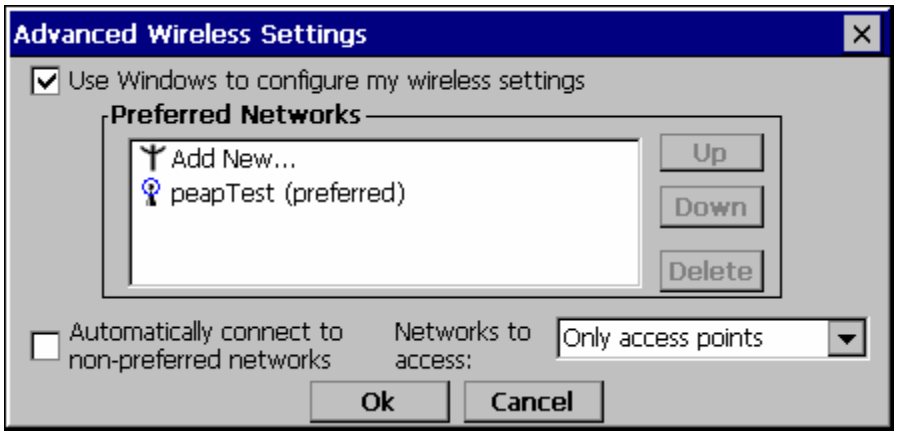


Figure 7-64 SSID Authenticated

Once the authentication completes the status changes to show the mobile device has authenticated to <SSID> as shown above.

WPA PSK Configuration

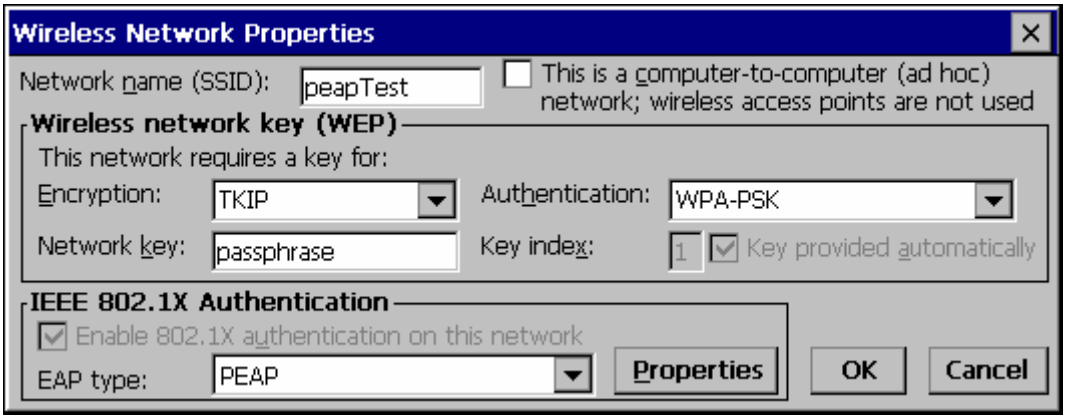


Figure 7-65 WPA PSK Configuration

Configure the Wireless Network Settings as described in “Wireless Network Settings”, earlier in this chapter.

Change the Network Authentication to **WPA-PSK**.

Enter an ASCII **network key** in the text field. Hex keys do not work in the Microsoft Zero Config utility at this time.

There is no server authentication when using WPA-PSK.

Click the OK button to complete the configuration.

Appendix A Key Maps

Keypad

Throughout this guide, an MX3X without an RFID Module is labeled "MX3X". The MX3X with an RFID Module is labeled "MX3-RFID". Information specific to one or the other is labeled appropriately. No distinction is made to information that is the same for both mobile devices.

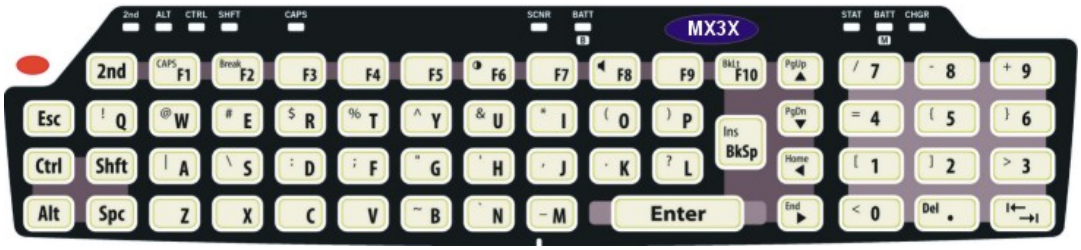


Figure A-1 QWERTY Keypad

Note: The key mapping in this appendix relates to the physical keypad. See section titled "Input Panel" for the Virtual (or Soft) Keypad used with the stylus.

Key Map 101-Key Equivalencies

Note: This key mapping is used on hand held computers that are NOT running an LXE Terminal Emulator.

When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.

Note: When the computer boots, the default condition of NumLock is On and the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with a 2nd+F1 key sequence. The CAPS LED is illuminated when CapsLock is On.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Contrast	x					F6
Volume	x					F8
Backlight	x					F10
2nd						2nd
Shift						Shft
Alt						Alt
Ctrl						Ctrl
Esc						Esc
Space						Spc
Enter						Enter

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Scan [3]						Scan
CapsLock (Toggle)	x					F1
Back Space						BkSp
Tab						Tab
BackTab	x					Tab
Break	x					F2
Pause	x	x				F3
Up Arrow						Up Arrow
Down Arrow						Down Arrow
Right Arrow						Right Arrow
Left Arrow						Left Arrow
Insert	x					BkSp
Delete	x					DOT
Home	x					Left Arrow
End	x					Right Arrow
Page Up	x					Up Arrow
Page Down	x					Down Arrow
ScrollLock	x	x				F4
F1						F1
F2						F2
F3						F3
F4						F4
F5						F5
F6						F6
F7						F7
F8						F8
F9						F9
F10						F10
F11	x	x				F1
F12	x	x				F2
a					Off	A
b					Off	B

[3] Left Scan key default value is Scan. Right Scan key default value is Enter. When RFID Module is installed, Right Scan key defaults to RFID Read and Left Scan key defaults to Scan or Enter or Field Exit (5250 only).

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
c					Off	C
d					Off	D
e					Off	E
f					Off	F
g					Off	G
h					Off	H
i					Off	I
j					Off	J
k					Off	K
l					Off	L
m					Off	M
n					Off	N
o					Off	O
p					Off	P
q					Off	Q
r					Off	R
s					Off	S
t					Off	T
u					Off	U
v					Off	V
w					Off	W
x					Off	X
y					Off	Y
z					Off	Z
A		x				A
B		x				B
C		x				C
D		x				D
E		x				E
F		x				F
G		x				G
H		x				H
I		x				I
J		x				J
K		x				K

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
L		x				L
M		x				M
N		x				N
O		x				O
P		x				P
Q		x				Q
R		x				R
S		x				S
T		x				T
U		x				U
V		x				V
W		x				W
X		x				X
Y		x				Y
Z		x				Z
1						1
2						2
3						3
4						4
5						5
6						6
7						7
8						8
9						9
0						0
DOT						DOT
<	x					0
[	x					1
]	x					2
>	x					3
=	x					4
{	x					5
}	x					6
/	x					7
-	x					8

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
+	x					9
*	x					I
: (colon)	x					D
; (semicolon)	x					F
?	x					L
`	x					N
_ (underscore)	x					M
, (comma)	x					J
‘ (apostrophe)	x					H
~ (tilde)	x					B
\	x					S
|	x					A
“	x					G
!	x					Q
@	x					W
#	x					E
$	x					R
%	x					T
^	x					Y
&	x					U
(	x					O
)	x					P

Creating Custom Key Maps

Prerequisite: LXE SDK CD

Introduction

A command-line compiler called KEYCOMP.EXE is provided on the SDK CD. Using this compiler, the System Administrator can convert a sample default key map text file into a custom key map text file which, when loaded onto the mobile device, can be chosen by the user to replace the default mobile device keymap and then switched back when they are finished using the customized keys. This custom key map file can be made to re-define the system return code for each of the 61 keys, key press or key press combinations. All keys, except the power key, can be re-mapped.

Custom keymaps for the mobile device are created on a desktop PC using the command line compiler KEYCOMP.EXE. Keycomp processes the input keymap source file and outputs a registry text file.

Note: Each VK_code has a numeric value (for example, VK_F20 = hex 83), these are documented in the SDK include file WINUSER.H (from Microsoft). The numeric value is what needs to go into the registry. Whether the value is hex or decimal depends on the registry editor being used - the one in the mobile device requires decimal, but the desktop one used over ActiveSync that a developer may use requires hex.

For Example
Default values: ScanCodeLeft = hex 83, decimal 131
ScanCodeRight = hex 84, decimal 132

Example:

KEYCOMP DEFAULT.KEY (writes KEYCOMP.REG to local directory)

Input File	→	Compiler	→	Text File
DEFAULT.KEY		KEYCOMP.EXE		KEYCOMP.REG

This output file should be renamed to **xxx.REG** (the suffix must remain REG), then copied to the mobile device over ActiveSync. Once the file is loaded on the mobile device, double-tap the file from the Windows CE Explorer desktop. This will run the REGLOAD utility to put it into the registry, and save the registry to non-volatile flash. The keymap is now a permanent part of the mobile device, and the REG file is no longer needed unless it is necessary to perform a cold boot; this will return the registry to factory defaults, and it will be necessary to double-tap the REG file again.

Once the keymap has been added to the registry, it should appear in the Keyboard control panel as the name given in the MAPNAME field in the key file. To activate the keymap, select the keymap from the popup menu, and close the control panel with the OK button. To return to the default keymap, select **0409** from the keymap popup and tap OK.

The compiler has three functional stages:

- First, the input file is read and parsed for any syntax errors. The data read is stored in internal tables.
- Second, the data parsed from the input file is validated to see that all of the items required by the keyboard driver for normal operation are present.

- Third and finally, the KEYCOMP.REG file is written out in the format required by the REGLOAD utility on the Windows CE device.

Programmable Scan Buttons and Custom Key Mapping

The Left and Right Scan buttons can be reset using Custom Key Mapping. Custom keymapping changes the placement of the buttons (e.g., F1 can now be Scan Left).

The keycode that the Scan Left (or F1) button generates is then determined by the setting in the scanner control panel (See Chapter 4 "System Configuration", Control Panel", "Scanner").

Remapping does not allow multiple entries. If the System Administrator uses Custom Key Mapping set a Scan button to ENTER, the original ENTER key must be redefined to something else. However, if the scanner control panel is used to change the Scan button to generate an ENTER, the original ENTER key is maintained as well.

Note: Tethered scanners are not activated/affected by the Scan buttons on the mobile device.

Keymap Source Format

The source file **DEFAULT.KEY** is supplied with the keymap compiler. This is the commented source for the default keymap **0409**. The comments in this file should make the majority of this document redundant. There is a copy of this file at the end of this section, in "Sample Input File**"**. This section should be read while referring to this sample source, for simplicity.

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

It is an important limitation that the keymap must have a 4, 5, or 6 digit numeric name; this is a limit of the Microsoft Windows CE layout manager.

The format of this file is familiar to anyone who has used .INI files under Windows. There is a section header in square brackets, followed by various values in the form *value=data*.

Lines beginning with a semicolon (;) or empty lines are ignored as comments. Spaces or tabs before or after the information are stripped off and ignored. Case is ignored in section names, value names, and value data.

*Note: Before connecting to a host using Remote Desktop Connection, go to **Start | Settings | Control Panel | Keyboard** and select **0409** from the keymap popup. Tap OK.*

COLxROWx Format

Note: There is no relationship between the physical layout COL/ROW of the keyboard / keypad and the COL/ROW listing in the key map file. The key map file represents the electrical layout not the physical layout.

All keys are specified in COLxROWx format. In this format, the first x is the 1 or 2 digit column in the keymap, and the second x is the 1 or 2 digit row in the keymap. All rows and columns are enumerated starting with zero (0).

In the **MAP** section, the **COLxROWx** is the value name, and the values must be less than the **MAPROWS** and **MAPCOLS** specified in the **GENERAL** section.

In the **SPECIAL** section, the **COLxROWx** is the value data, and the values given can be outside the normal key map limits.

GENERAL Section

The first section is the **GENERAL** section. This contains the keymap name (all numerics), as well as the number of rows and columns in the keymap, and the algorithm for converting rows and columns to a data byte to go into the keymap table.

```
.
[General]
MAPNAME=0409
MAPCNT=4
.
```

MAPNAME	Name of this map. This is what appears in the popup menu in the keyboard control panel.
MAPCNT	Gives the number of MAP sections (and hence keymap tables) in this source file.
MAPCOLS	Number of columns in each keymap table. This is defined by the hardware keyboard.
MAPROWS	Number of rows in each keymap table. This is defined by the hardware keyboard.
ALGOR	Defines the algorithm for converting row/column to internal scan code. Current values are: MX3X scancode = ((column << 3) + row)

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

SPECIAL Section

```
.
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
.
```

The second section is the **SPECIAL** section, which contains the row and column definitions for certain modifier keys which must be processed independent of the overall keymap. Currently, these are only modifier keys.

The only recognized names are: **KEYSHIFT**, **KEYALT**, **KEY2ND**, and **KEYCONTROL**, and these specify the row and column of these 4 specific modifier keys, in COLxROWx format. Note the row and column for these keys can be outside the keymap limits specified in the **GENERAL** section, since these are not loaded as part of the keymap proper.

MAP Section

```
.
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
.
```

There will be several (4 to 7) **MAP** sections, each defining the keymap for a given combination of modifier keys. The keyboard driver requires keymaps for normal (no modifiers), SHIFT only, 2ND only, and 2ND-SHIFT combined.

The CTRL modifier and ALT modifier do not have individual keymaps; the keystrokes are passed to the operating system, which is allowed to parse these keys according to Microsoft specifications (for example, ALT-keys are defined to only pulldown menus, with no other function).

The only recognized value names are **MAP** and **COLxROWx** (defining a key code). The only valid values for **MAP** are:

MAP_NORMAL	no modifier keys
MAP_2ND	2nd modifier only
MAP_SHIFT	shift modifier only
MAP_2NDSHF (or) MAP_2NDSHIFT	2nd and shift modifiers together

In addition, certain keymaps are used for special adjustment functions within the keyboard driver, via the **CHANGE+mapname** specification:

MAP_VOLUM (or) MAP_VOLUME	special keymap for volume adjustment
MAP_CONTR (or) MAP_CONTRAST	special keymap for contrast adjustment
MAP_BRITE (or) MAP_BRIGHT	special keymap for brightness adjustment

When these maps are selected, the keyboard driver handles the up arrow and down arrow as adjusting the particular parameter up and down, and any other key exits the adjustment state. Keys in these modes are handled completely inside the keyboard driver, and are not propagated to the operating system.

Key codes are defined by **COLxROWx=scancode**. **Scancode** has a number of options, as follows:

VK_code	any valid Windows VK code (see below for valid codes)
'x'	a single ASCII character ('A','b','1','@',' ', etc.)
SHIFT+VK_code	for a shifted VK code (see below for valid codes)
SHIFT+'x'	for a shifted ASCII character (should not be needed)
ACTION+code	special function key (valid codes listed below)
CHANGE+mapname	for modifier keys, change keymaps to mapname, as specified above
OPEN	an unused key position, does nothing when pressed

Valid **ACTION** codes are as follows:

SCAN1	Scan key 1 (left side of screen on mobile device)
SCAN2	Scan key 2 (right side of screen on mobile device)
SCAN3	Handle trigger button (unused on mobile device, but specified)
POWER	power button
BACKLIGHT	backlight on/off function

Note that specifying the power button in a different location will affect suspend/resume functions. The "15-second hold to force reboot" function is controlled by hardware, and will only work with the default power button.

Keycomp Error Messages

Most error messages will specify the line within the keymap source file where the error occurred.

Duplicate key

A COLxROWx code was found in a MAP table, but that COL/ROW already has a value assigned.

GENERAL section must come before MAP

The GENERAL section must come first, or at least before any MAP sections. The GENERAL section defines parameters which are needed to process Maps

Header line missing close bracket

The section header line must have square brackets before and after the section name

Header line missing open bracket

The section header line must have square brackets before and after the section name

Invalid ACTION code %s

The key scan code is specified as ACTION+code, but the ACTION code parsed is not recognized. The following values are valid: SCAN1, SCAN2, SCAN3, POWER, or BACKLIGHT.

Invalid keycode %s

The keycode parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A' or '#').
- OPEN for unused entries (will not do anything when pressed)

Invalid MAP value %s

The MAP value parsed is not one the following list: MAP_NORMAL, MAP_2ND, MAP_SHIFT, MAP_2NDSHF, MAP_2NDSHIFT, MAP_VOLUM, MAP_VOLUME, MAP_CONTR, MAP_CONTRAST, MAP_BRITE, or MAP_BRIGHT.

Invalid MAPCNT (1-%d valid)

The specified MAPCNT exceeds the limits of the KEYCOMP compiler.

Invalid MAPCOLS (1-%d valid)

The specified MAPCOLS exceeds the limits of the KEYCOMP compiler.

Invalid MAPROWS (1-%d valid)

The specified MAPROWS exceeds the limits of the KEYCOMP compiler.

Invalid ROWCOL format

A COLxROWx was expected, but the format was not correct. The only valid formats are: COLxROWx, COLxxROWx, COLxROWxx, or COLxxROWxx, where xx are decimal numeric digits (0-9).

Invalid scan code

The scan code parsed is not recognized. The scan code can take one of the following formats:

- VK_code
- 'x'
- SHIFT+VK_code
- SHIFT+'x'
- ACTION+code
- CHANGE+mapname
- OPEN

Invalid section name %s

The section name parsed is invalid. The only recognized names are: GENERAL, SPECIAL, or MAP

Invalid SHIFT code %s

The key scan code is specified as SHIFT+code, but the SHIFT code parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A', '3', or '#').

Invalid value %s in GENERAL section

The value name parsed is invalid for the GENERAL section. The recognized names are: MAPNAME, MAPCNT, MAPCOLS, MAPROWS, or ALGOR

Invalid value %s in MAP section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: MAP and COLxxx.

Invalid value %s in SPECIAL section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: KEYSHIFT, KEYALT, KEY2ND, and KEYCONTROL.

Invalid VK_ code %s

The VK code parsed is not recognized. See the VK Code Table (below) for valid values.

Map ended without MAP value

The MAP section must contain a MAP value, so the data fields can be parsed.

MAPNAME must be all numerics

Because of limitations in Microsoft Layout Manager, the map name must be all numeric (4, 5, or 6 digits). The name parsed did not fit this limitation.

No definition for map MAP_2ND

There is no 2nd keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_2NDSHIFT

There is no 2nd-SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_NORMAL

There is no Normal keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_SHIFT

There is no SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.key2nd

No 2ND modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyalt

No ALT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keycontrol

No CTRL modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keydnarrow

No down arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keypower

No power key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan1

No Scan Key 1 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan2

No Scan Key 2 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan3

No Trigger Button definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyshift

No SHIFT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyuparrow

No up arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No equal in value line

A value line must be of the form *value=data*. A value line was expected, but there was no equal in it. *(or)* A comment line did not begin with a semicolon (;).

No MAPNAME defined

There is no map name defined. The keyboard driver requires this name to be able to load the keymap tables. This message comes from the post-parse validation, so no line # is specified.

Scan code algorithm required

A COLxROWx data value was found before any ALGOR statement. ALGOR algorithm is parsed to decide how to encode COLxROWx into a keymap value.

Too many maps for specified MAPCNT

There are more MAP sections defined that the MAPCNT field specified.

Unknown scan code algorithm

The ALGOR algorithm specified is not one that KEYCOMP understands.

Unrecognized scancode algorithm %s

The ALGOR algorithm specified is not one that KEYCOMP understands.

Value outside of section

A value (defined as *value=data*) is only valid within a section (defined as *[section]*). A value line was found when a section header line was expected.

Sample Input File

```
;;-----------------------------------------------------
;; keymap file for MX3X default keyboard
;;-----------------------------------------------------

;;-----------------------------------------------------
;; general parms give the size of arrays
;; all numeric values are decimal
;; these numbers are validated with the data below
;; at compile time
;; MAPNAME must be all numerics
;;-----------------------------------------------------
[General]
MAPNAME=0409
MAPCNT=4
MAPCOLS=8
MAPROWS=8
ALGOR=MX3X

;;-----------------------------------------------------
;; special keys are accessed outside the map
;; this specifies the row and column
;; these should not need to change, but...
;;-----------------------------------------------------
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
KEY2ND=COL10ROW0
KEYCONTROL=COL11ROW0

;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with no modifier
;;-----------------------------------------------------
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=VK_F7
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0='Q'
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3='T'
COL1ROW4='U'
COL1ROW5='4'
```

```
COL1ROW6='O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0='A'
COL2ROW1=open
COL2ROW2='D'
COL2ROW3='G'
COL2ROW4='J'
COL2ROW5='1'
COL2ROW6='L'
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=' '
COL3ROW1=open
COL3ROW2='X'
COL3ROW3='V'
COL3ROW4='N'
COL3ROW5='0'
COL3ROW6=VK_LEFT
COL3ROW7=VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=VK_F9
COL4ROW1='S'
COL4ROW2=VK_RIGHT
COL4ROW3='F'
COL4ROW4='H'
COL4ROW5='K'
COL4ROW6='2'
COL4ROW7=VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1='Z'
COL5ROW2=VK_BACK
COL5ROW3='C'
COL5ROW4='B'
COL5ROW5='M'
COL5ROW6=VK_PERIOD
COL5ROW7=VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=VK_F10
COL6ROW1='W'
COL6ROW2=VK_RETURN
COL6ROW3='R'
COL6ROW4='Y'
COL6ROW5='I'
COL6ROW6='5'
COL6ROW7='P'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0='E'
COL7ROW1=open
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4=VK_F6
COL7ROW5='7'
COL7ROW6=VK_F8
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only 2ND
;;-----------------------------------------------------
[Map]
MAP=MAP_2ND
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_CAPITAL
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_PAUSE
COL0ROW4=open
COL0ROW5=open
COL0ROW6=VK_HYPHEN
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'1'
COL1ROW1=SHIFT+VK_EQUAL
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'5'
COL1ROW4=SHIFT+'7'
COL1ROW5=VK_EQUAL
COL1ROW6=SHIFT+'9'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+VK_BACKSLASH
COL2ROW1=open
COL2ROW2=SHIFT+VK_SEMICOLON
COL2ROW3=SHIFT+VK_APOSTROPHE
COL2ROW4=VK_COMMA
COL2ROW5=VK_LBRACKET
COL2ROW6=SHIFT+VK_SLASH
COL2ROW7=SHIFT+VK_PERIOD
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=VK_BACKQUOTE
COL3ROW5=SHIFT+VK_COMMA
COL3ROW6=VK_HOME
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=VK_BACKSLASH
COL4ROW2=VK_END
COL4ROW3=VK_SEMICOLON
COL4ROW4=VK_APOSTROPHE
COL4ROW5=VK_PERIOD
COL4ROW6=VK_RBRACKET
COL4ROW7=VK_PRIOR
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+VK_RBRACKET
COL5ROW1=open
```

```
COL5ROW2=VK_INSERT
COL5ROW3=open
COL5ROW4=SHIFT+VK_BACKQUOTE
COL5ROW5=SHIFT+VK_HYPHEN
COL5ROW6=VK_DELETE
COL5ROW7=VK_NEXT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=ACTION+BACKLIGHT
COL6ROW1=SHIFT+'2'
COL6ROW2=open
COL6ROW3=SHIFT+'4'
COL6ROW4=SHIFT+'6'
COL6ROW5=SHIFT+'8'
COL6ROW6=SHIFT+VK_LBRACKET
COL6ROW7=SHIFT+'0'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'3'
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=CHANGE+MAP_CONTRAST
COL7ROW5=VK_SLASH
COL7ROW6=CHANGE+MAP_VOLUME
COL7ROW7=open

;;-------------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with 2ND and SHIFT
;;-------------------------------------------------------
[Map]
MAP=MAP_2NDSHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=open
COL0ROW5=open
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=open
COL1ROW4=open
COL1ROW5='4'
COL1ROW6=open
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=open
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=open
```

```
COL2ROW5='1'
COL2ROW6=open
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5='0'
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=open
COL4ROW3=open
COL4ROW4=open
COL4ROW5=open
COL4ROW6='2'
COL4ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1=open
COL6ROW2=open
COL6ROW3=open
COL6ROW4=open
COL6ROW5=open
COL6ROW6='5'
COL6ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=VK_PAUSE
COL7ROW3=VK_SCROLL
COL7ROW4=VK_SNAPSHOT
COL7ROW5='7'
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only SHIFT
;;-----------------------------------------------------
[Map]
MAP=MAP_SHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=SHIFT+VK_ESCAPE
COL0ROW1=SHIFT+VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_F2
COL0ROW4=SHIFT+VK_F5
COL0ROW5=SHIFT+VK_F7
COL0ROW6=SHIFT+'8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'Q'
COL1ROW1=SHIFT+'9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'T'
COL1ROW4=SHIFT+'U'
COL1ROW5=SHIFT+'4'
COL1ROW6=SHIFT+'O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+'A'
COL2ROW1=open
COL2ROW2=SHIFT+'D'
COL2ROW3=SHIFT+'G'
COL2ROW4=SHIFT+'J'
COL2ROW5=SHIFT+'1'
COL2ROW6=SHIFT+'L'
COL2ROW7=SHIFT+'3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=SHIFT+' '
COL3ROW1=open
COL3ROW2=SHIFT+'X'
COL3ROW3=SHIFT+'V'
COL3ROW4=SHIFT+'N'
COL3ROW5=SHIFT+'0'
COL3ROW6=SHIFT+VK_LEFT
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=SHIFT+VK_F9
COL4ROW1=SHIFT+'S'
COL4ROW2=SHIFT+VK_RIGHT
COL4ROW3=SHIFT+'F'
COL4ROW4=SHIFT+'H'
COL4ROW5=SHIFT+'K'
COL4ROW6=SHIFT+'2'
COL4ROW7=SHIFT+VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+'6'
COL5ROW1=SHIFT+'Z'
```

```
COL5ROW2=SHIFT+VK_BACK
COL5ROW3=SHIFT+'C'
COL5ROW4=SHIFT+'B'
COL5ROW5=SHIFT+'M'
COL5ROW6=SHIFT+VK_PERIOD
COL5ROW7=SHIFT+VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=SHIFT+VK_F10
COL6ROW1=SHIFT+'W'
COL6ROW2=SHIFT+VK_RETURN
COL6ROW3=SHIFT+'R'
COL6ROW4=SHIFT+'Y'
COL6ROW5=SHIFT+'I'
COL6ROW6=SHIFT+'5'
COL6ROW7=SHIFT+'P'
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'E'
COL7ROW1=open
COL7ROW2=SHIFT+VK_F3
COL7ROW3=SHIFT+VK_F4
COL7ROW4=SHIFT+VK_F6
COL7ROW5=SHIFT+'7'
COL7ROW6=SHIFT+VK_F8
COL7ROW7=open
```

Sample Output File

```
[HKEY_CURRENT_USER\Keyboard Layout\0409]
;; header limits and special keys
;;   MAPCNT
;;   MAPCOLS
;;   MAPROWS
;;   # of keys in each map
;;   (unused)
;;   (unused)
;;   scancode value for power key
;;   scancode value for up arrow
;;   scancode value for down arrow
;;   scancode value for scan key 1
;;   scancode value for scan key 2
;;   scancode value for trigger button
;;   scancode value for SHIFT
;;   scancode value for ALT
;;   scancode value for 2ND
;;   scancode value for CTRL key
"Head"=hex: 04,08,08,40,00,00,02,27,2F,07,0F,0A,40,48,50,58

;; Map0 is the scancode values for the NORMAL key map
"Map0"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag0 is the shift codes for the NORMAL key map
"Flag0"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map1 is the scancode values for the 2ND key map
"Map1"=hex:\
    00,14,DF,13,00,00,BD,87,31,BB,89,35,37,BB,39,88,\
    DC,00,BA,DE,BC,DB,BF,BE,00,00,00,00,C0,BC,24,09,\
    00,DC,23,BA,DE,BE,DD,21,DD,00,2D,00,C0,BD,2E,22,\
    8A,32,00,34,36,38,DB,30,33,00,00,00,00,BF,00,00

;; Flag1 is the shift codes for the 2ND key map
"Flag1"=hex:\
    00,00,A0,10,00,86,00,A0,10,10,A0,10,10,00,10,A0,\
    10,00,10,10,00,00,10,10,00,00,00,00,00,10,00,10,\
    00,00,00,00,00,00,00,00,10,00,00,00,10,10,00,00,\
    A0,10,00,10,10,10,10,10,10,00,00,00,85,00,84,00

;; Map2 is the scancode values for the 2ND-SHIFT key map
"Map2"=hex:\
    00,7A,DF,7B,00,00,38,87,00,39,89,00,00,34,00,88,\
    00,00,00,00,00,31,00,33,00,00,00,00,00,30,00,00,\
    00,00,00,00,00,00,32,00,36,00,00,00,00,00,00,00,\
```

```
    00,00,00,00,00,00,35,00,00,00,13,91,2C,37,00,00

;; Flag2 is the shift codes for the 2ND-SHIFT key map
"Flag2"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map3 is the scancode values for the SHIFT key map
"Map3"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag3 is the shift codes for the SHIFT key map
"Flag3"=hex:\
    10,10,A0,10,10,10,10,A0,10,10,A0,10,10,10,10,A0,\
    10,00,10,10,10,10,10,10,10,00,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,00,10,10,10,10,10,00
```

List of Valid VK Codes for CE .NET

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 .NET.

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	

Appendix B Technical Specifications

Physical Specifications

Features		Specifications	Comments	
CPU		Xscale PXA255 CPU operating at 400 MHz. Turbo mode switching is supported.	32 bit CPU (with on-chip cache)	
Compact Flash (Internal)		Supports an ATA interface only.	3.3v ATA flash card. Inaccessible by customer.	
Memory	ROM RAM	64 MB Flash 64 or 128MB of SDRAM	 System Memory	
Display	LCD	Monochrome Transflective Transmissive Color	Transflective LCD with touchscreen. Customer Configurable Backlighting	
Mass Storage	Removable PC Card	SRAM or Flash PCMCIA Type I or II PC Cards (Various Sizes) Compact Flash Card	Bootable SRAM PC Card, ATA Flash PC Card, or ATA Hard Drive PC Card (Customer Installable)	
PCMCIA Interface		Slot 0 accepts Type I and II Slot 1 accepts Type I and II CF+	Compatible with the PCMCIA version 2.1 standard.	
Weights		Unit with radio, battery and scanner endcap	Less than 30 oz	<850g 1128.3g for RFID
		Battery	5.6 oz	157g
		Radio Card - 2.4GHz Type II	1.0 oz 1.6 oz	28g 45g
		SRAM Card	1 oz	28g
External Connectors/Interface USB Host / Client Ports		IrDA Connector (COM 2) bi-directional half-duplex	Supports 115k baud	
		Endcap - Dual Serial, DA-9 or DB-9 Connector (COM 1 and COM 3)	9 Pin “D” (male) Connector. Provides connection to external devices such as a printer.	
		Endcap - incl Scanner (COM 3), DA-9 or DB-9 Connector (COM 1)	9 Pin “D” (male) Connector. Provides connection to external devices such as a printer.	
		Endcap – incl Scanner (COM 3), DA-9 (COM 1)	Scanner – SE923 Symbol engine	

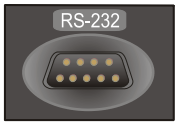
Features		Specifications	Comments	
Power Connector		8.5V - 15 VDC Input Power	External Battery Charger Contacts	
		10.8 - 16VDC Input Power	Power Jack	
Audio Connector			Audio Jack	
Dimensions w/Endcap		Length	6”	15 cm
		Width	8”	20 cm
		Depth (No RFID)	1.44”	3.66 cm
		Depth (With RFID Module)	1.88”	4.77 cm
Batteries	Main	1900 mAh 10.8V, 3 cell, Li-Ion battery pack	In-Unit Chargeable or Externally Chargeable	
	Backup (CMOS)	Internal Nickel-Cadmium (NiCd) 5.7V max.	Automatically charges from main battery during normal operation Memory operational for 5 minutes when main battery is depleted	

Display Specifications

Type	LCD - Transflective Monochrome, Transmissive Color Electroluminescent Backlighting
Resolution	640x240 pixels
Size	½ VGA landscape
Diagonal Viewing Area	5.92 in (150.4mm)
Dot Pitch	0.22mm
Dot Size	0.20mm x 0.20mm
Color Scale	Monochrome - 16 Shades of Gray Transmissive – 256 colors

Cable Specifications

Caution: Do Not Use this Port for Cables with USB Plugs/Receptacles:



Caution: Do Not Use these Labeled Ports for Tethered Scanners:

Cable Ends

Receptacle	Plug	Receptacle	Plug
 USB A	 USB A	 RS232	 RS232
 USB B	 USB B		

Cable Pinouts and Diagrams

MX3X068CBLD9USBHOST – CBL, USB D9F to USB Type A Receptacle

ActiveSync: Connect from mobile device USB-C port to USB Type A Host. E.g. laptop/desktop PC.

Mobile Device Client End	Goes To	USB Type A Plug End
1	Host Detect	1
2	Not Used	
3	D+	3
4	Not Used	
5	GND	4
6	Not Used	
7	D-	2
8	Not Used	
9	Not Used	

MX3XA069CBLD9USBCLNT – CBL, USB D9F to USB Type A Plug

Connect from MX3X USB-H port to USB Type B device. e.g. Hub, camera, other client device, etc.

Mobile Device Host port End	Goes To	USB Type B Plug End
1	Not Used	
2	Not Used	
3	D+	3
4	Not Used	
5	GND	4
6	Not Used	
7	D-	2
8	Not Used	
9	PWR	1

MX3XA070CBLD9RS232AS - Cable, RS232 (D9F) / RS232 (D9F)

ActiveSync: Connect from desk cradle male serial port to a D9 male serial port on a PC / Laptop. Cable used for serial ActiveSync.

MX3XA068CBLD9USBHOST – CBL, USB D9F to USB Type B Plug

Connect from mobile device USB-H to a USB device with a cable that has a Type A plug end. e.g. USB mouse, USB keyboard, etc.

Mobile Device Host port End	Goes To	USB Type A Receptacle End
1	Not Used	
2	Not Used	
3	D+	3
4	Not Used	
5	GND	4
6	Not Used	
7	D-	2
8	Not Used	
9	PWR	1

9000A054CBL6D9D9 - Cable, RS232 (D9F) / RS232 (D9F)

Null Modem Cable

D9 Female	D9 Female
1	7
2	3
3	2
4	6,8
5	5
6,8	4
7	1
9	Not Used

Tethered Scanner: Connect to MX3X powered Cradle D9F Serial port.

RS232 Tethered Scanner Serial Port on Cradle

Do Not Use these Endcap Labeled Ports for Tethered Scanners:

Environmental Specifications

Mobile Device and Endcaps

Operating Temperature	-4°F to 122°F (-20°C to 50°C) monochrome 32°F to 122°F (0°C to 50°C) color
Storage Temperature	-22°F to 158°F (-30°C to 70°C)
Water and Dust, MX3X Water and Dust, MX3-RFID	IEC IP66 IEC IP55
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Ambient Light – ranging from total darkness to direct sunlight	Display readable (with backlight on) for <= two hours Keypad readable (after previous exposure to a 60W bulb for 30 minutes) for <= 15 minutes.
Contamination	Resistant to exposure to skin oil and other lubricants.
Vibration	Based on MIL Std 810F
ESD	8 KV air, 4kV direct contact
Shock, MX3X	Multiple 4 foot drops to concrete. 6 foot with protective cover/boot

Power Supplies

US AC Wall Adapter

Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Thermal Fuse
Input Voltage	108VAC min - 132VAC max
Input Frequency	47 - 63 Hz
Input Connector	North American wall plug, no ground
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11.5mm, Center Positive
Output Voltage	+12VDC, unregulated
Output Current	0 Amps min, 1.5 A max
Operating Temperature	32° F to 104° F / 0° C to 40° C
Storage Temperature	-13° F to 158° F / -25° C to 70° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

International AC Adapter

Operating Temperature	32°F to 104°F (-0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Input Power Switch	None
Power "ON" Indicator	None
Input Voltage	108VAC min - 264VAC max
Input Frequency	47 - 63 Hz
Input Connector	Customer supplied
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11mm, Center Positive
Output Voltage	+12VDC, regulated
Output Voltage Regulation	+/- 5%
Output Current	0 Amps min, 1.00 Amps max

Radio Specifications

PCMCIA Cisco 2.4GHz Type II

Bus Interface	PCMCIA 2.0, Type II slot
Radio Frequencies	2.4 - 2.4835 GHz IEEE 802.11b DS SS
RF Data Rates	11 Mbps
RF Power Level	100 mW max.
Channels	11 US, 13 Europe, 4 France, 14 Japan
Operating Temperature	see Environmental Specs
Storage Temperature	see Environmental Specs
Connectivity	Novell, TCP/IP, Ethernet, ODI
Antenna	Internal

PCMCIA Symbol 11Mb 2.4GHz Type II

Bus Interface:	PCMCIA 2.0, Type II slot
Radio Frequencies:	2.4 - 2.5 GHz IEEE 802.11b DS SS
RF Data Rates:	11 Mbps maximum
RF Power Level:	100 mW
Channels	11 US, 13 Europe, 4 France, 1 Japan
Operating Temperature	see Environmental Specs
Storage Temperature	see Environmental Specs
Connectivity:	TCP/IP, Ethernet, NDSI

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z