

# MX8 Reference Guide

(Microsoft® Windows® CE 5.0 Equipped)



# LXE

Copyright © 2007 by LXE Inc.  
All Rights Reserved  
E-EQ-MX8RG-A



## Notices

LXE Inc. reserves the right to make improvements or changes in the products described in this document 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 document and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

---

### Copyright:

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

---

### Trademarks:

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

**Microsoft®**, **ActiveSync®**, **MSN**, **Outlook®**, **Windows®**, the Windows logo, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

**Summit Data Communications, Inc.** Summit Data Communications, the Summit logo, and “The Pinnacle of Performance” are trademarks of Summit Data Communications, Inc.

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

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

**Hand Held®** is a registered trademark of Hand Held Products, Inc., located in Skaneateles Falls, NY.

**Wavelink®**, the Wavelink logo and tagline, **Wavelink Studio™**, **Avalanche Management Console™**, **Mobile Manager™**, **Avalanche Mobility Center™**, **Avalanche MC™**, and **Mobile Manager Enterprise™** are trademarks of Wavelink Corporation, Kirkland.

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

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

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



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

# Table of Contents

<b>CHAPTER 1 INTRODUCTION</b>	<b>1</b>
<b>Overview</b>	<b>1</b>
Features	2
Important Battery Information	3
When to Use This Guide	3
Document Conventions	4
<b>Components</b>	<b>5</b>
Front	5
Back	6
Scanner / Imager Aperture	7
Trigger Handle	7
Handstrap	8
I/O Port and Cables	9
MX8 AC Adapter	10
<b>Quick Start</b>	<b>11</b>
Troubleshooting	12
Related Manuals for Startup	12
Entering the AppLock Activation Key	12
Hotkey	12
Touch	12
<b>Hardware Setup</b>	<b>13</b>
Installing Trigger Handle (Optional)	13
Installing the Handstrap	14
Inserting a Fully Charged Battery	15
About Lithium-Ion Batteries	15
Connecting an External Power Supply (Optional)	16
Putting it all together	16
Assembling the 5V AC Power Adapter	16
Connecting the Multipurpose USB / Power Cable	17
Connecting the Multipurpose RS-232 / Power Cable	18
Connecting the Audio Cable and a Headset	19
Adjust Microphone and Secure the Cable	19
<b>Power Key</b>	<b>20</b>
<b>Tapping the Touchscreen with a Stylus</b>	<b>21</b>
Keypad Shortcuts	21
<b>Software Setup</b>	<b>22</b>
Touchscreen Calibration	22
Set Time Zone (Optional)	22
Enter Owner Information (Optional)	22
Set the Display Backlight Timer	22
Set the MX8 Power Schemes Timers	23
Set The Audio Speaker Volume	24
Using the Keypad	24
Using the Touchscreen	24
Applying the Protective Film to the Display	25
Copy the MX8 LX Ebook to the MX8 (Optional)	25
<b>Wireless Client and Network Setup</b>	<b>26</b>
<b>Terminal Emulation Setup</b>	<b>26</b>
<b>Installing User Certificates and Private Keys</b>	<b>27</b>
User Certificate	27

Private Key.....	28
<b>Bluetooth .....</b>	<b>29</b>
Initial Use.....	29
Settings Tab   Bluetooth Options.....	29
Report when connection lost.....	30
Report when reconnected.....	30
Report failure to reconnect.....	30
Computer is connectable.....	30
Computer is discoverable.....	30
Prompt if devices request to pair.....	30
Continuous Search.....	30
Subsequent Use.....	31
Bluetooth Devices.....	32
Bluetooth Barcode Reader Setup.....	33
Introduction.....	33
MX8 with Label.....	34
MX8 without Label.....	34
Bluetooth Beep and LED Indications.....	35
<b>Entering Data.....</b>	<b>36</b>
Using the Keypad.....	36
Using the Input Panel or Virtual Keyboard.....	36
Using the Stylus.....	37
Using the Scanner.....	38
Voice Data.....	38
Tethered Scanners.....	38
<b>Getting Help.....</b>	<b>39</b>
Manuals.....	39
Accessories.....	39

---

## **CHAPTER 2 PHYSICAL DESCRIPTION AND LAYOUT** **43**

---

<b>Hardware Configuration .....</b>	<b>43</b>
System Hardware.....	43
Central Processing Unit.....	43
Core Logic.....	43
System Memory.....	44
Internal Mini SD Memory Card.....	44
Clear Registry.....	44
Video Subsystem.....	44
Power Supply.....	45
Main Battery Pack.....	45
Backup Battery.....	45
Wireless Client.....	45
802.11b/g.....	45
COM Port.....	46
RS-232 Serial Port.....	46
USB Client Port.....	46
Audio Headset Connection.....	46
Audio Support.....	47
Speaker.....	47
Volume Control.....	47
Voice.....	47
Scanner/Imager Port.....	47
<b>Power Key.....</b>	<b>48</b>
<b>Reboot Sequences.....</b>	<b>48</b>
Suspend / Resume.....	48

Warm Boot.....	48
Cold Boot.....	48
Reset to Default Settings.....	49
<b>Saving Changes to the Registry.....</b>	<b>49</b>
<b>Mini SD card .....</b>	<b>50</b>
Mini SD card Insertion / Removal .....	50
<b>Power Modes .....</b>	<b>51</b>
On Mode .....	51
The Display .....	51
The MX8.....	51
Suspend Mode.....	52
The MX8.....	52
Off Mode.....	52
<b>Bluetooth LXEZ Pairing.....</b>	<b>52</b>
<b>The Keypad.....</b>	<b>53</b>
Mappable Diamond Keys.....	54
LED Indicators.....	55
System Status .....	55
Scan Status .....	55
Alpha Mode (Alph Key) .....	55
Standard Keys .....	56
Function Keys .....	56
Sticky Keys .....	56
Mode Key Functions.....	58
CapsLock Mode .....	58
Example.....	58
<b>Touchscreen.....</b>	<b>59</b>
Display Backlight Timer .....	59
Cleaning the Display/Scanner Aperture.....	59
<b>Power Supply .....</b>	<b>60</b>
Checking Battery Status.....	60
MX8 Status LED and the Batteries .....	60
Main Battery Pack.....	60
Battery Hotswapping.....	61
Low Battery Warning.....	61
Backup Battery.....	61
Handling Batteries Safely .....	62
Battery Maintenance Publication .....	62
<b>MX8 Multi-Charger (Optional).....</b>	<b>63</b>
Multi-charger LEDs .....	63
<b>MX8 Cradles (Optional) .....</b>	<b>64</b>

---

## **CHAPTER 3 SYSTEM CONFIGURATION** **65**

---

<b>Introduction .....</b>	<b>65</b>
<b>Windows CE 5.0 .....</b>	<b>65</b>
<b>Installed Software .....</b>	<b>66</b>
Software Load.....	66
Software Applications.....	67
Software Backup .....	67
Version Control.....	67
Boot Loader.....	67
Startup Folders and Launch Sequences.....	67
Optional Software .....	68
AppLock (Option).....	68
Bluetooth (Option) .....	68

JAVA (Option).....	68
LXE RFTerm (Option).....	68
Wavelink Avalanche Enabler (Option).....	68
<b>Desktop.....</b>	<b>69</b>
My Device Folders.....	70
<b>Start Menu Program Options.....</b>	<b>71</b>
Communication.....	72
ActiveSync.....	72
Connect.....	72
Start / Stop FTP Server.....	72
Summit Client.....	73
Certs.....	73
Wireless Zero Config Utility and the Summit Client.....	73
Command Prompt.....	74
Inbox.....	74
Internet Explorer.....	74
Media Player.....	75
Microsoft WordPad.....	75
Transcriber.....	76
Windows Explorer.....	76
Taskbar.....	76
Advanced Tab.....	77
<b>Settings   Control Panel Options.....</b>	<b>78</b>
About.....	80
About LXE.....	81
Accessibility.....	82
Administration – For AppLock.....	82
Battery.....	83
Bluetooth.....	84
Discover.....	85
Bluetooth Devices.....	86
Bluetooth Device Properties.....	87
Settings.....	88
Turn Off Bluetooth Button.....	88
Options.....	88
About.....	89
Easy Pairing and Auto-Reconnect.....	90
Certificates.....	91
COM1.....	92
Date/Time.....	93
Dialing.....	94
Display.....	95
Background.....	95
Appearance.....	95
Backlight.....	95
Input Panel.....	96
Internet Options.....	97
Keyboard.....	99
Keymaps and Fonts.....	99
Mappable Keys.....	100
Mixer.....	101
Mouse.....	102
Network and Dialup Connections.....	103
Create a Connection Option.....	103
Owner.....	104
Password.....	105

Troubleshooting .....	105
PC Connection .....	106
Power .....	107
Regional Settings .....	108
Remove Programs .....	108
Scanner .....	109
Stylus .....	110
Double Tap .....	110
Calibration .....	110
System .....	111
General Tab .....	111
Memory Tab .....	112
Device Name Tab .....	112
Copyrights Tab .....	112
Volume and Sounds .....	112
<b>SD Flash Cards, CAB Files and Programs .....</b>	<b>113</b>
Access Files on Flash Cards .....	113
<b>ActiveSync / Get Connected Process .....</b>	<b>114</b>
Introduction .....	114
Initial Install .....	115
Install ActiveSync on Desktop/Laptop .....	115
Serial Connection .....	115
USB Connection .....	115
Connect -- Initial Install Process .....	116
Change Connection Parameters .....	116
Backup MX8 Files .....	117
Prerequisites .....	117
MX8 and PC Partnership .....	117
Serial Port Transfer .....	117
USB Transfer .....	117
Radio (RF) Transfer .....	117
Connect .....	118
Explore .....	118
Disconnect .....	118
Serial Connection .....	118
USB Connection .....	118
Radio Connection .....	118
Cold Boot and Loss of Host Re-connection .....	119
ActiveSync Troubleshooting .....	119
<b>Utilities .....</b>	<b>121</b>
LAUNCH.EXE .....	121
ClearHive.EXE .....	124
GrabTime.EXE .....	124
Synchronize with a local time server .....	124
RegEditor.EXE .....	124
RegDump.EXE .....	124
RegLoad.EXE .....	125
<b>Wavelink Avalanche Enabler Configuration .....</b>	<b>125</b>
Briefly .....	125
Enabler Install Process .....	125
Enabler Uninstall Process .....	125
Stop the Enabler Service .....	126
Update Monitoring Overview .....	126
Mobile Device Wireless and Network Settings .....	127
Enabler Configuration .....	128
File Menu Options .....	128

Avalanche Update using File   Settings .....	130
Menu Options .....	130
Connection Tab .....	131
Execution Tab .....	132
Server Contact Tab .....	133
Startup/Shutdown Tab .....	134
Scan Config Tab .....	135
Display Tab .....	135
Shortcuts Tab .....	136
Adapters Tab .....	137
Status Tab .....	139
Troubleshooting .....	140
<b>API Calls .....</b>	<b>140</b>
<b>Clearing Registry Settings .....</b>	<b>140</b>
<b>Reflash the Mobile Device .....</b>	<b>141</b>
Preparation .....	141
Procedure .....	141
Command Line Interface .....	142
<b>CHAPTER 4 SCANNER .....</b>	<b>143</b>
<b>Introduction .....</b>	<b>143</b>
<b>Barcode Processing Overview .....</b>	<b>144</b>
<b>Factory Default Settings .....</b>	<b>145</b>
<b>Main Tab .....</b>	<b>146</b>
<b>COM1 Tab .....</b>	<b>147</b>
<b>Barcode Tab .....</b>	<b>148</b>
Buttons .....	148
Enable Code ID .....	149
Barcode – Symbology Settings .....	150
Strip Leading/Trailing Control .....	152
Barcode Data Match List .....	153
Barcode Data Match Edit Buttons .....	153
Match List Rules .....	154
Add Prefix/Suffix Control .....	155
Barcode – Ctrl Char Mapping .....	156
Translate All .....	157
Barcode – Custom Identifiers .....	158
Control Code Replacement Examples .....	159
Barcode Processing Examples .....	160
Length Based Barcode Stripping .....	161
<b>Vibration Tab .....</b>	<b>163</b>
<b>CHAPTER 5 WIRELESS NETWORK CONFIGURATION .....</b>	<b>165</b>
<b>Introduction .....</b>	<b>165</b>
<b>Summit Client Configuration .....</b>	<b>166</b>
Summit Client Utility .....	166
Help .....	166
Summit Tray Icon .....	167
Main Tab .....	168
Admin Login .....	169
Profile Tab .....	170
Buttons .....	170
Profile Parameters .....	171



Status Tab.....	173
Diags Tab.....	174
Buttons.....	174
Global Tab.....	175
Custom Parameter Option.....	175
Global Parameters.....	175
Summit Wireless Security.....	179
Sign-On vs. Stored Credentials.....	179
Windows Certificate Store vs. Certs Path.....	181
User Certificates.....	181
Root CA Certificates.....	181
No Security.....	182
WEP Keys.....	183
LEAP w/o WPA Authentication.....	184
EAP-FAST Authentication.....	185
PEAP/MSCHAP Authentication.....	186
WPA/LEAP Authentication.....	188
WPA PSK Authentication.....	189
PEAP/GTC Authentication.....	190
EAP-TLS Authentication.....	191
Wireless Zero Config Utility and the Summit Client.....	193
<b>Certificates.....</b>	<b>194</b>
Root Certificates.....	194
Download a Root CA Certificate.....	194
Installing a Root CA Certificate on the Mobile Device.....	196
User Certificates.....	198
Generating a User Certificate for the MX8.....	198
Installing a User Certificate on the MX8 (WPA-TLS Only).....	203

**CHAPTER 6 APPLOCK****207**

<b>Introduction.....</b>	<b>207</b>
<b>Setup a New Device.....</b>	<b>208</b>
<b>Administration Mode.....</b>	<b>210</b>
<b>End User Mode.....</b>	<b>210</b>
<b>Passwords.....</b>	<b>211</b>
AppLock Password Troubleshooting.....	211
<b>End-User Switching Technique.....</b>	<b>212</b>
Using a Stylus Tap.....	212
Using the Switch Key Sequence.....	212
<b>Multi-Application Configuration.....</b>	<b>213</b>
Application Panel.....	213
Launch Button.....	215
Auto At Boot.....	215
Auto Re-Launch.....	216
Manual (Launch).....	216
Allow Close.....	217
End User Internet Explorer (EUIE).....	217
Security Panel.....	218
Setting an Activation Hotkey.....	218
Setting a Password in the Security Panel.....	218
Status Panel.....	219
View.....	219
Log.....	220
Save As.....	220
Troubleshooting AppLock.....	220

<b>Error Messages .....</b>	<b>221</b>
<b>AppLock Registry Settings .....</b>	<b>229</b>
<b>APPENDIX A KEY MAPS .....</b>	<b>231</b>
<b>Introduction .....</b>	<b>231</b>
<b>32-Key Numeric-Alpha Keypad .....</b>	<b>231</b>
<b>Creating Custom Key Maps .....</b>	<b>236</b>
Introduction .....	236
Keymap Source Format .....	237
COLxROWx Format .....	237
GENERAL Section .....	237
SPECIAL Section .....	238
MAP Section .....	238
Keycomp Error Messages .....	239
Sample Input File .....	242
Output File .....	251
<b>APPENDIX B TECHNICAL SPECIFICATIONS .....</b>	<b>253</b>
<b>Physical Specifications .....</b>	<b>253</b>
<b>Display Specifications .....</b>	<b>254</b>
Pinout I/O Port .....	254
<b>Environmental Specifications .....</b>	<b>255</b>
MX8 .....	255
AC Wall Adapter .....	255
<b>Radio Specifications .....</b>	<b>256</b>
Summit Client .....	256
Bluetooth .....	256
<b>List of Valid VK Codes for CE .....</b>	<b>257</b>
<b>ASCII Control Codes .....</b>	<b>258</b>
<b>INDEX .....</b>	<b>261</b>

---

**Illustrations**

Figure 1-1 Front of MX8 .....	5
Figure 1-2 Back.....	6
Figure 1-3 Scanner Aperture.....	7
Figure 1-4 Trigger Handle (Optional).....	7
Figure 1-5 Handstrap (Optional).....	8
Figure 1-6 I/O Port and Cables .....	9
Figure 1-7 5V AC Adapter – Assembled.....	10
Figure 1-8 MX8 Cabling Options .....	10
Figure 1-9 MX8 Desktop.....	11
Figure 1-10 Trigger Handle Attach Points.....	13
Figure 1-11 MX8 Handstrap.....	14
Figure 1-12 Main Battery Pack.....	15
Figure 1-13 USB – MX8 – Power Assembly.....	16
Figure 1-14 AC 5V External Power Supply.....	16
Figure 1-15 Connect Power Cable to the Cradle.....	17
Figure 1-16 Connect the USB / Power Cable to the MX8 Port.....	17
Figure 1-17 Connect the RS-232 / Power Cable to the MX8 Port .....	18
Figure 1-18 Audio Cable and Headset.....	19
Figure 1-19 Power Key Location.....	20
Figure 1-20 Suspend Mode.....	20
Figure 1-21 Speaker Location.....	24
Figure 1-22 Volume & Sounds Properties.....	24
Figure 1-23 Certificate   Stores .....	27
Figure 1-24 View Certificate Details .....	28
Figure 1-25 Bluetooth Devices Display – Before Discovering Devices .....	29
Figure 1-26 Sample Bluetooth Address Barcode Label.....	33
Figure 1-27 About tab and Bluetooth Address.....	34
Figure 1-28 Input Panel / Virtual Keyboard.....	36
Figure 1-29 Scan Beam.....	38
Figure 1-30 Scan Status LED.....	38
Figure 2-1 System Hardware .....	43
Figure 2-2 COM1 Port.....	46
Figure 2-3 Mini SD card Location.....	50
Figure 2-4 Power Modes – On, Suspend and Off.....	51
Figure 3-1 Pocket CMD Prompt Screen .....	74
Figure 3-2 Taskbar General Tab .....	76
Figure 3-3 Advanced Tab .....	77
Figure 3-4 About Panels .....	80
Figure 3-5 About LXE Panels.....	81
Figure 3-6 System – Accessibility .....	82
Figure 3-7 Administration – For AppLock .....	82
Figure 3-8 System – Battery .....	83
Figure 3-9 LXEZ Pairing Control Panel .....	84
Figure 3-10 Control Panel - Bluetooth.....	85
Figure 3-11 Discover Bluetooth Devices.....	85
Figure 3-12 Bluetooth Devices Panel.....	86
Figure 3-13 Bluetooth Device Disconnect / Delete.....	87
Figure 3-14 Bluetooth Device Properties Menu.....	87
Figure 3-15 Bluetooth Device Settings Panel .....	88
Figure 3-16 Bluetooth About Panel .....	89
Figure 3-17 System – Stored Certificates .....	91
Figure 3-18 COM1.....	92
Figure 3-19 Date/Time Properties.....	93

Figure 3-20 Dialing.....	94
Figure 3-21 Display Properties .....	95
Figure 3-22 Input Panel.....	96
Figure 3-23 Internet Options.....	97
Figure 3-24 Keyboard Properties .....	99
Figure 3-25 Mappable Keys.....	100
Figure 3-26 Mixer Settings .....	101
Figure 3-27 Mouse Properties.....	102
Figure 3-28 Network and Dialup Connections.....	103
Figure 3-29 Owner Properties.....	104
Figure 3-30 Password.....	105
Figure 3-31 PC Connection.....	106
Figure 3-32 Power Properties.....	107
Figure 3-33 Regional Settings.....	108
Figure 3-34 Stylus - Double-Tap .....	110
Figure 3-35 Stylus - Calibrate.....	110
Figure 3-36 System Properties .....	111
Figure 3-37 Volume & Sounds .....	112
Figure 3-38 ActiveSync Connection Settings on a Windows PC .....	117
Figure 3-39 Avalanche Enabler Opening Screen .....	128
Figure 3-40 Avalanche Enabler Connection Options.....	131
Figure 3-41 Avalanche Enabler Execution Options (Dimmed) .....	132
Figure 3-42 Avalanche Enabler Server Contact Options .....	133
Figure 3-43 Avalanche Enabler Startup / Shutdown Options .....	134
Figure 3-44 Avalanche Enabler Scan Config Option.....	135
Figure 3-45 Avalanche Enabler Window Display Options.....	135
Figure 3-46 Avalanche Enabler Application Shortcuts.....	136
Figure 3-47 Avalanche Enabler Adapters Options - Network .....	137
Figure 3-48 Avalanche Network Profile Displayed.....	138
Figure 3-49 Manual Settings Properties Panels .....	139
Figure 3-50 Status Display.....	139
Figure 3-51 SD Card Location.....	141
Figure 3-52 MX8 Image Update .....	142
Figure 4-1 Scanner Control Panels.....	145
Figure 4-2 Scanner Control / Main .....	146
Figure 4-3 Scanner Control / COM1.....	147
Figure 4-4 Scanner Control / Barcode tab.....	148
Figure 4-5 Barcode Tab / Symbology Settings .....	150
Figure 4-6 Symbology / Strip Leading / Trailing.....	152
Figure 4-7 Symbology / Barcode Data Match List .....	153
Figure 4-8 Symbology / Prefix and Suffix Control.....	155
Figure 4-9 Barcode Tab / Ctrl Char Mapping .....	156
Figure 4-10 Barcode Tab / Custom Identifiers.....	158
Figure 4-11 Scanner Control / Vibration tab.....	163
Figure 5-1 Summit Client Utility (SCU).....	166
Figure 5-2 SCU – Main Tab.....	168
Figure 5-3 Main Tab – Enter Admin Password .....	169
Figure 5-4 SCU – ProfileTab .....	170
Figure 5-5 SCU – Scan .....	171
Figure 5-6 SCU – Status Tab .....	173
Figure 5-7 SCU – Diags Tab.....	174
Figure 5-8 SCU – Global Tab .....	175
Figure 5-9 Sign-On Screen .....	180
Figure 5-10 Choose Certificate .....	181
Figure 5-11 Configure a Summit Profile with No Security .....	182
Figure 5-12 Summit WEP Keys.....	183

Figure 5-13 Configure a Summit Profile for LEAP w/o WPA .....	184
Figure 5-14 LEAP Credentials Dialog .....	184
Figure 5-15 Configure a Summit Profile for EAP-FAST .....	185
Figure 5-16 Summit EAP-FAST Credentials .....	186
Figure 5-17 Configure a Summit Profile for PEAP/MSCHAP .....	186
Figure 5-18 PEAP/MSCHAP Credentials .....	187
Figure 5-19 Configure a Summit Profile with LEAP for WPA TKIP .....	188
Figure 5-20 LEAP Credentials .....	188
Figure 5-21 Configure a Summit Profile with WPA PSK Encryption .....	189
Figure 5-22 Summit PSK Entry Dialog .....	189
Figure 5-23 Configure a Summit Profile with PEAP/GTC .....	190
Figure 5-24 PEAP/GTC Credentials .....	190
Figure 5-25 Configure a Summit Profile with EAP-TLS .....	191
Figure 5-26 EAP-TLS Credentials Dialog .....	192
Figure 5-27 Logon to Certificate Authority .....	194
Figure 5-28 Certificate Services Welcome Screen .....	194
Figure 5-29 Download CA Certificate Screen .....	195
Figure 5-30 Download CA Certificate Save to Desktop .....	195
Figure 5-31 Certificate Stores .....	196
Figure 5-32 Import Certificate From a File .....	196
Figure 5-33 Browsing to Certificate Location .....	197
Figure 5-34 Logon to Certificate Authority .....	198
Figure 5-35 Certificate Services Welcome Screen .....	198
Figure 5-36 Request a Certificate Type .....	199
Figure 5-37 Advanced Certificate Request Screen .....	199
Figure 5-38 Advanced Certificate Details .....	200
Figure 5-39 Script Warnings .....	201
Figure 5-40 Script Warnings .....	201
Figure 5-41 User Certificate Issued .....	201
Figure 5-42 Download Certificate Security Warning .....	202
Figure 5-43 My Certificates Stores .....	203
Figure 5-44 Import User Certificate .....	203
Figure 5-45 Browsing to Certificate Location .....	204
Figure 5-46 Browsing to Private Key Location .....	205
Figure 6-1 AppLock Panels .....	209
Figure 6-2 Switchpad Menu .....	212
Figure 6-3 Application Panel .....	213
Figure 6-4 Application Launch Options .....	215
Figure 6-5 Security Panel .....	218
Figure 6-6 Status Panel .....	219



# Chapter 1 Introduction

## Overview

The LXE MX8 is a rugged, portable, hand-held Microsoft® Windows® CE 5.0 equipped mobile computer capable of wireless data communications. The mobile device can receive and transmit information using an 802.11 b/g radio. The MX8 can store data for later transmission through an RS-232 or USB port.

The mobile device is vertically oriented and features backlighting for the display. The touch-screen display supports graphic features and Windows icons that the Windows CE 5.0 operating system supports. Keypads are available in 32-key numeric-alpha versions.

This device is a Windows CE 5.0 compatible computer that can be scaled from a limited function batch computer to an integrated RF scanning computer. A trigger handle is available as an accessory.

The stylus attached to the handstrap is used to assist in entering data and configuring the mobile device. Protective film for the touchscreen is available as an accessory.

The MX8 is powered by a 3000 mAh Lithium-Ion main battery pack and an internal Ni-MH backup battery.

### Important

- If the mobile device has AppLock installed, please refer to *Chapter 6 – AppLock* for setup and processing information.
- Wireless configuration and security parameters are described in detail in *Chapter 5 – Wireless Network Configuration*.

## Features

The following features affect user interaction and internal operation of the MX8.

The appropriate wireless client utility for your device configuration has been pre-installed by LXE. The desktop will display a Summit Client Utility icon for 802.11 b/g configuration and security.

	Optional?
Windows® CE 5.0	No
LXE 802.11 b/g Radio	No
Summit® Client Utility	No
Bluetooth®	Yes
520MHz CPU	No
128MB RAM	No
128MB, 512MB or 1GB SD Flash	Yes
SE955 Laser Scanner	Yes
EV-15 Linear Imager	Yes
5380SF 2D Imager	Yes
Voice	Yes
LXE RFTerm®	Yes
JAVA®	Yes
LXE AppLock	Yes
Wavelink® Avalanche® Enabler	Yes

The MX8 has one mini SD card interface for storage for User data. Use only LXE-qualified SD Cards (see *Accessories*).

The MX8 does not have a Bluetooth managed LED. The MX8 does not have InfraRed capability.

The MX8 is not approved for use in Hazardous Locations.



---

## Important Battery Information

*Note: The mobile device's backup battery maintains its charge by drawing power from the main battery pack. Always store unused devices with a fully charged main battery pack installed. LXE recommends an in-use mobile device be frequently connected to an external power source to maintain optimum power levels in the main battery pack and the backup battery. When the backup battery and main battery pack are dead, the mobile device reverts to the last saved setup defaults when a fully charged main battery pack is installed and the device is powered On again.*

Tap  | **Settings** | **Control Panel** | **Battery** tab.

- Until the main battery and backup battery are completely depleted, the MX8 is always drawing power from the batteries (On).
- New batteries must be fully charged prior to use.
- Whenever possible, use the AC power adapter with the MX8 to conserve the main battery and recharge the backup battery. The backup battery receives power from the main battery.
- When the MX8 is connected to AC power and the main battery is being hotswapped, do not disconnect AC power from the MX8 until a main battery is secured in the battery well.
- Ni-MH backup battery replacement must be performed by qualified service personnel.

---

## When to Use This Guide

As the reference for LXE's MX8 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 MX8, and then referring to it when you need more information about a particular subject. This guide takes you through all aspects of installation and configuration for the LXE MX8.

Operation and safety instructions for the general user are contained in the “MX8 User's Guide.”

This chapter, “**Introduction**”, describes this reference guide's structure, contains initial setup 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 MX8 components, controls and connectors. Also describes the external power supplies and vehicle mounting options for the MX8.

**Chapter 3 “System Configuration”** takes you through the CE 5.0 operating system setup and the MX8 file structure. Also describes and explains initial ActiveSync processes, the Wavelink Avalanche Enabler and MX8 specific utilities.

**Chapter 4 “Scanner”** describes the function, layout and setup for the integrated Scanner/Imager.







**Chapter 5 “Wireless Network Configuration”** details 2.4GHz networked client setup. Configuration for WEP and WPA is included.

**Chapter 6 “AppLock”** covers all aspects of the LXE AppLock program.

**Appendix A “Key Maps”** describes the key press sequences for the keypad. Custom Key mapping instruction is included.

**Appendix B “Technical Specifications”** lists MX8 technical specifications.

## Document Conventions


ALL CAPS	All caps are used to represent disk directories, file names, and application names.
Menu   Choice	Rather than use the phrase “choose the Save command from the File menu”, this manual uses the convention “choose File   Save”.
“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.
<b>ATTENTION</b>	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.
<i>Note:</i>	Keyword that indicates immediately relevant information.
<b>CAUTION</b> 	Keyword that indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
<b>WARNING</b> 	Keyword that indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
<b>DANGER</b> 	Keyword that indicates a imminent hazardous situation which, if not avoided, will result in death or serious injury.

## Components

### Front



**Figure 1-1 Front of MX8**

- 1 Imager/Scanner Aperture
- 2 Speaker
- 3 System Status LED
- 4 Scan Button
- 5 Orange Key (Sticky Key)
- 6 Blue Key (Sticky Key)
- 7 Scan Status LED
- 8 Cable Port
- 9 On / Off Button
- 10 Alpha Mode LED
-  Diamond Number Keys

---

**Back**

**Figure 1-2 Back**

- 1 Imager/Scanner Aperture
- 2 Trigger Handle Attach Points  
and  
Handstrap Retainer Bracket Attach Points
- 3 Main Battery
- 4 Battery Fastener
- 5 Cable Ports (I/O Port)

*Note:* The touch screen stylus is tethered to the handstrap or the trigger handle.

## Scanner / Imager Aperture

**CAUTION:** *Never stare directly into the beam aperture. Read “Laser Warnings and Labels” in the MX8 User’s Guide before using the scanner/imager.*



**Figure 1-3 Scanner Aperture**

Identify the type of integrated imager or laser scanner installed in the MX8 by looking at the type of plastic lens covering the Beam aperture.

- The No-Scanner option has an opaque lens protecting the MX8 internal components.
- The SE955 laser barcode scanner has a red lens protecting the laser engine.
- The EV-15 integrated imager has a clear lens protecting the imager engine.
- The 5380SF 2D imager has an opaque lens protecting the imager engine.

## Trigger Handle



**Figure 1-4 Trigger Handle (Optional)**

- |   |               |   |                     |
|---|---------------|---|---------------------|
| 1 | Scan Aperture | 3 | Handle              |
| 2 | Trigger       | 4 | Tether Attach Point |

*Note:* Either the trigger handle is attached to the MX8 or the handstrap is attached, not both. LXE recommends that, in the absence of a trigger handle, the handstrap be used at all times. The stylus is tethered to the handstrap or the trigger handle.

Refer to the Trigger Handle installation instruction later in this chapter.

---

## Handstrap



**Figure 1-5 Handstrap (Optional)**

- 1 Handstrap Retainer Bracket
- 2 Handstrap
- 3 Handstrap Clip

*Note:* Either the trigger handle is attached to the MX8 or the handstrap is attached, not both. LXE recommends that, in the absence of a trigger handle, the handstrap be used at all times. The stylus is tethered to the handstrap or the trigger handle. LXE pre-installs the handstrap when the MX8 is purchased without a trigger handle.

---

## I/O Port and Cables

*Note:* There is no InfraRed port on the MX8. Tethered scanners are not supported on the MX8.



**Figure 1-6 I/O Port and Cables**

The pinout for the I/O port is located in *Appendix B – Technical Specifications*.

Cable: Multipurpose RS-232 and Power  
MX8A055MULTICBLDA9F



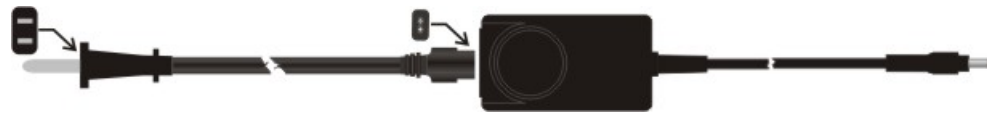
Cable: Multipurpose USB and Power  
MX8A052MULTICBLUSB



Adapter/Cable : Audio  
MX8A060ADPTCBLVOICE



## MX8 AC Adapter

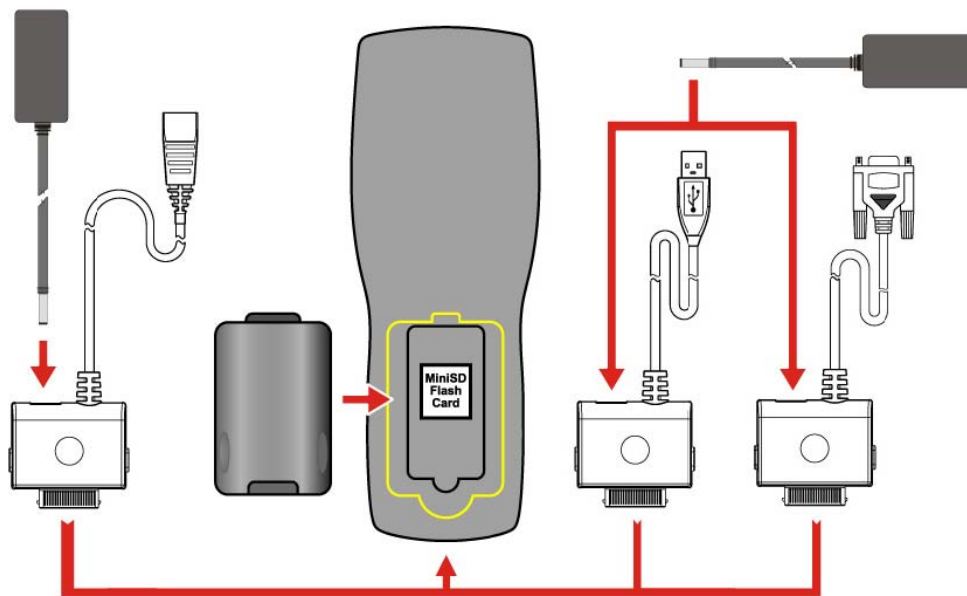


AC Adapter and AC Power Cable



**Figure 1-7 5V AC Adapter – Assembled**

*Note: The MX8 AC Power Adapters (MX8A301CRDLPSAC and MX8A302CRDLPSACWW) are only intended for use with the MX8 multi-purpose cables and the MX8 Desktop Cradle. Do not connect the adapter cables to any other type of device.*



**Figure 1-8 MX8 Cabling Options**

*Note: Tethered scanners connected to the MX8 I/O port are not supported by LXE.*




## Quick Start

*Note: When your mobile device is pre-configured, the client, keypad and scan aperture configurations are assembled by LXE to your specifications. The desktop will display a Summit Client Utility icon.*

This section's instructions are based on the assumption that your new device is pre-configured and requires only accessory installation (e.g. trigger handle) 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.

In general, the sequence of events is:

1. Insert a fully charged battery. (Always put a fully charged battery in the mobile device at the beginning of the shift or workday.)
2. Connect an external power source to the unit (if available).
3. If the screen does not automatically display, tap the Power key.
4. Calibrate the touchscreen.
5. A white screen will appear during the boot process until all CAB files and applications are loaded and installed. Wireless client setup screens may appear and disappear while files are loading.
6. After all files are loaded and the Microsoft Windows CE Desktop is displayed, adjust audio volume and other parameters if desired.
7. Pair Bluetooth devices.
8. Setup wireless client parameters.
9. Setup terminal emulation parameters.
10. Setup mappable keys.
11. Save changed settings to the registry.

If needed, change the Time and Date from it's default value by tapping the  | Settings | Control Panel | Date/Time icon.



**Figure 1-9 MX8 Desktop**

---

## Troubleshooting

Can't calibrate the touchscreen, change the date, time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts User access to running programs. Changes or modifications require Administrator access.  Refer to <i>Chapter 6 – AppLock</i> for setup and processing information.
RFTerm opens and runs upon each cold boot and warm boot.	Tap File   Exit to close the RFTerm application. When installed, RFTerm runs upon each cold boot and warm boot. Suspend/resume does not activate RFTerm, if it was not running when Suspend mode initiated.
The MX8 seems to lockup as soon as it is warm booted.	There may be small delays while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the MX8 startup completes, and Bluetooth relationships establish or re-establish.

---

## Related Manuals for Startup

Integrated Scanner Programming Guide – contains programming barcodes used when setting up integrated scan engines.

- SE955 scanner barcode reading parameters, refer to Chapter 2 in the *Integrated Scanner Programming Guide*.
- Intermec EV-15 linear imager, refer to Chapter 3 in the *Integrated Scanner Programming Guide*.
- 5380SF 2D imager, refer to Chapter 4 in the *Integrated Scanner Programming Guide*.

MX8 User's Guide – contains instruction, explanations and troubleshooting information for the MX8 end-user.

MX8 Cradle Reference Guide – contains user instruction, technical and troubleshooting information for the MX8 desktop cradle.

MX8 Multi-Charger User's Guide – contains user, technical and troubleshooting information for the MX8 battery multi-charger.

---

## Entering the AppLock Activation Key

See Also: Chapter 6 - AppLock.

---

### Hotkey

If the mobile device uses LXE's AppLock to allow the user to switch between two applications, the default Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. *Note that the system administrator may have assigned a different key sequence to use when switching applications.*

---

### Touch

*Note: The touch panel must be enabled.*

Tap the taskbar icon to place the popup menu on screen. Tap one of the application icons in the popup menu. The selected application is brought to the foreground while the other application continues to run in the background. Stylus taps affect the application running in the foreground only.

## Hardware Setup

### Installing Trigger Handle (Optional)

The MX8 can be purchased with a customer-installable pistol grip handle. The handle enables the user of the MX8 to hold the unit while pointing and activating the scanner with the trigger on the handle. Pressing the trigger activates the scanner and functions the same as the Scan key on the keypad. With the handle installed the Scan key on the keypad remains active. The trigger duplicates the operation.

The handle is built of a durable, flexible plastic. The handle will not detach from the MX8 if the unit is dropped. The trigger handle is a mechanical device. Battery or external A/C power is not required for operation of the trigger handle. The trigger handle does not need to be removed when replacing the main battery pack.

Either the trigger handle is attached to the MX8 or the handstrap is attached, but not both.



**Figure 1-10 Trigger Handle Attach Points**

#### Handle Installation

*Equipment Needed:* Torque wrench capable of torquing to  $3\pm 1$  in/lb ( $.34\pm .11$  N/m) .

1. Place the MX8, with the screen facing down, on a flat stable surface.
2. Remove the main battery pack.
3. Slide the locking tab on the underside of the pistol grip into the slot at the back of the battery compartment and press it firmly into place.
4. Ensure that the battery can be inserted into the battery compartment before securing the pistol grip handle into place.
5. Attach the pistol grip handle to the MX8 (as shown above) with the two screws provided.
6. Torque the Pan Head Screws to  $3\pm 1$  in/lb ( $.34\pm .11$  N/m).
7. Test the handle's connection making sure the MX8 is securely connected to the handle.

Periodically check the pistol grip handle for wear and the connection for tightness. If the handle gets worn or damaged, it must be replaced. If the pistol grip connection loosens, it must be tightened before the MX8 is placed in service.

## Installing the Handstrap

*Note:* The handstrap cannot be used/installed when the MX8 has the trigger handle installed at the same time.

An elastic hand strap is available for the MX8. Once installed, the handstrap provides a means for the user to secure the computer to their hand. It is adjustable to fit practically any size hand and is easily moved to allow installation or removal of the battery pack.

*Note:* Loosen the top strap of the handstrap to allow access to the battery well.



**Figure 1-11 MX8 Handstrap**

- 1 Handstrap Retainer Bracket
- 2 Handstrap and tethered stylus
- 3 Handstrap Clip

Tool Required: #1 Phillips Screwdriver (not supplied by LXE)

### Installation

1. Place the MX8, with the screen facing down, on a flat stable surface.
2. Attach the handstrap retainer bracket to the MX8 with the screws provided.
3. Slip the Handstrap Clip into the bracket at the base of the MX8.
4. Making sure the closed loop fastener surfaces on the handstrap are facing up, slide the strap through the pin in the retainer bracket and the clip.
5. Fold each end of the the strap over so that the closed loop fastener surfaces mate evenly.
6. Test the strap's connection making sure the MX8 is securely connected to each end of the strap connectors.

Check the closed loop fastener, retainer bracket and clip connections frequently. If they have loosened, they must be tightened before the MX8 is placed into service again. If the handstrap gets worn or damaged, it must be replaced.

---

## Inserting a Fully Charged Battery

Press the Power key after the battery is inserted into the MX8.

*Note:* On first use the MX8 batteries should be charged with an external power source (i.e. AC Adapter) – 5 hours for the main battery and 7 hours for the backup battery. New main battery packs alone must be charged prior to first use – this process takes up to five hours in an MX8 Multi-Charger.



**Figure 1-12 Main Battery Pack**

The MX8 Battery Compartment is located at the bottom of the back of the computer. The main battery functions as the battery well cover.


Push the locking tab towards the I/O connector until it stays in place. Place the battery in the battery well, making sure the tab at the top of the battery pack fits into the slot at the top end of the battery well. With a hinging motion, slip the battery down into the battery well until the locking tab clicks into place and the battery pack is secured to the MX8.

The backup battery is trickle-charged by the main battery. Whenever possible, use the AC power adapter with the MX8 to conserve the main battery and charge the backup battery.

The Status LED indicates battery condition. It is steady red when the main battery is Low. When the battery has sufficient energy the Status LED is unlit. The Battery control panel displays main and backup battery charging and power status (Start | Settings | Control Panel | 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 MX8 is always ‘on’ even when in the Suspend state and draws power from the batteries at all times. Tap the  | **Settings** | **Control Panel** | **Power** tab to check the battery status and power reading.

The following chart is an approximation. Actual battery capacity varies based on usage, ambient temperature and peripherals drawing power from the MX8:

100% capacity	2800 mAh minimum
80% capacity	2280mAh minimum

Deciding when to put a fully charged main battery pack in the MX8 is difficult to quantify because it is very application specific. 2000 mAh may be the cutoff for one customer who uses the mobile device frequently, while 1500 mAh may be perfectly fine for a customer who occasionally uses the mobile device. You need to determine the point at which battery life becomes unacceptable for your business practices and replace the main battery pack before that point.

## Connecting an External Power Supply (Optional)

The MX8 receives AC/DC power from the AC/DC 5V Power Supply. The MX8 external power connection is part of the RS-232 cable assembly and the USB cable assembly.

### Putting it all together ....



To apply external power to the MX8 follow the steps below in sequence.

1. Plug the 2 prong adapter cable end of the external power module into an AC power source (e.g. wall outlet).
2. Squeeze the sides of the power connector and push the power cable connector into the MX8 I/O port until it clicks. The click means the connector is seated firmly.

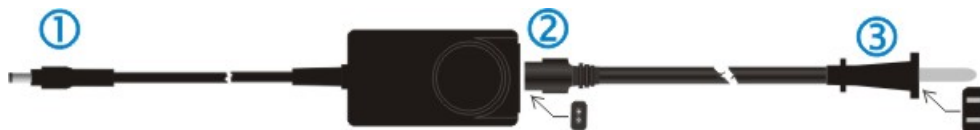
The System LED above the Scan key illuminates when the MX8 is charging the main battery pack using external power through the power cable. The backup battery is always being trickle charged by the main battery pack.

Whenever possible, use the AC power adapter with the MX8 to conserve the main battery power and maintain a charge in the backup battery.

### Assembling the 5V AC Power Adapter

*Note: The MX8 AC Power Adapters (MX8A301CRDLPSAC and MX8A302CRDLPSACWW) are only intended for use with the MX8 multi-purpose cables and the MX8 Desktop Cradle.*

If the 2-prong AC power cable is not included with the Adapter, please contact your LXE representative for assistance.



**Figure 1-14 AC 5V External Power Supply**

1. To cradle -- Firmly press the **cradle end** of the power cable into the female connector on the back of the cradle.
2. From AC Power to Adapter -- Firmly press the **female end** of the power cable into the male connector on the power adapter.

3. To AC wall outlet -- Plug the **2-prong cable** into any AC wall outlet with a dependable power source.

AC power is now being supplied to the AC power adapter and the cradle.



**Figure 1-15 Connect Power Cable to the Cradle**

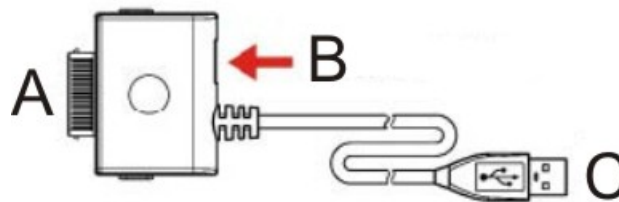
Input : 100-240V, 50-60 Hz, 0.5A

Output : 5V, 3A

Indoor, dry location use only.

---

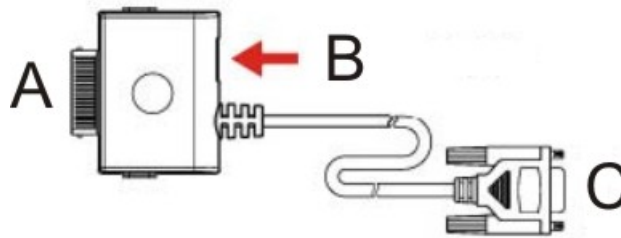
### Connecting the Multipurpose USB / Power Cable



**Figure 1-16 Connect the USB / Power Cable to the MX8 Port**

- Connector A Squeeze the clips on the connector cable to open the catches in the connector assembly. Firmly press Connector A into the connector at the base of the MX8. Release the clips in the connector cable. Test the connection for stability before connecting to USB
- Connector B Firmly push the power cable connector pin into connector B. Plug the 2-prong cable into an AC wall outlet.
- Connector C Insert the USB Type A plug into an appropriate USB port on a desktop/laptop computer for ActiveSync communication.

---

**Connecting the Multipurpose RS-232 / Power Cable**

**Figure 1-17 Connect the RS-232 / Power Cable to the MX8 Port**

- Connector A Squeeze the clips on the connector cable to open the catches in the connector assembly. Firmly press Connector A into the connector at the base of the MX8. Release the clips in the connector cable. Test the connection for stability before connecting the B or C connector.
- Connector B Firmly push the power cable connector pin into connector. Plug the 2-prong cable into an AC wall outlet.
- Connector C Align the RS-232 serial cable end carefully to an appropriate serial port on a desktop/laptop computer for ActiveSync communication. Press the ends together and hand tighten the screws on either side of the serial cable until the MX8 is securely connected to the serial device.

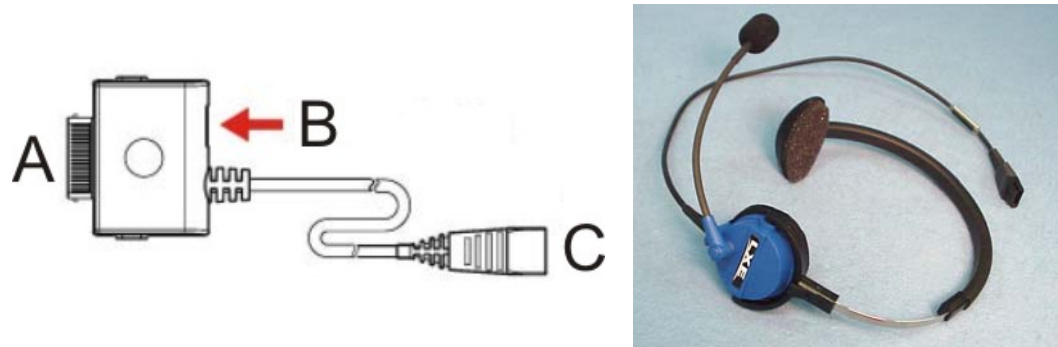


## Connecting the Audio Cable and a Headset

See section titled “Set the Audio Speaker Volume”.

*Note:* The audio option draws power from the main battery.

The headset consists of an earpiece, a microphone and an attached cable. The headset attaches to the audio cable which attaches to the MX8. Use the control panel option “Mixer” to set up mono headphone. The Summit Client supports mono only.



**Figure 1-18 Audio Cable and Headset**

- |             |  |
|-------------|--|
| Connector A | Squeeze the clips on the connector cable to open the catches in the connector assembly. Firmly press Connector A into the connector at the base of the MX8. Release the clips in the connector cable. Test the connection for stability before continuing. |
| Connector B | (Optional) Firmly push the power cable connector pin into the MX8 connector. Plug the 2-prong cable into an AC wall outlet.  |
| Connector C | Align Connector C and the headset quick connect cable end. Firmly push the cable ends together until they click and lock in place.   |

## Adjust Microphone and Secure the Cable

Do not twist the microphone boom when adjusting the microphone.

The microphone should be adjusted to be about two finger widths from your mouth.

Make sure the microphone is pointed at your mouth. Note the small “Talk” label near the mouthpiece. Make sure the Talk label is in front of your mouth.

The microphone cable can be routed over or under clothing.

### Under Clothing

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

### Over Clothing

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

## Power Key

*Note:* Refer to the section titled “Power Modes” later in this guide for information relating to the power states of the MX8.



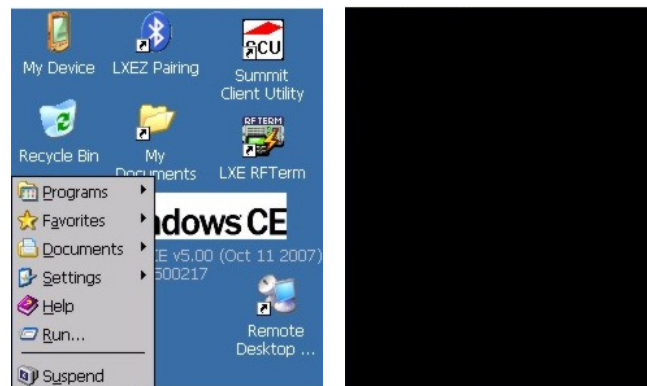
**Figure 1-19 Power Key Location**

The Power key is located at the bottom of the keypad. When a battery is inserted in the MX8 for the first time, press the Power key to turn the device On.

Tapping the Power key places the MX8 immediately in Suspend mode. Tapping the Power key again releases the MX8 from Suspend Mode.

*Or*

Tap  | **Suspend**.



**Figure 1-20 Suspend Mode**

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

See Also: *Reboot Sequence* for reboot options and instruction.

---

## 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, sharp or abrasive 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. Place 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 Scan button or an input/output device connected to the serial port.
- A mouse right-click is performed by holding the stylus down on the touchscreen. A circle of dots appear and then the right-click operation can be performed. See note.

*Note:* A “right mouse click” function must be programmed by the customer to accept a Tap and Hold function. An application can choose to interpret this function as a right mouse click. LXE does not support non-LXE application programming.

---

## Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

- Press <Tab> and an <Arrow> key to select a file.
- Once you’ve selected a file, press <Enter> to open the file or press <Alt> then press <Enter> to open its Properties dialog.
- Press <Del> to delete a file.
- To force the Start menu to display, press <Ctrl> and release, press <Blue> and release, then press <Esc> (the Alt key).

See the section titled *Accessories* for the stylus replacement kit part number.

---

## Software Setup

---

### Touchscreen Calibration

*Note: The first time it is used, the MX8 automatically runs the touchscreen calibration program.*

If the MX8 is not responding properly to stylus touch taps, the touchscreen may need to be recalibrated.

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

Tap the **Recalibrate** button. 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 Time Zone (Optional)

*Note: The first time it is used, or the device returns from a Clear Hive, the MX8 resets the Time Zone to the factory default values (GMT-05:00 Eastern Time).*

To set the Time Zone, tap the  | **Settings** | **Control Panel** | **Date/Time** icon.

Select the physical time zone. Enable the checkbox next to “Automatically adjust clock for daylight saving” if applicable.

If required, adjust the time and calendar date and tap Apply. Tap OK when you are finished or X to ignore any changes.

---

### Enter Owner Information (Optional)

Use the virtual keyboard or keys on the keypad to enter the following data.

To set Owner information, tap the  | **Settings** | **Control Panel** | **Owner** icon.

Select the **Identification** tab, and enter Name, Company, Address, and telephone numbers. Enable the “Display owner identification” checkbox if you want this information displayed each time the system powers on.

Select the **Notes** tab, enter a note to see at power on. Enable the “display owner notes” checkbox to see the note at power on.

Select the **Network ID** tab and enter the User Name, Password and Domain.

Tap OK when finished or X to ignore any changes.

---

### Set the Display Backlight Timer

*Note: Refer to the section titled “Power Modes” later in this manual for information relating to the power states of the MX8.*

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


The first option affects the MX8 when it is running on battery power only. The second option affects the MX8 when it is running on external power (e.g. AC adapter, powered vehicle or desktop cradle).

The default value for the battery power timer is 3 seconds. The default value for the external power timer is 2 minutes and the checkbox is enabled. **The backlight will remain on all the time when both checkboxes are blank.**

---

## Set the MX8 Power Schemes Timers

*Note:* Refer to the section titled “Power Modes” later in this guide for information relating to the power states of the MX8.

Select  | **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 MX8 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 MX8 will be running on external power.

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

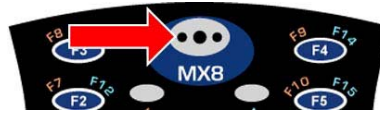
These mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, 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.



**Figure 1-21 Speaker Location**

The speaker is located on the front of the device above the MX8 logo. The audio volume can be adjusted to a comfortable level for the listener. The volume is increased or decreased one step each time the volume key sequence 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

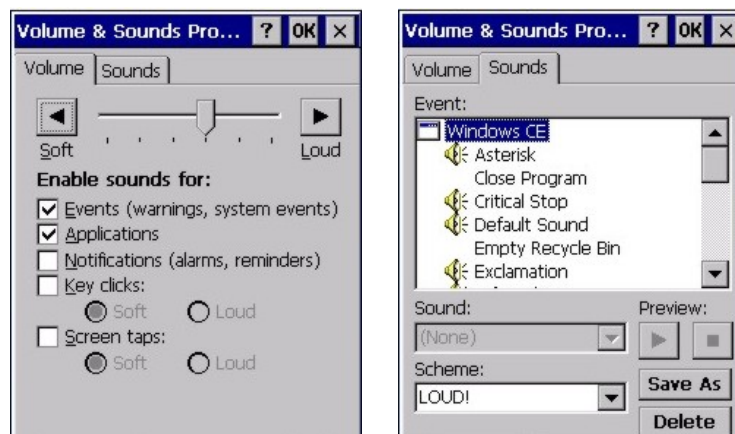
*Note:* *Volume & Sounds (in Control Panel) must be enabled before the following key sequences will adjust the volume.*

To adjust speaker volume:

- Tap the Orange key then the Scan 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.

### Using the Touchscreen

Tap the  | **Settings** | **Control Panel** | **Volume & Sounds** | **Volume** tab.



**Figure 1-22 Volume & Sounds Properties**

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.

---

## Applying the Protective Film to the Display

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

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

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

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

---

## Copy the MX8 LXEbook to the MX8 (Optional)

*Note:* The LXEbook user guides do not contain the illustrations and regulatory information contained in the full user guides on the LXE Manuals CD and on the LXE ServicePass website. See the full format User Guide "MX8 User's Guide" on the LXE Manuals CD.

Mobile Device	Required Adobe Acrobat Reader Version
---------------	---------------------------------------

MX8	Windows CE PDF Viewer (pre-installed).
-----	--

**First**, using your desktop computer download "LXEbook – MX8 Users Guide" from the LXE Manuals CD to your desktop computer.

**Next**, refer to "ActiveSync Processes" and "Initial Install" in Chapter 3 of this guide before connecting the MX8 to your PC.

When the MX8 and the desktop ActiveSync applications are synchronized, tap Explore on the ActiveSync menu on your PC to display the contents of the MX8 folders.

**Then**, open the folder on your desktop computer containing the downloaded LXEbook. Tap and drag the LXEbook to the My Documents folder on the MX8.

When the file copy process is finished, disconnect the MX8 from the synchronization equipment and close ActiveSync.

To view the LXEbook on the MX8, select Start / Programs / Microsoft File Viewers / Microsoft PDF Viewer / File / Open. Locate the LXEbook on the MX8 and "open" the file.

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

## Wireless Client and Network Setup

### Prerequisites

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

*Note:* If the access point uses authentication protocol (LEAP, WEP etc.) your network card must use the same authentication keys. Please contact your IT department for WEP or LEAP encryption keys before contacting LXE. WEP and LEAP are authentication protocols used to encrypt data sent and received from the mobile device to the access point. WEP is disabled by default.

*Note:* The MX8 uses the Summit Client Utility to configure the network card.

When the MX8 boots up for the first time and all programs are loaded, the Wireless Information window may appear. The client is attempting to connect to the local network.


Please refer to Chapter 5 “Wireless Network Configuration” to continue setting up the client and network.

## Terminal Emulation Setup

### Prerequisites

- the mobile client network settings are configured and functional
- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system


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.

1. From the  | Programs, run LXE RFTerm or tap the RFTerm icon on the desktop.
2. 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.
3. 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.
4. 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.
5. Select OK
6. 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 User Certificates and Private Keys

 Date/Time	<p>It is important that all dates are correct on CE and desktop/laptop computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.</p>
--	---

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

Prerequisites:

- The MX8 has the correct Date and Time. See Chapter 3, section titled “Date/Time.”
- A User Certificate file is available
- A Private Key file is available

**First**, using ActiveSync, copy the User Certificate file and the Private Key file to the mobile device’s persistent file location.

A persistent file location does not get erased when the mobile device performs a warm or cold boot. For example, the internal flash folder select **My Device** | **Storage**.

**Next**, place a copy of the User Certificate file and the Private Key file in the My Device\System folder. The certificate and key files should display in the Certificates and Authentication applet windows.

*Note:* After the MX8 is reflashed with a new operating system, the User Certificate and Private Key files must be re-installed and re-authenticated.

### User Certificate

To check if a user certificate is installed navigate to **Start** | **Settings** | **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.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

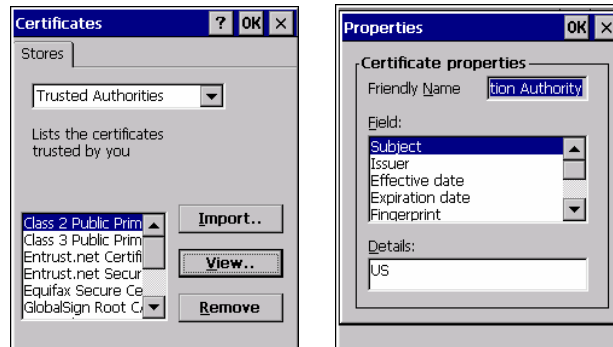
Tap the “?” button and follow the instructions in the Help file when working with trusted authorities and digital certificates.



**Figure 1-23 Certificate | Stores**

## Private Key

Tap the **View . . .** button.



**Figure 1-24 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. See Chapter 5 “Wireless Network Configuration”.

## Bluetooth

**Access:**  | **Settings | Control Panel | Bluetooth**  
or **Bluetooth icon in taskbar** or **Bluetooth icon on Desktop**



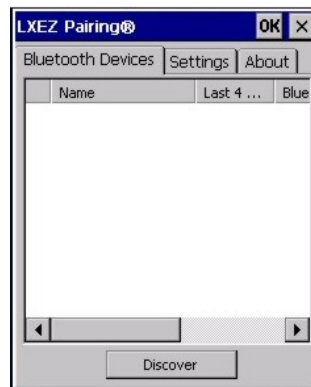
or

Tap the Bluetooth icon in the taskbar or the Desktop to open the Bluetooth LXEZ Pairings application.

The MX8 default Bluetooth setting is Enabled.

The LXE MX8 Bluetooth module is designed to Discover and pair with LXE Bluetooth scanners and LXE Bluetooth printers.

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



**Figure 1-25 Bluetooth Devices Display – Before Discovering Devices**

## Initial Use

1. Select **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon in the taskbar.
2. Tap the **Settings** Tab.
3. Change the **Computer Friendly Name** at the bottom of the Settings display. The Bluetooth MX8 default name is determined by the LXE factory installed software version. LXE strongly urges assigning every MX8 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the MX8 Bluetooth options on the Settings tab.
5. Tap the OK button to save your changes or the X button to discard any changes.

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

## Settings Tab | Bluetooth Options

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

As Bluetooth devices pair with the MX8, the name of the device and an icon representing the type of device is displayed in the Devices window. The icon state changes as the paired Bluetooth devices connect and disconnect from the MX8. When the Bluetooth devices are disconnected, the device icon has a red background.

### **Report when connection lost**

A dialog box appears on the MX8 display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. This option is enabled by default.

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

### **Report when reconnected**

A dialog box appears on the MX8 display notifying the user a connection between one (or all) of the previously-paired Bluetooth devices is complete. This option is disabled by default.

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

### **Report failure to reconnect**

If the reconnect timeout (default is 30 minutes) expires, a dialog box appears on the MX8 display notifying the end-user the connection between one (or all) of the previously-paired Bluetooth devices has failed. This option is enabled by default.

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

### **Computer is connectable**

There is no dialog connected to this checkbox. Enable this checkbox when you want the MX8 to be able to pair with other Bluetooth devices. This option is enabled by default.

### **Computer is discoverable**

There is no dialog connected to this checkbox. Enable this checkbox when you want the MX8 to be Discovered by other Bluetooth devices. This option is disabled by default.

### **Prompt if devices request to pair**

A dialog box appears on the MX8 screen notifying the user a Bluetooth device requests to pair with the MX8. This option is disabled by default.

The requesting Bluetooth device does not need to have been Discovered by the MX8 before the pairing request is received.

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

### **Continuous Search**

This option is disabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with if the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the MX8 stops searching after 30 minutes. This option draws power from the Main Battery.

---

## Subsequent Use

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



1. Tap the Bluetooth icon in the taskbar to open the Bluetooth LXEZ Pairing application.
2. Tap the Settings tab.
3. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Doubletap a Bluetooth device in the Discovered window to open the device properties menu.
6. Tap Pair as Scanner to set up the MX8 to receive scanner data.
7. Tap Pair as Printer to set up the MX8 to send data to the printer.
8. Tap Disconnect to stop pairing with the device. Then tap Delete. The device name and data is removed from the MX8 Bluetooth Devices list after the next Suspend/Resume.
9. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX8 display.
10. Whenever the MX8 returns from Suspend Mode, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the MX8. If the devices cannot connect to the MX8 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

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

## Bluetooth Devices

**Assumption:** The System Administrator has Discovered and Paired targeted Bluetooth devices for each MX8. The System Administrator has also enabled / disabled Bluetooth settings and assigned a Computer Friendly Name for each MX8. See *Chapter 3 System Configuration, Bluetooth control panel applet* and supported Bluetooth printers and scanners.

The Bluetooth taskbar Icon state and Bluetooth LED states change as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the MX8.

Taskbar Icon	Legend
	Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
	MX8 is not connected to any Bluetooth device. MX8 is ready to connect with any Bluetooth device. MX8 is out of range of all paired Bluetooth device(s). Connection is inactive.

*Note:* When an active paired device, not the MX8, enters Suspend Mode, is turned Off or leaves the MX8 Bluetooth scan range, the Bluetooth connection between the paired device and the MX8 is lost. There may be audible or visual signals as paired devices disconnect from the MX8.

See *Accessories* for supported Bluetooth printers and scanners.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the MX8 while AppLock is in control. See *Chapter 6 – AppLock* for more information.

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

---

## Bluetooth Barcode Reader Setup

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

### Introduction

LXE supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the MX8 using Bluetooth functions.

- The MX8 must have the Bluetooth hardware and software installed. An MX8 operating system upgrade may be required. Contact your LXE representative for details.
- If the MX8 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The MX8 batteries are fully charged. Alternatively, the MX8 may be cabled to AC/DC power.
- The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.
- To open the LXEZ Pairing program, tap Start | Settings | Control Panel | Bluetooth or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.



**Figure 1-26 Sample Bluetooth Address Barcode Label**

Locate the barcode label, similar to the one shown above, attached to the mobile device. The label is the Bluetooth address identifier for the MX8.

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

**Important:** The MX8 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

### MX8 with Label

If the MX8 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the MX8, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the MX8 Bluetooth label, the devices are paired. See section titled “Bluetooth Beep and LED Indications”. If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel [Start | Settings | Control Panel | Bluetooth].
4. Tap Discover. Locate the Bluetooth scanner in the Discovery panel.
5. Doubletap the Bluetooth scanner until the right-mouse-click menu appears.
6. Select Pair as Scanner to pair the MX8 with the Bluetooth mobile scanner.

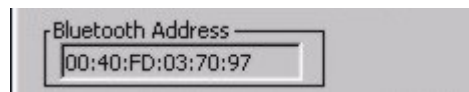
The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled “Bluetooth Beep and LED Indications”.

*Note: After scanning the MX8 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.*

### MX8 without Label

If the MX8 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the MX8:

First, locate the MX8 Bluetooth address by tapping Start | Settings | Control Panel | Bluetooth | About tab.



**Figure 1-27 About tab and Bluetooth Address**

Next, create a Bluetooth address barcode label for the MX8 <sup>1</sup>.

The format for the barcode label is as follows:

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

Create and print the label.

Scan the MX8 Bluetooth address barcode label with the Bluetooth barcode reader.

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

*Note: After scanning the MX8 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.*

<sup>1</sup> Free barcode creation software is available for download on the world wide web. Search using the keywords “barcode create”.



**Bluetooth Beep and LED Indications**

<b>Beep Type from Bluetooth Device</b>	<b>Behavior</b>
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

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

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

## Entering Data

You can enter data into the MX8 through several different methods. The Scanner aperture provides barcode data entry, the I/O port is used to input/output data, and the keypad provides manual entry.

Mobile devices with a touch screen use a stylus to input data, the I/O port and/or the keypad. An input panel (virtual keyboard) is available in applications that expect keyed input.

---

## Using the Keypad

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 MX8 keypads but it may take a few more keystrokes to accomplish a keyed task. Please refer to “Appendix A – Key Maps” for instruction on the specific key presses to access all keypad functions.

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

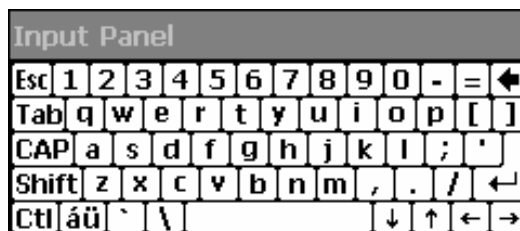
The Orange or Blue keys are pressed when you want to use a “sticky” key function. For example, when you press a Blue or Orange key (the sticky key), then press the key that has the desired second-function key, the second-function key is the “active” key. The specific sticky character is printed above the corresponding key in either Orange or Blue.

---

## Using the Input Panel or Virtual Keyboard

The virtual keyboard is always available when needed e.g. text field input. Tap the keyboard icon at the bottom of the screen to put the virtual keyboard on the display. Using the stylus:

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



**Figure 1-28 Input Panel / Virtual Keyboard**

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

1. Tap the Input Panel/Virtual Keyboard icon in the taskbar.
2. Select “Keyboard” from the menu.
3. Tap the data entry area on the display when you want to enter data using the Input Panel.

---

## Using the Stylus

*Note: This section is directed to the MX8 daily user. The assumption is that the mobile device has been configured and the touch panel calibrated by the System Administrator prior to releasing the MX8 for daily use. The touchscreen should be calibrated before initial use.*

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

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. The 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 the serial port.

- 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 physical keypad, virtual keyboard, or the integrated scanner.

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

## Using the Scanner

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

**Do not look into the laser's lens.**

**Do not stare directly into the laser beam.**

To scan with the integrated laser barcode reader, point the laser aperture towards a barcode and press the Scan button. You will see a red laser beam strike the barcode.



**Figure 1-29 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 MX8 towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.



**Figure 1-30 Scan Status LED**

The Scan Status LED (oval shaped LED below keypad) turns red when the laser beam is on. Following a barcode scan and read the Scan Status LED turns green for two seconds and the MX8 beeps or vibrates, indicating a successful scan. When the scan light is OFF and there is no successful decode then the Scan Status LED turns off and a different beep sequence is heard.

The laser engine and Scan Status LED automatically turn off after a certain time out for unsuccessful decode and will turn off immediately after successful decode. The scanner is ready to scan again after the Scan key (or trigger on the handle if installed) is released.

## Voice Data

Data is entered into the MX8 by speaking into the headset's microphone when prompted. Please contact your System Administrator if assistance is needed with the voice software.

## Tethered Scanners

Tethered scanners connected to the MX8 I/O port are not supported on the MX8 device.

## 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 get help from LXE by calling the telephone numbers listed on the LXE Manuals CD, in the file titled “Contacting LXE”. This information is also available on the LXE website.

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

---

## Manuals

- [MX8 User’s Guide - English](#)
- [MX8 User’s Guide - German](#)
- [MX8 Cradle Reference Guide](#)
- [MX8 Multi-Charger User’s Guide](#)
- [LXEbook – MX8 User’s Guide \(download to mobile device\)](#)
- [RFTerm Reference Guide](#)
- [LXE Security Primer](#)
- [CE API Programmers Guide](#)
- [Integrated Scanner Programmers Guide](#)

---

## Accessories

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

MX8 <b>Main Battery</b> , Lithium Ion	<b>R</b>	MX8A380BATT
MX8 (and MX8 Desktop cradle) <b>power supply</b> , with US power cord	<b>R</b>	MX8A301CRDLPSACUS
MX8 (and MX8 Desktop cradle) <b>power supply</b> , without power cord	<b>R</b>	MX8A302CRDLPSACWW
MX8 Passive vehicle <b>cradle</b> . Does not support charging or communication. U-Bracket included.	<b>R</b>	MX8A003VMCRADLE
MX8 Desktop cradle, requires power supply	<b>R</b>	MX8A002DESKCRADLE
RAM <b>mount kit</b> for MX8 Vehicle Bracket. This kit does NOT include the Cradle. Attaches to U-Bracket.	<b>R</b>	MX8A001RAMBRKT
MX8 4 Unit Main Battery Multi-Charger (US power cord)	<b>R</b>	MX8A385CHGR4US
MX8 4 Unit Main Battery Multi-Charger (no power cord)	<b>R</b>	MX8A386CHGR4WW
<b>Carry case</b> for MX8 with no handle, includes shoulder strap	<b>R</b>	MX8A410CASENOHDL
<b>Carry case</b> for MX8 with handle, includes shoulder strap	<b>R</b>	MX8A411CASEHDL
<b>Holster</b> for MX8 without handle or boot, belt not included	<b>R</b>	MX8A420HOLSTERNHDL
<b>Holster</b> for MX8 with handle, without boot, belt not included	<b>R</b>	MX8A421HOLSTERHDL

<b>Holster</b> for MX8 with handle and boot, belt not included	<b>R</b>	MX8A423HLSTRWHDLBOOT
MX8 Padded <b>handle</b> with rubber overmold and two finger trigger, includes wrist strap	<b>R</b>	MX8A401HANDLE
Replacement MX8 <b>Hand Strap</b>	<b>R</b>	MX8A405HANDSTRAP
Black rubber protective <b>boot</b>	<b>R</b>	MX8A402PROTBOOTBLK
Yellow rubber protective <b>boot</b>	<b>R</b>	MX8A403PROTBOOTYEL
Holster <b>belt</b>	<b>R</b>	9200L67
MX8 Replacement <b>Stylus</b> , fits MX8 carry cases, 10-pack	<b>R</b>	MX8A501STYLUSPACK
<b>CD</b> with CE 5.0 API's and LXE API's with documentation for custom application development	<b>R</b>	MX8A505CE50SDK
Touch screen anti-glare anti-reflective protective <b>film</b> , 10 pack	<b>R</b>	MX8A580PROTFILM
MX8 Charge/Comm Interface <b>Cable</b> , USB Client for ActiveSync with power connector	<b>R</b>	MX8A051MULTICBLUSB
MX8 Charge/Comm Interface <b>Cable</b> , RS-232 Serial ActiveSync, D9 Female with power connector	<b>R</b>	MX8A055MULTICBLDA9F
MX8 RS-232 Serial Adapter <b>cable</b> , 6in, for use with printers that provide their own source of power.	<b>R</b>	MX8A058ADPTCBLPER
MX8 Headset coiled adapter <b>cable</b> , includes quick disconnect headset connector. A headset is still required.	<b>R</b>	MX8A060ADPTCBLVOICE
128MB <b>mini-SD Card</b>	<b>R</b>	MX8A226SD128MB
512MB <b>mini-SD Card</b>	<b>R</b>	MX8A227SD512MB
1GB <b>mini-SD Card</b>	<b>R</b>	MX8A228SD1GB
<b>VoxBrowser™</b> English & Americas		VOXBROWSER ENG
<b>VoxBrowser™</b> Rest-of-the-World		VOXBROWSER ROW
Single ear, single headband, <b>headset</b> with noise canceling microphone, includes 5 replacement windscreens		HX1A501SNGBHEADSET
Single ear, dual headband, <b>headset</b> with noise canceling microphone, includes 5 replacement windscreens		HX1A502DUALBHEADSET
Dual ear, behind the head, <b>headset</b> with noise canceling microphone, includes 5 replacement windscreens		HX1A503BTHHEADSET
Replacement foam <b>block</b> for 502 dual band headsets, qty 1		HX1A504AHSBLOCKFOAM
Replacement head <b>yoke</b> for dual band 502 headset, qty 1		HX1A505DUALYOKE

Replacement head <b>yoke</b> for single band 501 headset, qty 1		HX1A506SINGLEYOKE
Replacement <b>windscreen</b> for all headset microphones, 10 Pack		HX1A508WINDSCREEN10
Replacement <b>windscreen</b> for all headset microphones, 50 Pack		HX1A509WINDSCREEN50
Replacement foam <b>ear piece cover</b> for 501 and 502 headsets, 10 pack		HX1A510FOAMEAR10
Replacement foam <b>ear piece cover</b> for 501 and 502 headsets, 50 pack		HX1A511FOAMEAR50

### Mobile Bluetooth Barcode Readers and Accessories

PowerScan 7000BT Scanner RS-232 with pointer	<b>R</b>	8700A301SCNRBTSRI
PowerScan 7000BT Base Station, RS232, without universal power supply.	<b>R</b>	8700A501BASERS232
PowerScan 7000BT Base Station Power Supply, Std US, 120V	<b>R</b>	8700A502PSACUS
PowerScan 7000BT, RS232 Cable for Base Station, DB9S, Coil, 8'	<b>R</b>	8700A001CBL8DA9F
PowerScan 7000BT Battery Charger with Power Supply, Four Station, US Std	<b>R</b>	8700A503CHGR4US
PowerScan 7000BT Battery Pack	<b>R</b>	8700A504BATT
Bluetooth Standard Range Fuzzy Logic laser	<b>R</b>	8810A326SCNRBTFZ
Bluetooth Auto Range LORAX laser	<b>R</b>	8820A327SCNRBTER
Spare battery	<b>R</b>	8800A376BATTERY
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	<b>R</b>	8800A051POWERCORD
Single Slot Universal Battery Charger adapter cup for 8800 Battery	<b>R</b>	8800A377CHGRADPTRCUP
Single slot battery charger with International power supply	<b>R</b>	8800A378CHGR1SLOT
Universal Battery charger 4-Slot Base. Power Supply included, no AC power cord.	<b>R</b>	8800A379CHGRBASE
LS3408 Scanner Holster for Belt	<b>R</b>	8200A501HOLSTRBELT
Mounted Take Up Reel (Mounted applications)	<b>R</b>	8000A501INDREEL
Auto Sense Intellistand, Hands Free Scanning	<b>R</b>	8500A505STANDSMT
CBL ASSY, DA9F, 9ft (cradle to terminal)	<b>R</b>	8500A051CBL9DA9F
Desk Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	<b>R</b>	8800A001CRADLERCMI

Desk Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	<b>R</b>	8800A002CRADLECFMI
Forklift Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	<b>R</b>	8800A003CRADLEVRCFMI
Forklift Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	<b>R</b>	8800A004CRADLEVCFMI
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	<b>R</b>	8800A051POWERCORD
Universal Desktop Power Supply 90-264VAC, 9VDC, 2A, EPS	<b>R</b>	8800A301ACPS
9-60VDC Forklift Power Supply (For Use with Forklift Cradles)	<b>R</b>	8800A302DCPS
Power Cable: Connects DC Power Supply to Forklift Cradle	<b>R</b>	8800A052DCPWRCABLE
Forklift Rugged Scanner Holder with RAM mount (all metal with cloth padding)	<b>R</b>	8800A005STAND



## Chapter 2 Physical Description and Layout

### Hardware Configuration

#### System Hardware

The MX8 hardware configuration is shown in the following figure.

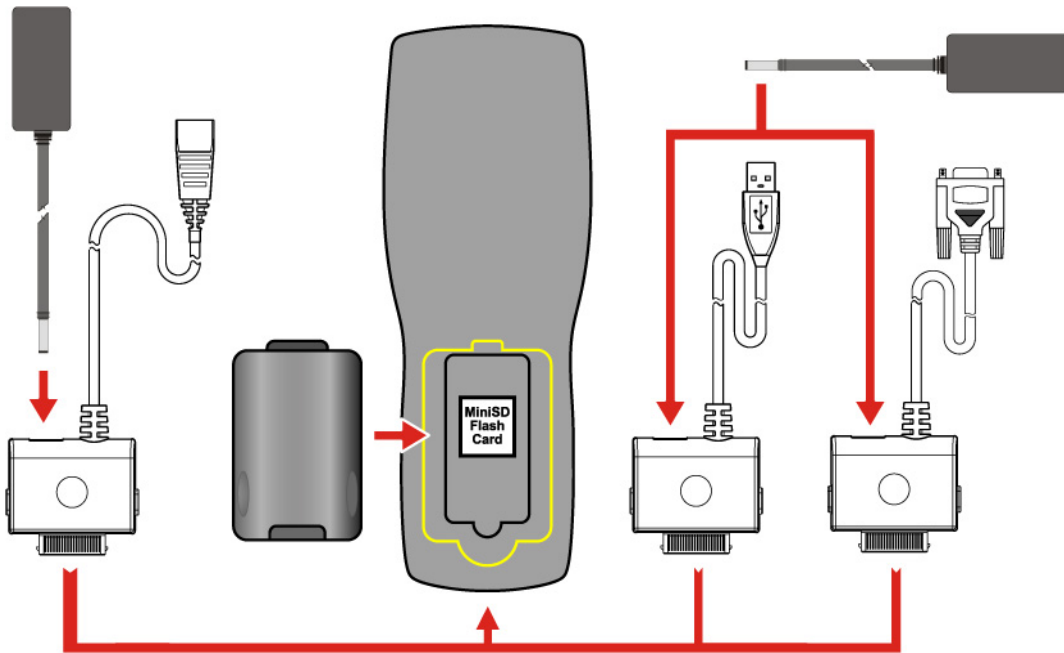


Figure 2-1 System Hardware

#### Central Processing Unit

The LXE MX8 CPU is a 520MHz Intel Xscale PXA27X CPU. The operating system is Microsoft Windows CE 5.0. The OS image is stored on an internal flash memory and is loaded into DRAM for execution.

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

#### Core Logic

The MX8 supports the following I/O components of the core logic:

- One Mini SD card slot under the main battery pack.
- One serial port.
- One Digitizer Input port (Touchscreen).

## System Memory

The 520MHz CPU configuration supports 128 MB Strata Flash ,128MB SDRAM,

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

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID required by CE 5.0 is stored in the boot flash.

---

## Internal Mini SD Memory Card

The MX8 has one mini SD card interface for storage for User data. The Mini SD slot is accessible from the battery compartment and ships with an LXE-qualified 128MB Mini SD card.

The internal Mini SD card supports a FAT16 file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface.


---

## Clear Registry

MX8 has implemented the hive-based registry that can then allow the registry data to persist during a warm boot and cold boot of the OS. Hive based registry can only be removed by the **ClearHive.exe** utility.

---

## Video Subsystem

The touchscreen is a 2.8" (7.1 cm) diagonal viewing area, ¼ VGA 320 by 240 pixel TFT Transmissive Active Color LCD. Backlighting is available and can be turned on and off with key sequences. The turn-off timing is configured through the  | **Settings** | **Control Panel** | **Display** | **Backlight** icon. The display controller supports Microsoft CE 5.0 graphics modes.

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

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

---

## Power Supply

The LXE MX8 uses two batteries for operation.

---

### Main Battery Pack

A replaceable 3000 mAh Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while in the MX8 when the mobile device is connected to the MX8 optional external AC/DC power source. The main battery pack can be removed from the MX8 and inserted in the MX8 Multi-Charger which simultaneously charges up to four battery packs in five hours. The status indicator is illuminated when the backup battery is being charged by the main battery pack. A new main battery pack can be fully charged in 5 hours when it is in an MX8 connected to AC power and 5 hours when it is in the MX8 multi charger.

---

### Backup Battery

An internal 160 mAh Nickel Metal Hydride (Ni-MH) backup battery. The backup battery is recharged directly by the MX8 main battery pack. Recharging maintains the battery near full charge at all times. When the backup battery is fully drained, it may take up to 5 hours to recharge. The capability to discharge the backup battery is provided to allow the user to condition the battery in order to recover full battery capacity. The backup battery must be replaced by qualified service personnel. The battery has a minimum 2 year service life.

*Note: An uninterrupted external power source (wall AC adapters) transfers power to the computer's internal charging circuitry which, in turn, recharges the main battery and backup battery. Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.*

---

## Wireless Client

---

### 802.11b/g

The MX8 supports an LXE 802.11b/g radio. The LXE radio supports diversity with two internal antennas. The CPU board does not allow hot swapping the radio. Adjusting power management on the radio is set to static dynamic control.

WEP, WPA and LEAP are supported.

---

## COM Port

The MX8 has one 20-pin multifunction I/O port that can be configured by the user.

*Note: The MX8 AC Power Adapters (MX8A301CRDLPSAC and MX8A302CRDLPSACWW) are only intended for use with the MX8 multi-purpose cables and the MX8 Desktop Cradle.*



**Figure 2-2 COM1 Port**

The COM1 port pinout diagram is located in Appendix B – Technical Specifications.

---

## RS-232 Serial Port

Configured as COM1. Bi-directional full duplex and supports data rates up to 115 Kb/s. The port does not have RI or CD signals nor does it support 5V switchable power on pin 9 for tethered scanners. The serial port driver supports full duplex communications over the serial port. It supports data exchange via ActiveSync, but does not automatically start ActiveSync when connected.

The “Adapter, RS-232 terminal port to D9 male” accessories can be used with the RS-232 serial port.

External AC power is available when the “Adapter, RS-232 terminal port to D9 male” cable is connected.

---

## USB Client Port

The MX8 has one USB Client port for ActiveSync applications. An accessory USB cable, “Cable, Multipurpose USB and Power” is available to connect the MX8 to a USB Type A plug on a PC for ActiveSync functions.

External AC power is available when the multipurpose USB Client/Power cable is connected.

---

## Audio Headset Connection

An audio headset interface is available using the “Adapter, Audio” accessory with the I/O port. The connection cable connects the MX8 to a Voxware quick disconnect 4-pin interface. This cable adapts to specific styles of headsets for voice input, stereo or mono output. The MX8 with a Summit Client supports mono only. A 3-wire connector with (at a minimum) connections for ground, microphone, and 1 speaker. Connecting the headset to the MX8 COM port turns off audio output to the MX8 speaker on the front of the mobile device. All sounds previously directed to the speaker are redirected to the headphone, including beeps. Bias voltage for an electric condenser microphone is available.

External AC power is available for this option. Power is drawn from the main battery pack.

---

## Audio Support

---

### Speaker

The speaker supplies audible verification signals normally used by the Windows CE operating system. The speaker is located on the front of the MX8, above the MX8 logo. The mobile device emits a Sound Pressure Level (loudness) of at least 102 dB measured as follows:

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

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

---

### Volume Control

Volume control is managed by Windows CE control panel applet, an API and the Orange-Scan-up/down arrow key key sequence. Volume control is covered in greater detail later in this guide.

---

### Voice

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the “Adapter, Audio” accessory cable and the bottom end connector.

---

## Scanner/Imager Port

The MX8 has one integrated barcode scanner port. There is one internal scanner engine and two internal imagers are available. Only one scan engine is installed at a time. Scan engines are not hot swappable. The scan engine options are:

- EV-15 linear imager from Intermec
- SE 955 high performance scanner from Symbol
- 5380SF 2D image undecoded scanner from Hand Held Products.

The internal scanner activates when the scan button on the front of the MX8 is depressed or when the trigger on an installed trigger handle is depressed. A Scanner utility is available to set scan engine power management options.

Functionality of the internal scanner driver is based on the driver version installed in the MX8. Functions may include failed scan, LED indication of a scan in progress, among other functions.

Configuring specific barcode parameters for any of the scan or imager engines is performed by using the MX8 scanner to scan setup barcodes located in the *Integrated Scanner Programming Guide*.

## Power Key

*Note:* Refer to the section titled “Power Modes” for information relating to the power states of the MX8.

The power key is located next to the <Diamond 2> key on the 32-key keypad. When a main battery pack is inserted in the MX8 for the first time, the Power key must be pressed.

## Reboot Sequences

When the Windows CE desktop is displayed or an application begins, the power up (or reboot) sequence is complete. If you have previously saved your settings, they will be restored on warm boot and cold boot. Application panel changes are saved when OK is tapped on an application properties panel.

---

## Suspend / Resume

Quickly tapping the Power key places the MX8 in Suspend mode. Quickly tapping the Power key again, pressing any key, pressing the trigger (on the trigger handle), or tapping the touchscreen, returns the MX8 from Suspend. The System LED blinks green when the video display is Off.

---

## Warm Boot

Temporary data not saved is lost. All previous user control panel settings and changes are saved. Warm boot is also called warm reset.

Hold down the Enter key and then the Power key until the screen blanks. Release the keys and the MX8 warm boots.

or

Tap Start | Run and, using the virtual keyboard or SIP, type WARMBOOT. Tap the OK button and the MX8 warm boots. This command is not case-sensitive.

---

## Cold Boot

Temporary data not saved is lost. All programs are re-launched. Previously saved user settings are restored. Cold boot is also called cold reset.

Hold down the **Blue** key, the **Scan** key and the **Power** key until the screen blanks. Release the keys and the MX8 cold boots.

or


Tap Start | Run and, using the virtual keyboard or SIP, type COLDBOOT. Tap the OK button and the MX8 cold boots. This command is not case-sensitive.

There may be small delays while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the MX8 startup completes, and Bluetooth relationships establish or re-establish.


---

## Reset to Default Settings

***Important:-- Because of the extreme nature of resetting the MX8 to factory default settings, LXE recommends that this process be used only as an emergency procedure and the Warm Boot be used whenever necessary.***

1. Tap  | Run and, using the virtual keyboard or SIP, type CLEARHIVE. Tap the OK button. This command is not case-sensitive.
2. A dialog appears, explaining the restore to default settings process. Select either Yes or Cancel.
3. Selecting Yes causes the reset process to continue and factory default settings are restored when the device powers on again. Selecting Cancel stops the reset process. **All previous user settings, authorizations and configurations, wireless connection settings, Bluetooth relationship settings and Control Panel parameter settings are cleared.**
4. Programs begin installing and messages are shown on the display as each is installed. When the CE Desktop appears or the final application opens, the reset is complete.

Calibrating the touchscreen will need to be performed during the reset process.


If needed, change the MX8 Time and Date from its factory default value by tapping the  | Settings | Control Panel | Date/Time icon.

*Note: Coldboot.exe vs ClearHive.exe – ClearHive.exe utility clears the registry and coldboots the MX8. Coldboot.exe utility clears the registry, resets the persist keys in the Launch.reg file to factory defaults and coldboots.*

## Saving Changes to the Registry

The MX8 saves the registry every time a Suspend / Resume function is initiated. The registry save process takes less than 10 seconds.

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel property (e.g. Date/Time) parameters are changed by the user and the OK button is tapped.

When you tap  | Run | and, using the virtual keypad or SIP, type ClearHive, factory default registry settings are loaded. All user changes and settings are lost. The command is not case-sensitive.

## Mini SD card

*Note:* When removing or inserting a Mini SD card, protect the MX8 internal components from electrostatic discharge.

Make sure the proper software is pre-loaded and wireless client cards are properly configured. The MX8 has one internal Mini SD card port.

The internal Mini SD card supports FAT file system, via a special device driver, and appears to the OS as a Storage Card folder. This allows the contents to be manipulated via the standard Windows CE interface.



**Figure 2-3 Mini SD card Location**

*Note:* As there is no card management software loaded on the MX8, LXE recommends purchasing preformatted Mini SD cards from LXE as the cards have been tested and qualified for use by the MX8 (see “Accessories”). LXE does not support other types of Flash cards at this time. Contact your LXE representative for the latest information about the availability of LXE qualified flash cards for the MX8.

---

## Mini SD card Insertion / Removal

Equipment required: None

- LXE recommends that installation/removal of cards be performed on a clean, well-lit surface.
- Anti-static protection is required when installing/removing cards. (Not supplied by LXE)
- If you anticipate keeping a card out of the MX8 for a long period of time place it in a static-free storage container. Store in an area that is protected from dirt, moisture, and electrostatic contact.

### Installation

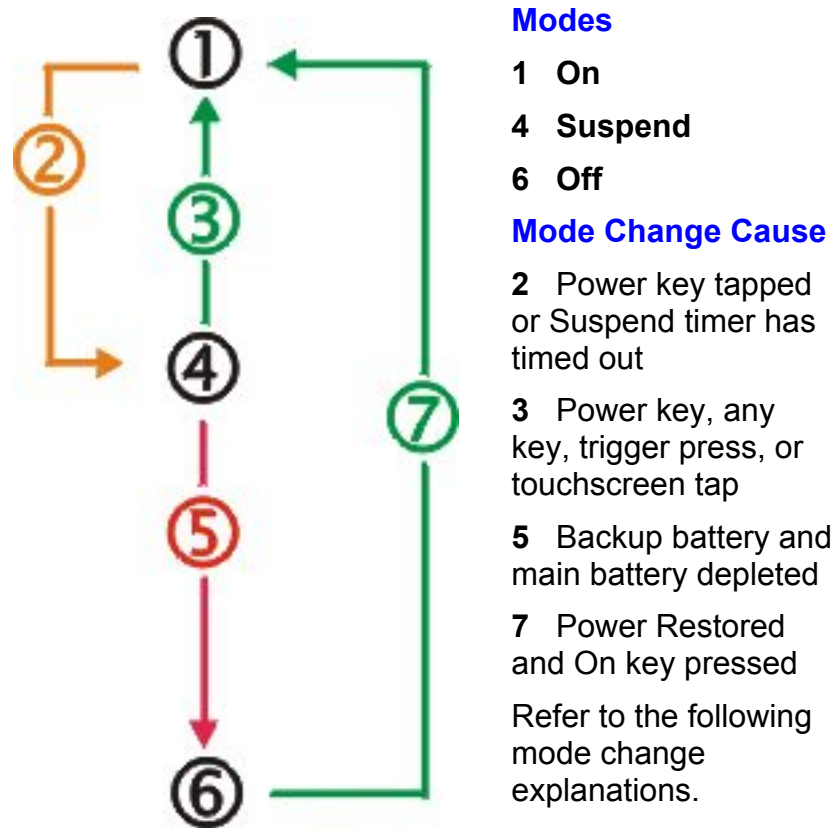
1. Place the MX8 into Suspend Mode. Disconnect the AC adapter from the MX8.
2. Loosen then remove the main battery pack.
3. Lift the rubber barrier and hold it aside. Do not remove it from the battery well.
4. Slide the Mini SD card into the recessed slot, label side uppermost, until it clicks into place.
5. Replace the rubber barrier and the main battery pack and perform a warm boot. Always perform a warm boot when exchanging one Mini SD card for another.

### Removal

1. Place the MX8 into Suspend Mode. Disconnect the AC adapter from the MX8.
2. Loosen then remove the main battery pack.
3. Lift the rubber barrier and hold it aside. Do not remove it from the battery well.
4. Carefully slide the flash card out and away from the recessed slot.



## Power Modes



**Figure 2-4 Power Modes – On, Suspend and Off**

---

### 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, then it dims.

---

#### The MX8

After a new MX8 has been received, a charged main battery inserted, and the Power key tapped, the MX8 is always active 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 and the Power key is pressed.

---

## Suspend Mode

---

### The MX8

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

MX8 Suspend timers are set using  | **Settings** | **Control Panel** | **Power** | **Schemes tab**.

A Power key tap wakes the unit and resets the display backlight timers. Wake up sources can be configured by the administrator, e.g.; any key press, a trigger press, a touchscreen tap, AC adapter insert, USB cable insert, or **Serial cable CTS** will also wake the unit and reset the display backlight timers.

When the unit wakes up, the Display Backlight and the Power Off timers begin the countdown again.

The MX8 should be placed in Suspend mode before hot swapping the main battery.

---

## 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 key to turn the MX8 On.

## Bluetooth LXEZ Pairing

The MX8 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains network connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections from the MX8. However, the MX8 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX8 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

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

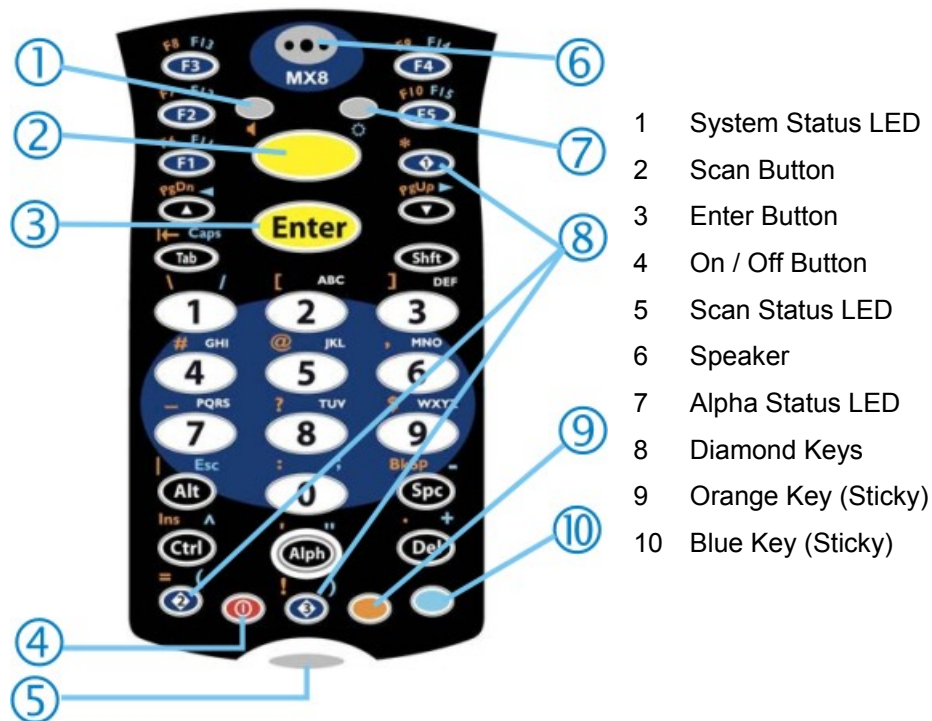
See *Chapter 3 System Configuration*, control panel section titled *Bluetooth*.

### Notes

- The MX8 does not have a Bluetooth managed LED.
- The LED on the Bluetooth scanner illuminates during a scanning operation; the Scan LED on the MX8 does not illuminate.
- Barcode data captured by the Bluetooth scanner is manipulated by the settings in the MX8 Scanner Properties control panel applet.
- Multiple beeps may be heard during a barcode scan using the Bluetooth scanner; beeps from the Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the MX8 during final barcode data manipulation.

## The Keypad

The keypad is installed and configured by LXE to your specifications.



**Figure 2-6 The 32-Key Keypad**

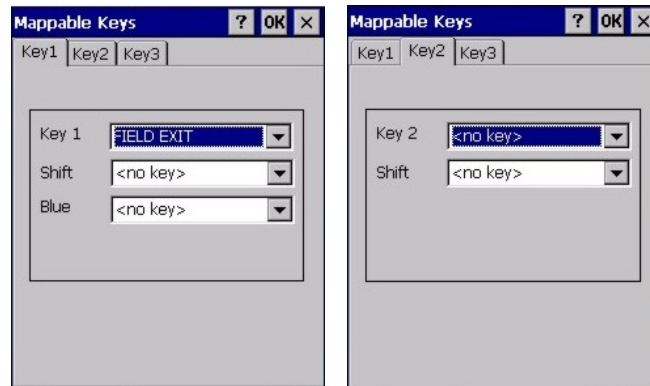
- When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shift sticky key or the Caps key sequence (Blue+Tab) for upper case alphabetic characters.
- Pressing the Alph key forces “Alpha” mode for the 2,3,4,5,6,7,8, and 9 keys. The 1 and 0 keys continue to place a 1 and 0 into the text field.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alph key to toggle between Alpha and Numeric mode.
- When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.

The keymaps (keypress sequences) are located in “Appendix A – Key Maps

## Mappable Diamond Keys

The Diamond keys can be programmed to perform specific functions.

For example, using this Settings applet, you could set the Diamond 1 key to function as an ESC key enabling you to use one keypress instead of two when you want to use the ESC function. Setting the Diamond 1 key to function as an ESC key does not disable the function of the “standard” ESC key sequence (Blue+Alt).



**Figure 2-7 Mappable Diamond Keys**

The Diamond 1 key defaults to Field Exit on the keypad. All other Diamond keys and Diamond Sticky keys have no assigned default value (i.e. their default value is <no key>).

To edit the diamond key parameters, Tap  | **Settings** | **Control Panel** | **Mappable Keys** tab. Change the parameter values using the drop down list and tap OK to save the changes. The change takes effect immediately.

See Also: *Appendix A Key Maps*.

These keys can be mapped by the user to generate any key code defined by Windows CE with the exception of Shift, Alt, Ctrl, Left/Right Shift, Alt, Ctrl.

## LED Indicators

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

### System Status

The System Status LED is located at the top left of the keypad, above the Scan button.

When the LED is . .	The Status is . . .	Action to be taken
Blinking Red	Power Fail	Replace the main battery with a fully charged main battery. Or Connect MX8 to external AC power.
Steady Red	Main Battery Low	Replace the main battery with a fully charged main battery. Or Connect MX8 to external AC power.
Blinking Green	Display Off	No user intervention required.
No Color	Good	No user intervention required.

### Scan Status

The Scan Status LED is located below the MX8 keypad.

When the Scan Status LED is . . .	The Status is . . .
Steady Green	Good Scan
Steady Red	Scan in Progress
Amber	Scanner engine is being accessed by the Scanner Wedge.
No Color	Scanner/Imager ready for use.

### Alpha Mode (Alph Key)

The Alpha Mode LED is located beside the <F5> key.

When the Alph LED is . . .	The Status is . . .
Steady Green	Device is in “Alpha” character input mode.
No Color	Device is in “Numeric” key input mode.

## Standard Keys




See: *Appendix A Key Maps.*


Scan	The integrated scanner scans only when the Scan button is pressed (or when the scan trigger is pressed on the optional trigger handle).
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 mobile device.
Diamond	The Diamond key(s) can be programmed to duplicate a single key press (as defined by Windows CE) with the exception of the Shift, Alt and Ctrl/Ctl keys. Refer to the <i>Mappable Diamond Keys</i> section for instruction.
Numeric	The number keys are used to add numbers to data entry fields.
Alpha	The alpha keys are used to add letters and characters to data entry fields.
Space	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.

## Function Keys

### Sticky Keys

The Sticky Key feature allows the user to activate multi-key press combinations with one finger.

Sticky Key	Function
Ctl / Ctrl (Control key) 	A Control sticky key press stays active until the Control key is pressed again. The Control key enables the control functions of the keypad. This function is similar to a regular keyboard's Control key. Each time you need to use a Control function, you need to press the Ctl / Ctrl key before pressing the desired key.
Alt (Alternate key) 	An Alt sticky key press stays active until the Alt key is pressed again. The Alt key enables the alternate functions of the keypad. This function is similar to a regular keyboard's Alt key. Each time you need to use an alternate function, you need to press the Alt key before pressing the desired key.
Shft (Shift key) 	A Shift key press ends a sticky key function. The Shift 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 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.

Sticky Key	Function
Orange and Blue Keys 	<p>The Orange and Blue keys are sticky keys that, when tapped, activate the second functions of the keypad. Printed above many keys are small characters, in either orange (on the left side of the key) or blue (on the right side of the key), that represent the second function of that key. Using the sticky key activates the second key function. Note that the blue and orange sticky keys only stay active for one keystroke. Each time you need to activate a second function you must press the Orange or Blue key. To cancel a sticky key function before pressing another key, press the same sticky key again.</p>
	<p><b>Orange Key</b></p> <p>Tap the Orange key to enter “orange” mode. Tap it again to cancel “orange” mode.</p> <p>If you were in “blue” mode before you pressed the Orange key, blue mode is cancelled and you enter Orange mode.</p>
	<p><b>Blue Key</b></p> <p>Tap the Blue key to enter “blue” mode. Tap it again to cancel “blue” mode.</p> <p>If you were in “orange” mode before you pressed the Blue key, orange mode is cancelled and you enter Blue mode.</p>

## Mode Key Functions

### 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 CapsLock mode press the Caps key sequence again.

The CapsLock key sequence is Blue key then the <Tab> key.

### Example

**Example:      2 B or Not 2 B**

- |  |   |
|--|---|
| To put the number 2 in a text entry field: | Tap the <2> key once.   |
| To put a lowercase "b" in a text field:    | Tap the <Alph> key, then tap the <2> key twice.   |
| To put an uppercase "B" in a text field:   | Tap the <Alph> key, tap the <Shft> key or the <CapsLock> key, then tap the <2> key twice. |
- To enter a string of letters in a text field, tap the <Alph> key to toggle it On. It remains active until it is tapped again and toggled off.
- To enter a string of numbers in a text field, make sure the <Alph> key is toggled off.



## Touchscreen



**Figure 2-8 Touchscreen**

The touchscreen display is an active color LCD unit capable of supporting VGA graphics modes. Display size is 240 x 320 pixels in portrait orientation. The covering is designed to resist stains. The touchscreen allows signature capture and touch input. A pen stylus is included with the handstrap and the trigger handle. The touchscreen responds to an actuation force (touch) of 4 oz. of pressure (or greater).

The color display is optimized for indoor lighting. The display is black when the device is in suspend mode or when both batteries have expired and the unit is Off.

---

## Display Backlight Timer

When the Backlight timer expires the display backlight is dimmed.

The default value for the battery power timer is 3 seconds. The default value for the external power timer is 2 minutes and the checkbox is enabled.

The backlight timer *dims the backlight* on the touchscreen at the end of the specified time. When the display wakes up, the Backlight timer begins the countdown again.

See the section titled *Set the Display Backlight Timer* in *Chapter 1 – Introduction*.

---

## Cleaning the Display/Scanner Aperture

If there is a static screen protector installed, remove the screen protector before cleaning the display panel.

Keep fingers and rough or sharp objects away from the scan aperture and display. If the scanner aperture or display become 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 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.

Static screen protectors for the MX8 are available from LXE.

## Power Supply

The MX8 computer is designed to work with a Lithium-Ion (Li-Ion) battery from LXE. Under normal conditions a fully charged battery should last approximately eight to ten hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

A suspended MX8 maintains data and time for a minimum of 2 days using a main battery that has a reached the Low Warning point and a fully charged backup battery. The MX8 retains data during a main battery hot swap for at least 5 minutes.

*Note: **New main battery packs must be charged prior to use.** This process takes up to five hours in an MX8 Multi-Charger and five hours when the MX8 is connected to external power.*

---

## Checking Battery Status


Tap the  | **Settings** | **Control Panel** | **Battery** tab. Battery level, power status and charge remaining is displayed.

---

## MX8 Status LED and the Batteries

The Status LED is located next to the <F2> button.

When the LED is . . .	The Status is . . .	Comment
Blinking Red	Power Fail	Replace the main battery with a fully charged main battery. Or Connect the MX8 to external AC power
Steady Red	Main Battery Low	Replace the main battery with a fully charged main battery. Or Connect the MX8 to external AC power
No Color	Good	No user intervention required.

Important: When the backup battery power is Low ( | **Settings** | **Control Panel** | **Power** | **Battery** tab) connect the AC adapter to the MX8 before replacing the main battery pack.

---

## Main Battery Pack


The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the MX8 Multi-Charger or the MX8 unit. The battery pack enclosure functions as the protective cover for the battery well.

When the main battery pack is properly installed in the unit it provides up to eight hours of operation depending upon use 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 a fully charged battery should last approximately eight hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

---

## Battery Hotswapping

Important: When the backup battery power is Low ( | **Settings** | **Control Panel** | **Power** | **Battery** tab) connect the AC adapter to the MX8 *before* replacing the main battery pack.

When the main battery power level is low, the MX8 will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the MX8 using an AC Adapter.

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

When the main battery is removed the device enters Critical Suspend state, the MX8 remains in Suspend mode, the display is turned off and the backup battery continues to power the unit for at least five minutes. Though data is retained, the MX8 cannot be used until a charged main battery pack is installed. After installing the new battery, press the Power key. Full operational recovery from Suspend can take several seconds while the radio (if installed) is reestablishing a wireless client link.

If the backup battery depletes before a fully charged main battery can be inserted, the MX8 will turn Off.

---

## Low Battery Warning

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

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

---

## Backup Battery

The MX8 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 160 mAh Nickel Metal Hydride (Ni-MH) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times comes from the MX8 main battery.

It takes several hours of operation before the backup battery is capable of supporting the operation of the mobile device. The duration of backup battery life is dependent upon operation of the MX8, its features and any operating applications.

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

## 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.

NiMH 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.

---

## Battery Maintenance Publication

The LXE publication “Getting the Most from Your Batteries” is available on the LXE Manuals CD and is a single-source guide to battery management. The publication contains information about battery recharging, conditioning, and other pertinent issues.

## MX8 Multi-Charger (Optional)

Please refer to the *MX8 Multi-Charger User's Guide*.

The multi-charger requires an external power source before battery pack charging can commence. The battery pack begins to recharge as soon as it is placed in the battery well. There are four Charging bays.

The external AC power supply cable connection for the multi-charger is shipped with the multi-charger. The multi-charger AC adapter and cable is only compatible with the MX8 multi-charger.

The main battery pack can be charged in either 1) a powered MX8 Multi-Charger or 2) by a powered AC Adapter connected by multipurpose cables to the mobile device.

Insert the main battery into any charging well in the Multi-Charger. Remove the battery pack by pulling the battery straight up and out.

Do not “slam” or drop the battery into the charging well. Do not allow foreign material to fall or spill into the charging well. Failure to follow these instructions can result in damage to the main battery pack or the Multi-Charger.

---

## Multi-charger LEDs

The status of the charge operation is communicated by the LED located at the base of each charging well.

LED	Indication	Description
Off	No Battery/power	Battery pack not plugged in or no power applied.
Green	Charged	Battery pack fully charged.
Red	Charging	Battery pack charging.
Yellow	Standby	Battery pack temperature out of range.
Flashing Red on any station	Fault	Battery pack fault or failure.

Please refer to the *MX8 Multi-Charger User's Guide* for instruction.

## MX8 Cradles (Optional)

The **MX8 Desktop Cradle** restrains the MX8, re-charges MX8 main batteries, and enables serial or USB communication with a PC, scanner, printer or other peripheral device. MX8 keypad data entries can be mixed with cradle-tethered scanner barcode data entries while the MX8 is in a powered cradle. Bluetooth device connection and use, while the MX8 is docked, are managed by the MX8 Control Panel Bluetooth program, not the cradle.

Using wall AC adapters or DC/DC converters, the desktop cradle can also recharge a spare MX8 battery in approximately 4 hours while the mobile device is docked. The MX8 battery recharging is managed by the power management configuration in the docked MX8. The MX8 can be either On or in Suspend Mode while in the cradles. Special purpose and power cables are available from LXE.

Wireless host/client communications can occur whether the cradle is receiving external power or not as wireless functions draw power from the main battery in the MX8.

The cradles are designed to secure an MX8 with or without a protective boot, a handstrap and/or a trigger handle.



*Note: The MX8 AC Power Adapters (MX8A301CRDLPSAC and MX8A302CRDLPSACWW) are only intended for use with the MX8 multi-purpose cables and the MX8 Desktop Cradle.*

The **MX8 Passive Vehicle Cradle** does not have connectors that can accept an external power source or tethered scanner. It is designed to secure the MX8 in a vehicle.



Please refer to the *MX8 Cradle Reference Guide* for installation, technical specifications and user instruction.

## Chapter 3 System Configuration

### Introduction

There are several different aspects to the setup and configuration of the MX8. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the mobile device. The examples found in this chapter are to be used *as examples only*, because the configuration of your specific MX8 may vary. The following sections provide a general reference for the configuration of the MX8 and some of its optional features.

*Note:* LXE recommends frequently charging the MX8 using an external power source to ensure continuous charging of the backup battery.

### Windows CE 5.0



For general use instruction, please refer to commercially available Windows CE 5.0 user's guides or the Windows CE on-line Help application installed with the MX8.

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

***Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX8 and its Windows CE environment.***

## 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 MX8 you receive the software files required by the separate programs needed for operation and wireless client communication. The files are loaded by LXE and stored in folders in the mobile device.

This section lists the contents of the folders and the general function of the files. Files installed in each MX8 are specific to the intended function of the MX8.

Files installed in LXE mobile devices that are configured for a wireless environment usually contain a radio specific driver – the driver for the radio is specific to the manufacturer of the radio installed in the wireless host environment and are not interchangeable.

---

## Software Load

The software loaded on the MX8 computer consists of Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer for Windows CE browser and MX8-specific utilities. The software supported by the MX8 is summarized below:

### Operating System

**Full Operating System License:** Includes all operating system components, including Windows CE 5.0 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touchscreen input, window management, and common controls.

### Network and Device Drivers

#### Bluetooth (Option)

#### Wavelink Avalanche (Option)

#### LXE AppLock (Option)

#### Java (Option)

#### RFTerm (VT220, TN5250, TN3270) Terminal Emulation (Option).

#### LXE API Routines (See “Accessories” for the LXE SDK Kit part number)

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



---

## Software Applications

The following applications are included:

ActiveSync	Viewer: Excel
Internet Explorer	Viewer: Image
Media Player	Viewer: PDF
Pocket Inbos	Viewer: Word
Scanner Wedge (LXE developed)	WordPad

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

---

## Software Backup

Application programs and data that are normally RAM resident are backed up via ActiveSync.

## Version Control

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

The MX8 has a unique 128-bit ID code as required by the CE 5.0 specification. This ID number is generated by the boot loader. This ID code is available in the control panel, and via a Win32 standard API.

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

See “Accessories” for the LXE MX8 SDK Kit part number.

## Boot Loader

The MX8 supports a proprietary boot loader. It is the responsibility of the boot loader to:

- Initialize all system hardware
- Initiate OS startup
- Handle wakeup from system suspend, loading saved state

The MX8 starts the OS every time during warm boot or cold boot.

---

## Startup Folders and Launch Sequences

The MX8 operating system uses two startup folders:

- User applications placed in the Windows\Startup folder automatically run during a warm boot. They are deleted upon a cold boot.
- User applications placed in the System\Startup folder automatically run during a warm boot and a cold boot. They are lost after a return to factory defaults with CLEARHIVE.EXE.

These applications are launched at different times during startup – applications placed in the Windows\Startup folder run before LAUNCH.EXE executes. Applications stored in System\Startup run after LAUNCH.EXE executes.

## Optional Software

---

### AppLock (Option)

The AppLock program is accessed by the user or the AppLock Administrator at bootup or upon completion of a warm boot. Set parameters using the **Administration option** in the **Control Panel**. See *Chapter 6 AppLock* for instruction.

---

### Bluetooth (Option)

Only installed on a Bluetooth equipped MX8. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX8. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly Name for each MX8. The Bluetooth control panel can be accessed by tapping **Start | Settings | Control Panel | Bluetooth**, or by doubletapping the Bluetooth icon in the taskbar or on the Desktop.

---

### JAVA (Option)

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

---

### LXE RFTerm (Option)

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

---

### Wavelink Avalanche Enabler (Option)

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

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

The MX8 has the Avalanche Enabler installation files loaded, *but not installed*, on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used. After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will, by default, be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. The designation of the mobile device to the Avalanche CE Manager is LXE\_MX8.

See *Wavelink Avalanche Enabler Configuration* at the end of this chapter for instruction. See also *Using Wavelink Avalanche on LXE Windows Computers*.

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


## Desktop



For general use instruction, please refer to commercially available CE user's guides or the CE on-line Help on the MX8.


*Note: Whenever possible, use the AC power adapter with the MX8 to conserve the main battery and to ensure the backup battery is charged.*

The MX8 Desktop appearance is similar to that of a laptop/desktop PC running Windows 2000 or XP. At a minimum, it has the My Device, Internet Explorer, and the Recycle Bin icons that can be tapped with the stylus to access the contents .

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 MX8 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 MX8 into Suspend mode. Tap the Power button to "wake" the unit up.

Desktop Icon	Function
My Device	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
Radio Config Utility	Used when setting radio power management, antenna diversity and roaming profiles. LXE recommends using the defaults set by the manufacturer. WZC icon in toolbar.
Summit Client	Used for configuring Summit client for radio security settings.
Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
My Documents	Storage for downloaded files / applications.
Start 	Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help, run programs or place the unit into Suspend mode.

---

**My Device Folders**

<b>Folder</b>	<b>Description</b>	<b>Preserved upon Cold Reset</b>
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System (Storage)	Internal SD Flash Card	Yes
Storage Card	External Storage card	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

## Start Menu Program Options

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

**Access:**  | **Programs**

<b>Communication</b>	Stores Network communication options
ActiveSync	Begin ActiveSync connection
Connect	Run this command after setting up a connection
Start FTP Server	Begin connection to FTP server
Stop FTP Server	Stop connection with FTP server
<b>Microsoft File Viewers</b>	View downloaded files (see Note)
Excel Viewer	View Excel documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word and RTF files
<b>Command Prompt</b>	The command line interface in a separate window
<b>Inbox</b>	Microsoft Outlook mail inbox
<b>Internet Explorer</b>	Access web pages on the world wide internet
<b>JAVA</b>	Option.
<b>LXE RFTerm</b>	Option. Terminal emulation application. RFTerm automatically runs as soon as a reboot is completed.
<b>Media Player</b>	Music management program
<b>Microsoft WordPad</b>	Opens an ASCII notepad
<b>Radio Config Utility</b>	Radio management program. WZC icon in toolbar
<b>Remote Desktop</b>	Displays MX8 file structure on a remote desktop monitor.
<b>Summit Client</b>	RF client management program. See Chapter 5.
<b>Transcriber</b>	Handwriting recognition program using an integrated dictionary
<b>Wavelink Avalanche</b>	Option. Remote management for networked devices.
<b>Windows Explorer</b>	File management program

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

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

## Communication

**Access:**  | **Programs** | **Communication**


*Note:* Some communication menu options require an external modem connection to the MX8. Modems are not available from LXE nor supported by LXE.

---

## ActiveSync

After a relationship (partnership) has been established with the MX8 and a desktop computer, ActiveSync can synchronize using the radio link, serial port, or USB port on the MX8.

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

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

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

---

## Connect

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

The default connect setup is USB direct connect.

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

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

---

## Start / Stop FTP Server

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

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

---

## Summit Client

**Access:**  | Programs | Summit

Summit automatically installs and runs after every cold and warm boot. **Start | Programs | Summit | scu** -- See *Chapter 5 - Wireless Network Configuration* for Summit Client Utility setup information and instruction.

---

## Certs

**Access:**  | Programs | Summit | Certs

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

This directory is the default directory for digital certificates and protected access credentials (PACs) used in conjunction with Extensible Authentication Protocol (EAP) types.

When you use PEAP or EAP-TLS, you must provision a certificate authority (CA) certificate for the EAP authentication server and distribute that certificate to every client device. On the device, you can store the certificate in the Microsoft certificate store or in the directory with the path specified as the value for Certs Path on the Summit Client Utility (SCU) Global tab. When you don't specify a Certs Path value, SCU uses the path to this directory for the Certs Path value.

When you enter a CA certificate name on a SCU Credentials page, you enter only the filename and extension, not the path. The Certs Path global setting provides the path.

If you import CA certificates into the Microsoft certificate store and want to use them in the SCU, select "Use MS store" on the Credentials page. When using the Microsoft certificate store, SCU ignores the Certs Path global setting and the value specified in the CA Cert filename field on the Credentials window.

User (not CA) certificates for EAP-TLS must be selected from the Microsoft certificate store.

When you use EAP-FAST, you must create a PAC for each client device. When you create a PAC manually, you must store it in the directory identified by the Certs Path global setting.

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

---

## Wireless Zero Config Utility and the Summit Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the Wireless Zero Config application is enabled and the MX8 is not connected to a network. You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network.

***LXE recommends using the Summit Client Utility to manage wireless connectivity.***

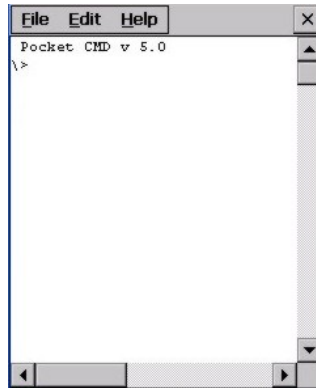
1. To use Wireless Zero Config, first open the Summit Client Utility.
2. Select ThirdPartyConfig in the Active Profile drop down box.
3. A message appears that a Power Cycle is required to make settings activate properly. Tap OK.
4. Tap the Power button to place the MX8 in Suspend, then tap the Power button again to wake the MX8 from Suspend mode.

The Wireless Zero Config utility begins. See *Chapter 5 Wireless Network Configuration* for instruction and complete information.

---

## Command Prompt

**Access:**  | Programs | Command Prompt



**Figure 3-1 Pocket CMD Prompt Screen**

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

---

## Inbox

**Access:**  | Programs | Inbox

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

ActiveSync can be used to transfer messages between the MX8 inbox and a PC’s desktop inbox. Refer to “ActiveSync Processes” in this guide.

---

## Internet Explorer

**Access:**  | Programs | Internet Explorer

The default start page is [www.lxe.com](http://www.lxe.com) and the default search page is [www.google.com](http://www.google.com).

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

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

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

Tap the “?” button to access Internet Explorer Help.



---

## Media Player

**Access:**  | Programs | Media Player

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

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

Tap the “?” button to access Media Player Help.

---

## Microsoft WordPad

**Access:**  | Programs | Microsoft WordPad

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

Tap the “?” button to access WordPad Help.

---

## Transcriber

**Access:**  | Programs | Transcriber

Select Transcriber on the **Start | Programs** menu or tap the icon on the Desktop. 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. When the “hand with a pen” is active, all touchscreen activity is captured/read by the transcriber program.

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

---

## Windows Explorer

**Access:**  | Programs | Windows Explorer

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

---

## Taskbar

**Access:**  | Settings | Taskbar ...

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

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

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



**Figure 3-2 Taskbar General Tab**

## Advanced Tab

### Expand Control Panel

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

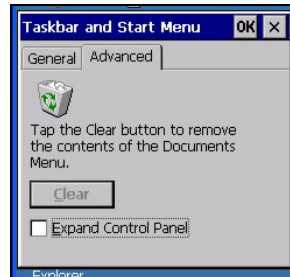
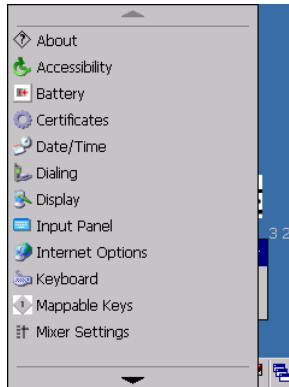
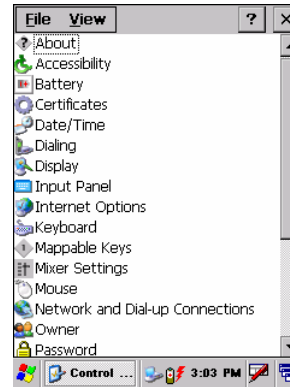


Figure 3-3 Advanced Tab



The Result of “Expand Control Panel”  
checkbox enabled



One Result of “Expand Control Panel”  
checkbox disabled

### Clear Contents of Document Folder

Tap the Clear button to remove the contents of the “Recently Opened” Document folder.

## Settings | Control Panel Options

**Access:**  | [Settings | Control Panel or My Device | Control Panel link](#)

**Getting Help** Please tap the “?” box to get Help when changing Settings options.

Option	Function
About	Software, hardware, and installed versions of hardware and software. No user intervention allowed. Integrated scanner type is identified.
About LXE	Software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse functions.
Administration	LXE AppLock Administration utility. See Chapter 4 for details.
Battery	View voltage and status of the main and backup batteries.
Bluetooth	Discover and manage Bluetooth devices.
Certificates	Manage digital certificates used for secure communication.
COM1	Displays the current settings for the COM1 (I/O) port. See “Scanner”.
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 and scheme. Set backlight properties and timers.
Input Panel	Select the current key / data input method.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
Mappable Keys	Assign multiple key presses to Diamond keys.
Mixer	Adjust the input and output parameters – volume, side tone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password	Set MX8 access password properties for sign on and/or screen saver.

Option	Function
PC Connection	Control the connection between the MX8 and a local desktop or laptop computer.
Power	Set Power scheme properties. Review device status and properties..
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Remove user installed programs in their entirety. <i>Note: Programs listed in this location are deleted upon warm and cold boot processes.</i>
Scanner	Set scanner key wedge, internal scanner port, enable/disable internal scanner sounds, enable/disable illumination LEDs, and set vibration options. Assign baud rate, parity, stop bits and data bits for COM1 port. See also: Chapter 5 – Scanner.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses	Select a server client license from a drop down list. <i>(Not available for LXE support at this release)</i>
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound wav files to CE events.

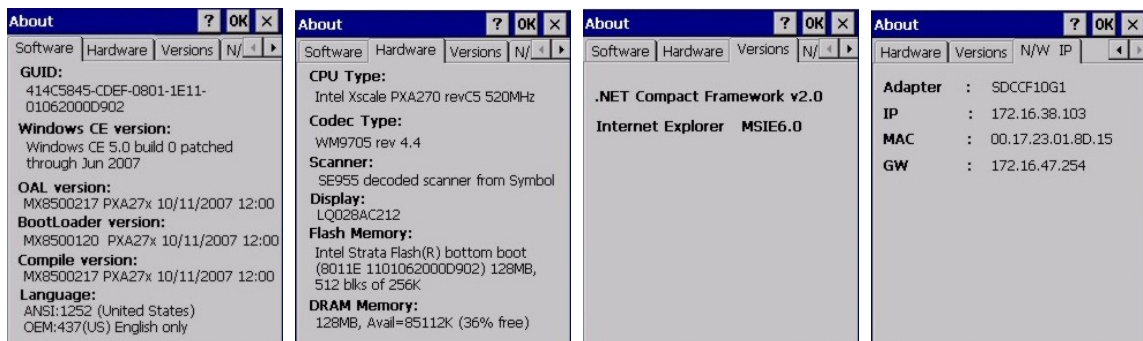
*Note:* Change the font displayed on the screen by choosing  | Settings | Control Panel | Keyboard and then the Key map dropdown list.

## About

**Access:**  | [Settings | Control Panel | About](#)

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, Scanner type, Display, Flash memory, and DRAM memory
Versions	NET Framework Version and Internet Explorer version.
Network IP	Current network connection adapter, IP and MAC address.



**Figure 3-4 About Panels**

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

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

The registry settings for the Version window are under HKEY\_LOCAL\_MACHINE \ Software \ LXE \ Version in the registry.

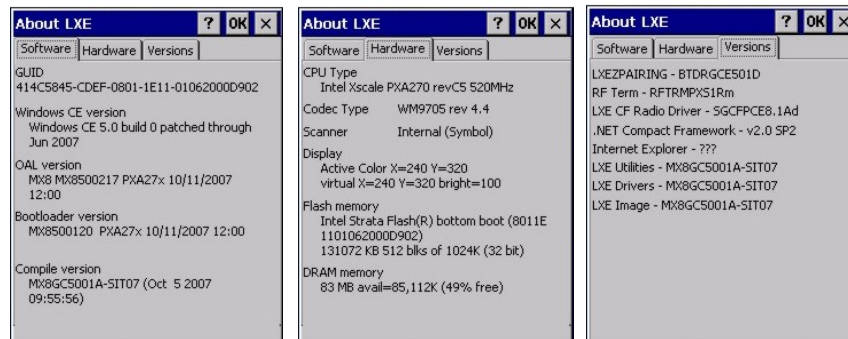
Create a new string value under this key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

## About LXE

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

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, Scanner type, Display, Flash memory, and DRAM memory
Versions	LXE Utilities, LXE Drivers, LXE Image, LXE API, Internet Explorer, and .NET Framework Version.



**Figure 3-5 About LXE Panels**

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

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

The registry settings for the Version window are under HKEY\_LOCAL\_MACHINE \ Software \ LXE \ Version in the registry.

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

## Accessibility

**Access:**  | [Settings](#) | [Control Panel](#) | [Accessibility](#)

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general desktop Accessibility options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.



**Figure 3-6 System – Accessibility**

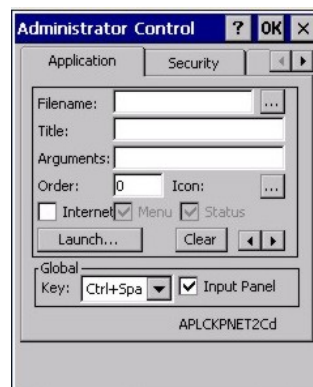
The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

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

## Administration – For AppLock

**Access:**  | [Settings](#) | [Control Panel](#) | [Administration](#)

Use this option to set parameters for mobile devices intended to be used as dedicated, single or multiple application devices. In other words, only the application or feature specified in the AppLock configuration by the Administrator are available to the end-user. See *Chapter 4 AppLock* for information and instruction.



**Figure 3-7 Administration – For AppLock**

LXE devices with the AppLock feature are shipped to start up in Administration mode with no default password, and when the device is started for the first time, the user has full access to the



mobile device and no password prompt is displayed. After the Administrator specifies an application or applications to lock, assigns a password and the device is rebooted (or the hotkey is pressed), the mobile device is then in end-user mode.

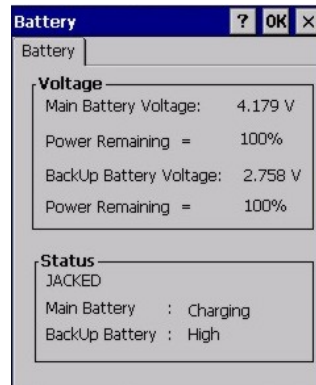
AppLock also contains a component which sets configuration parameters as specified by the Administrator.

---

## Battery

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

View the status of the Main and Backup batteries.



**Figure 3-8 System – Battery**

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

LXE recommends Discharging and Recharging the backup battery twice a year.

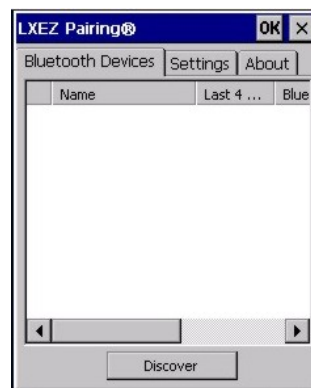
## Bluetooth

**Access:**  | [Settings](#) | [Control Panel](#) | [Bluetooth](#)

Discover and manage pairing with nearby Bluetooth devices.

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

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

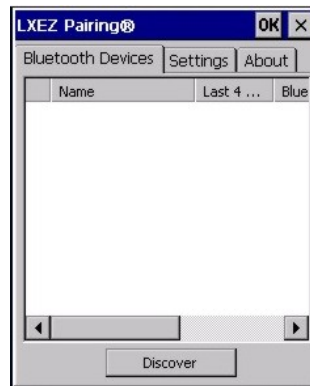


**Figure 3-9 LXEZ Pairing Control Panel**

- The default Bluetooth setting is On.
- The MX8 cannot be discovered by other Bluetooth devices when the *Computer is discoverable* option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- The mobile device can pair with one Bluetooth scanner and one Bluetooth printer.
- Paired scanners and printers do not need to be deleted before a different scanner or printer can be paired with the MX8.
- The Bluetooth device should be as close as possible (line of sight) to the mobile device during the pairing process.

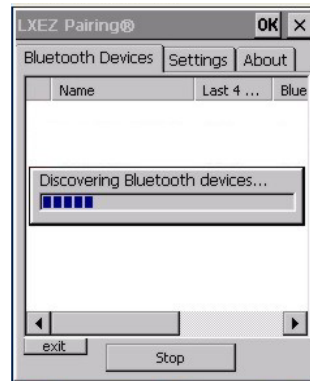
See Also: *Bluetooth* in Chapter 1-Introduction and *Bluetooth LXEZ Pairing* in Chapter 2-Physical Description and Layout.

---

**Discover**

**Figure 3-10 Control Panel - Bluetooth**

Tap the **Discover** button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier for each device discovered.



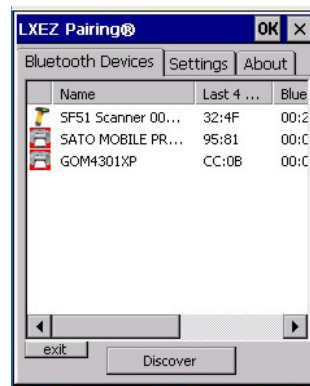
**Figure 3-11 Discover Bluetooth Devices**

Tap **Stop** at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after a Suspend/Resume function.

---

## Bluetooth Devices

A device previously discovered and paired with the MX8 is shown in the Bluetooth Devices panel.



**Figure 3-12 Bluetooth Devices Panel**

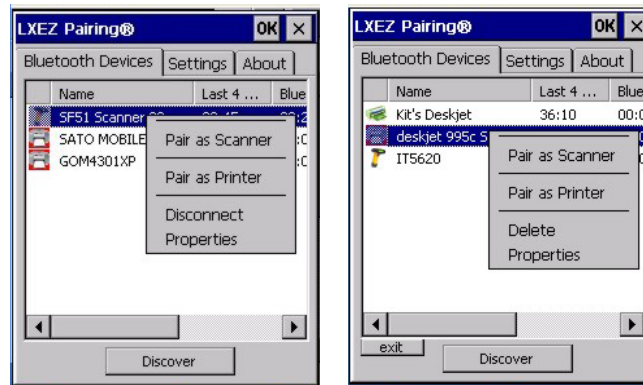
*Note:* When an active paired device, not the MX8, enters Suspend Mode, is turned Off or leaves the MX8 Bluetooth scanning range, the Bluetooth connection between the paired device and the MX8 is lost. There may be audible or visual signals as paired devices disconnect from the MX8.

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

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

An icon with a white background indicates the device is connected to the MX8 and the device Bluetooth connection is active.

Doubletap a device in the list to open the device properties menu. The targeted device does not need to be active.



**Figure 3-13 Bluetooth Device Disconnect / Delete**

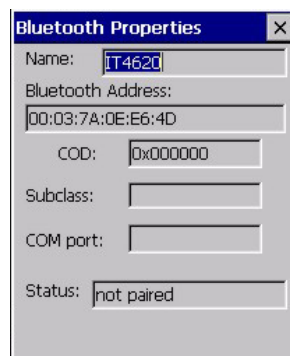
Tap Pair as Scanner to set up the MX8 to receive data from the scanner.

Tap Pair as Printer to set up the MX8 to send data to the printer.

Tap Disconnect to stop the connection between the MX8 and a paired Bluetooth device.

Tap Delete to remove an unpaired device from the Bluetooth device list. Tap OK. The deleted device name and identifier is gone from the MX8 Bluetooth Devices panel when the control panel reopens.

### Bluetooth Device Properties



**Figure 3-14 Bluetooth Device Properties Menu**

Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

## Settings



**Figure 3-15 Bluetooth Device Settings Panel**

### Turn Off Bluetooth Button

Tap the button to toggle Bluetooth hardware On or Off.

### Options

Option	Default	Information
Report when connection lost	Enabled	There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.
Report when reconnected	Disabled	There may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.
Report failure to reconnect	Enabled	The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.  Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.
Computer is connectable	Enabled	Disable this option to inhibit MX8 connection with all Bluetooth devices.
Computer is discoverable	Disabled	Enable this option to ensure other devices can discover the MX8.

Option	Default	Information
Prompt if devices request to pair	Disabled	When enabled, a dialog box is placed on the display. Tap the X button, OK button or No button to close the dialog box.
Continuous Search	Disabled	When enabled, the Bluetooth connection never stops searching for a device it has paired with if the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the MX8 stops searching after 30 minutes. This option draws power from the Main Battery.
Computer Friendly Name	Empty	The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

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

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

## About



**Figure 3-16 Bluetooth About Panel**



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

---

## Easy Pairing and Auto-Reconnect

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

Up to two Bluetooth devices can be connected to the MX8 at a time; LXE supports one scanner and one printer (see *Accessories*).

Taskbar Icon	Legend
	Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
	MX8 is not connected to any Bluetooth device. MX8 is ready to connect with any Bluetooth device. MX8 is out of range of all paired Bluetooth device(s). Connection is inactive.

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

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

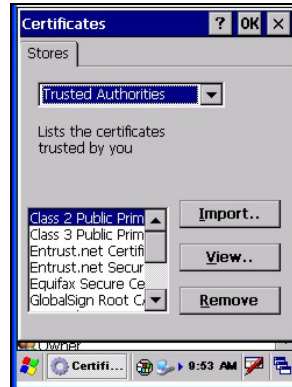
AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the MX8 while AppLock is in control. See *Chapter 6 – AppLock* for more information.



## Certificates

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

Manage digital certificates used for secure communication.



**Figure 3-17 System – Stored Certificates**

Lists the Stored certificates trusted by the MX8 user. These values may change based on the type of radio security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

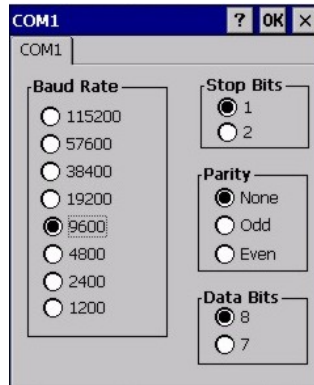
Tap the “?” button and follow the instructions in the Help file when working with trusted authorities and digital certificates.

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

## COM1

Access:  | Settings | Control Panel | COM1

Factory Default Settings	
COM1 (I/O port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8



**Figure 3-18 COM1**

COM1 port default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

If these values are changed, the default values are restored after a cold boot or reflashing.

*Note:* COM1 does not support 5V switchable power on Pin 9 for tethered scanners.

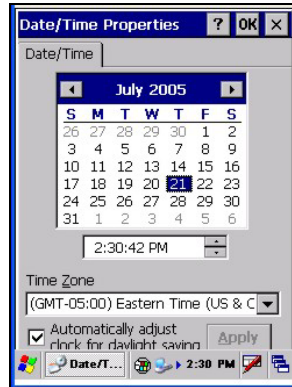
See Also: Chapter 4 - Scanner

## Date/Time

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

If required set Date, Time, Time Zone, and assign a Daylight Savings location.

Factory Default Settings	
Time Zone	GMT-05:00
Daylight Savings	Enabled



**Figure 3-19 Date/Time Properties**

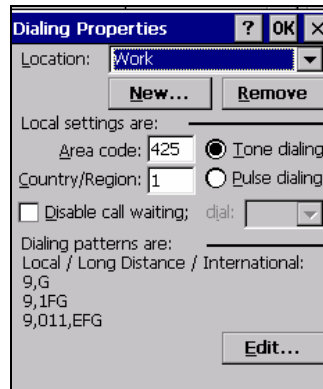
There is very little functional change from general desktop PC Date/Time Properties options. Adjust the settings and tap the OK box or the Apply button to save the changes. The changes take effect immediately. Double-tapping the time displayed in the Taskbar causes the Date/Time Properties screen to appear.

## Dialing

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

Set dialup properties for internal modems (not supplied/supported by LXE).

Factory Default Settings	
Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled



**Figure 3-20 Dialing**

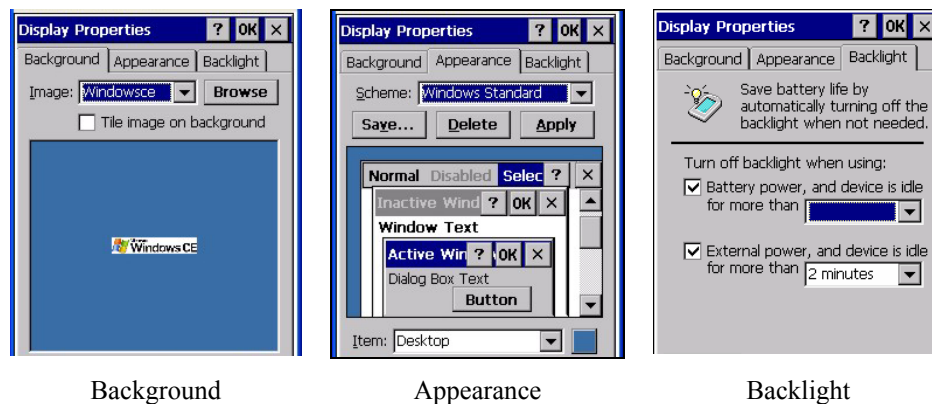
Tap the Edit button to make changes to Dialing properties. Tap the “?” and follow the instructions in Help.

## Display

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

Select the Desktop image and set the display/keypad backlight timers when on battery or external power.

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



**Figure 3-21 Display Properties**

### Background

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

### Appearance

There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the MX8. Tap the OK box to exit, or “X” to escape without making any changes. Saved changes take effect immediately.

### Backlight

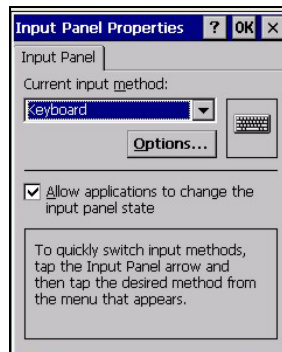
When the backlight timer expires, the screen backlight is dimmed not turned off. Default values are 3 seconds for Battery and 2 minutes for External and both the check boxes are enabled. Adjust the settings and tap the OK box to save the changes or the “X” button to escape without making any changes. Tap the “?” button for Help. The changes take effect immediately.

## Input Panel

**Access:**  | 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	Enabled
Options	
Keys	Small keys
Use gestures	Disabled



**Figure 3-22 Input Panel**

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

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

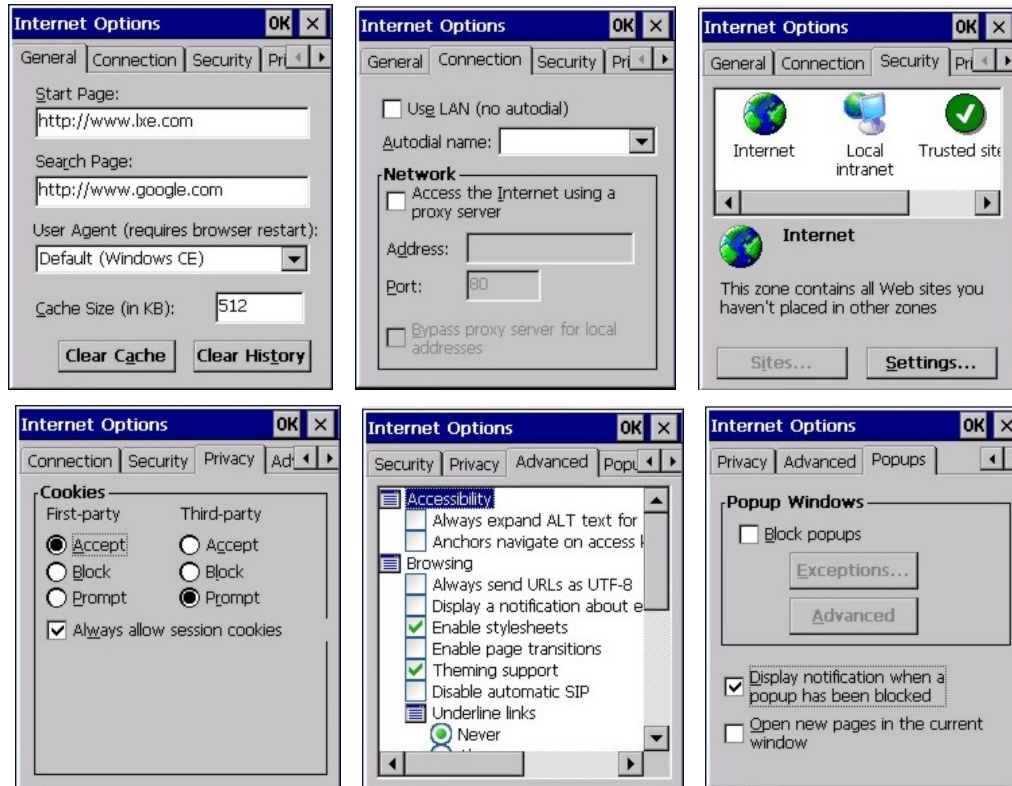
Tap the “OK” button to save any changes and exit, or tap the “X” button to exit without saving any changes. Tap the “?” button for Help.

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

## Internet Options

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

Set options for internet connectivity.



**Figure 3-23 Internet Options**

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

Factory Default Settings	
<b>General</b>	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
<b>Connection</b>	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Bypass Proxy	Disabled
<b>Security</b>	
Allow cookies	Enabled
Allow TLS 1.0 security	Enabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled

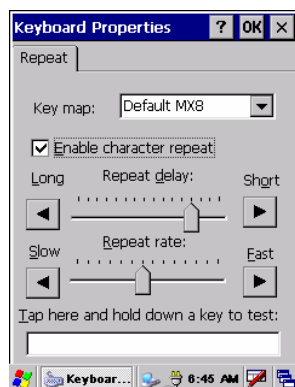
<b>Factory Default Settings</b>	
<b>Privacy</b>	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
<b>Advanced</b>	
Stylesheets	Enable
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
<b>Popups</b>	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled



## Keyboard

**Access:**  | [Settings | Control Panel | Keyboard Icon](#)

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



Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key map	Default MX8

**Figure 3-24 Keyboard Properties**

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

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

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

## Keymaps and Fonts

Please contact your LXE representative about the availability of these fonts for your MX8:

Descriptive name	Font filename	Notes
Simplified Chinese	simsun.ttc	These Asian fonts are ordered separately and built-in to the MX8 OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the default (extended) fonts. See <a href="#">About   Software   Language</a> for the name of any installed fonts.
Traditional Chinese	mingliu.ttc	
Japanese	msgothic.ttc	
Korean	gulim.ttc	

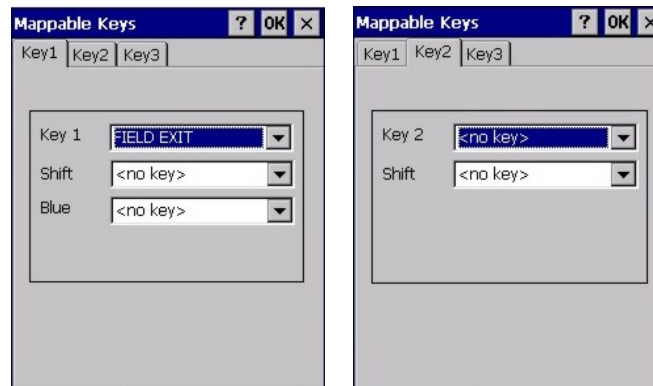
When an Asian font is copied into the fonts folder on the card/System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in Regional Control Panel, the font does not work for naming desktop icons with Asian names, the font does not work for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

## Mappable Keys

**Access:**  | Settings | Control Panel | Mappable Keys Icon

Use this option to assign key sequences to Diamond keys.

Factory Default Settings		
32 Key Keypad		
<b>Diamond 1</b>		
No sticky key	Field Exit	
Shift+Diamond 1	No key	
Blue+Diamond 1	No key	
<b>Diamond 2</b>		
No sticky key	No key	
Shift+Diamond 2	No key	
<b>Diamond 3</b>		
No sticky key	No key	
Shift+Diamond 3	No key	



Diamond 1

Diamond 2 / Diamond 3  
options are the same

**Figure 3-25 Mappable Keys**

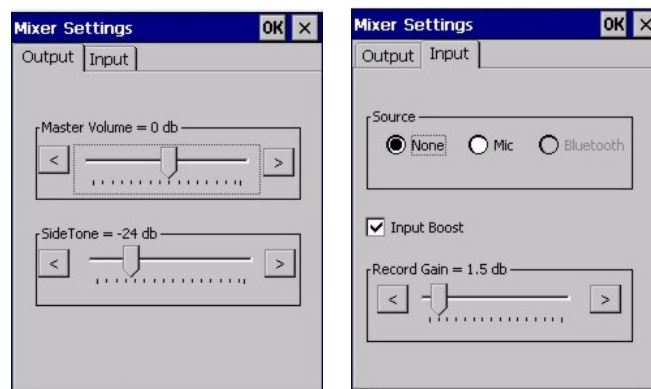
Assign key sequence settings by selecting keys from the drop down boxes. Tap the OK box to save the changes. Tap the “X” box to ignore changes. Tap the “?” box for Help. The changes take effect immediately.

## Mixer

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

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

Factory Default Settings	
<b>Output</b>	
Master Volume	-6dB
Sidetone	12dB
<b>Input</b>	
Input	None
Input Boost	Disabled
Record Gain	22.5dB



**Figure 3-26 Mixer Settings**

Tap and hold the **Output** sliders, move them left and right to adjust the decibel level or tap the left and right arrows to adjust the sliders.

**Input Boost** - When checked (enabled) increases the sensitivity of the microphone by 20 dB.

### How To . . .

Enable Microphone      Enable the **Mic** radio button and the **Input Boost** checkbox.

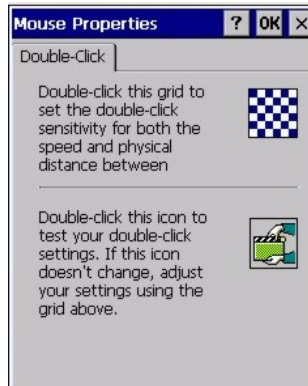
Disable Microphone      Enable the **None** radio button.

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

---

## Mouse

Access:  | Settings | Control Panel | Mouse



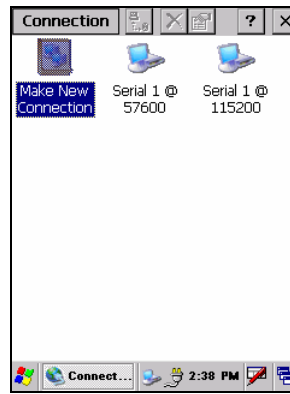
**Figure 3-27 Mouse Properties**

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

## Network and Dialup Connections

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



Set network driver properties and network access properties. Select a connection to use, or create a new connection on the MX8.



**Figure 3-28 Network and Dialup Connections**

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

### Create a Connection Option

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

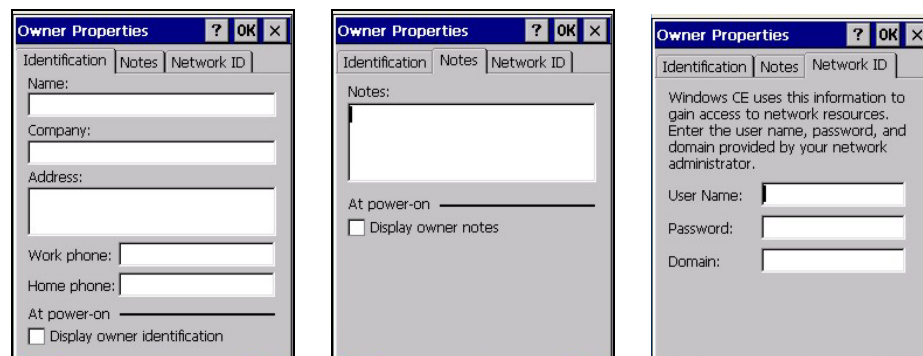
You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

## Owner

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

Set the mobile device owner details.

Factory Default Settings	
<b>Identification</b>	
Name, Company, Address, Telephones	Blank
Display at power-on	Disabled
<b>Notes</b>	
Notes	Blank
Display at power-on	Disabled
<b>Network ID</b>	
User Name	Blank
Password	Blank
Domain	Blank



**Figure 3-29 Owner Properties**

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

The changes take effect immediately.

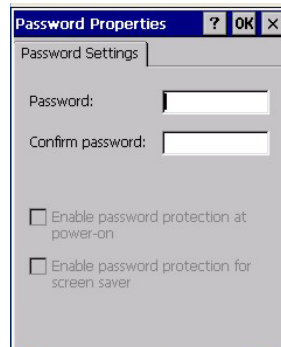
## Password

**Access:**  | [Settings](#) | [Control Panel](#) | [Password Icon](#)

Set MX8 user access/power up password properties. Password and password settings are saved during a warm boot and a cold boot. The screensaver password affects the Remote Desktop screensaver only.

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

*Note:* Once a password is assigned, each Settings option requires the password be entered before each Settings option can be accessed.



**Figure 3-30 Password**

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

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

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

## Troubleshooting

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

## PC Connection

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

Control the connection between the MX8 and a nearby desktop/laptop computer.

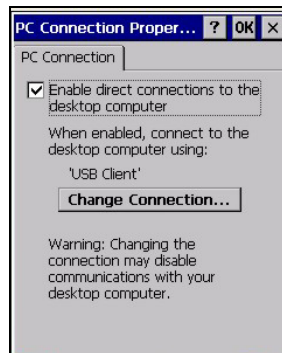
Factory Default Settings	
Enable direct connection	Enabled
Connect Using	'USB Client'

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

Unchecking the “Enable direct connections .....” disables ActiveSync.

### Change Connection ....

Selecting Change Connection displays a list of configured ActiveSync connections.



**Figure 3-31 PC Connection**

Please refer to the “Backup MX8 Files” section later in this chapter for parameter setting recommendations.



## Power

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

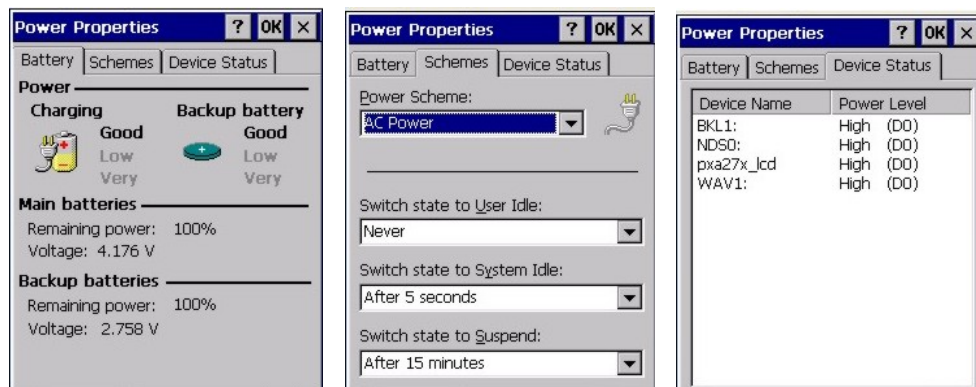
Please refer to Chapter 2 “Physical Description and Layout” section titled “Power Modes”.

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

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

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

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



**Figure 3-32 Power Properties**

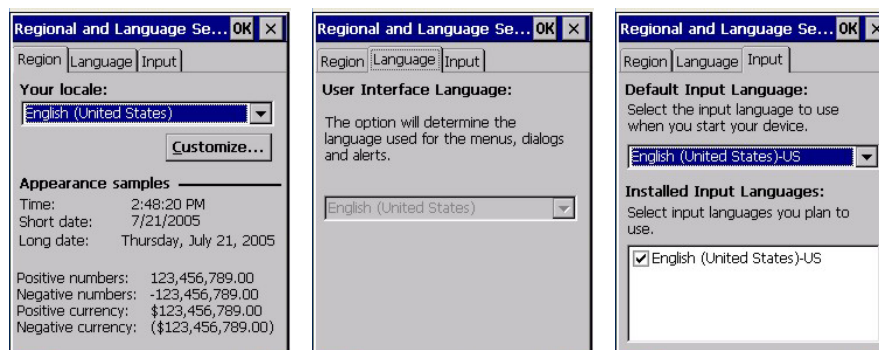
Adjust the settings and tap the OK box to save the changes. Changes are saved across tabs. Tap the “X” box to discard any changes. Tap the “?” for Help. The changes take effect immediately.

## Regional Settings

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

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

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



**Figure 3-33 Regional Settings**

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

## Remove Programs

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

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

Select a program and tap Remove. Follow the prompts on the screen to uninstall **user-installed only** programs. The change takes effect immediately.

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

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

---

## Scanner

**Access:**  | [Settings](#) | [Control Panel](#) | [Scanner](#)

Set 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. Scanner parameters apply to the MX8 integrated scanner/imager *only*. Barcode manipulation parameters apply to barcodes scanned by the integrated scanner/imager engine *only*.

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

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



***Integrated Scanner Programming Guide* and the factory defaults barcodes. After scanning the scanner-engine-specific barcode to reset all scanner parameters to factory default settings (i.e. Reset All, Set Factory Defaults, Default Settings, etc.), the next step is to open the Control Panel Scanner Properties panel. Tap the OK button and close the Scanner panel. This action will synchronize all scanner formats.**

---

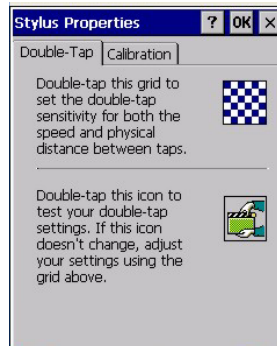
## Stylus

**Access:**  | [Settings](#) | [Control Panel](#) | [Stylus](#)

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

---

### Double Tap

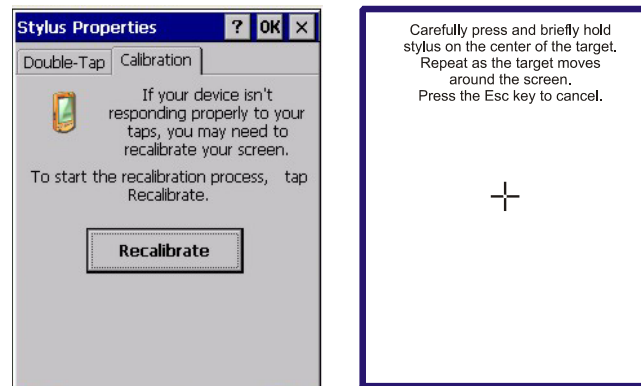


**Figure 3-34 Stylus - Double-Tap**

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

---

### Calibration



**Figure 3-35 Stylus - Calibrate**

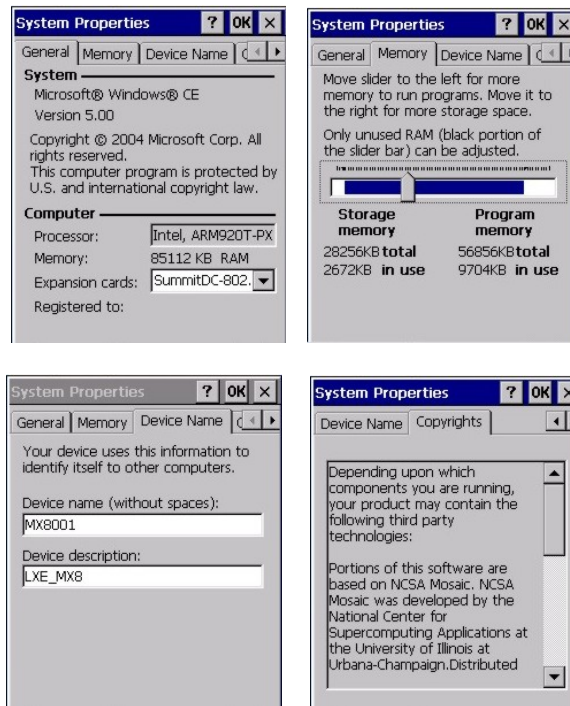
Press and hold the stylus on the center of the target as it moves around the screen. Press Enter to keep the new calibration settings or Esc to cancel.

## System

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

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

Factory Default Settings	
General	N/A
Memory	1/3 storage, 2/3 program memory
Device Name	MX8001
Device Description	LXE_MX8



**Figure 3-36 System Properties**

### 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. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

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

---

## Memory Tab

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 MX8 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 Tab

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 Tab

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

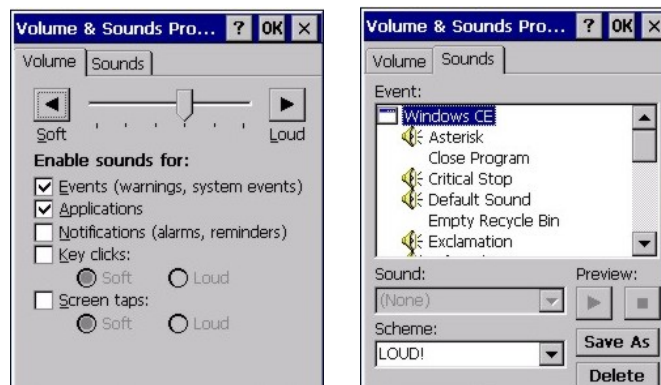
---

## Volume and Sounds

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

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

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



**Figure 3-37 Volume & Sounds**

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

## SD Flash Cards, CAB Files and Programs

### Access Files on Flash Cards

The SD flash card used for permanent storage of the OS, LXE drivers and utilities is built into the CPU board. It is also used for registry content back up. Tap the **My Device** icon on the Desktop then tap the **System** icon.

Flash cards installed by the end-user are located in the socket under the main battery pack. Files on the end-user flash card can be accessed by tapping the **Storage Card** icon on the desktop.

CAB files, when executed, are not deleted.

ABOUTLXE.CAB	Lists installed OS, hardware and software versions.
API.CAB	Opens API files needed for proper operation.
SUMMIT.CAB	Summit Client files needed for radio operation. See Chapter 5 “Summit”
<b>The following CAB files are optional and may or may not be present:</b>	
BLUETOOTH.CAB	Bluetooth Client files needed for LXEZ Pairing operation.
LXE_MX8_ENABLER.CAB	Wavelink Avalanche Enabler.
RFTERM.CAB	RFTerm terminal emulation application.
JAVA.CAB	Java application.
APPLOCK.CAB	AppLock program. See Chapter 4 “AppLock”.

*Note: Always perform a warm boot when exchanging one flash card for another. Pre-formatted SD Flash cards are available from LXE, see “Accessories”. If a flash card requires formatting, it must be removed from the MX8 before formatting the card to FAT16.*

---

## ActiveSync / Get Connected Process

---

### Introduction

**Requirement:** ActiveSync version 3.7 (or higher) must be on the host (desktop/laptop, PC) computer.

A partnership between a PC and the MX8 must be established using serial RS-232 or USB connection. When more than one PC will be synchronizing with the MX8, each PC will need its own partnership with the MX8 established. See section titled “Initial Install” for the procedure.

After the partnership has been established with the MX8 and the host computer, ActiveSync can be performed over serial, USB, or radio (RF).

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your PC with the MX8 and vice versa. Synchronization compares the data on the MX8 with the PC and updates both with the most recent data. For example, you can:

- Synchronize Microsoft Word and Microsoft Excel files between your mobile device and PC. Your files are automatically converted to the correct format.
- Back up and restore your mobile device data.
- Copy (rather than synchronize) files between your mobile device and PC e.g. the MX8 LXEbook (the user’s guide in CE compatible format).
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your PC or only when you choose the synchronize command.
- Select which information types are synchronized and control how much data is synchronized.

*Note: By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your PC and your mobile device. If an information type is selected that does not exist on the MX8, the data appears to transfer, but it is ignored by the MX8 and not loaded.*

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


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

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



---

## Initial Install

Initial installation / relationship must be established using serial RS232 or USB cable connection between the MX8 and the desktop/laptop (PC). Once a relationship has been established, tap  | **Help** | **ActiveSync** for help.

---

## Install ActiveSync on Desktop/Laptop


Go to the Microsoft Windows website ActiveSync Download | Install file location:

[www.microsoft.com/downloads](http://www.microsoft.com/downloads)

and type **ActiveSync** in the Keywords text box. This process should locate the latest version of ActiveSync.

Install ActiveSync 3.7 (or later) on the PC before using ActiveSync to connect the PC to the mobile device.


Follow the instructions in the ActiveSync Wizard.

Check that  | **Programs** | **Communication** | **ActiveSync** | **Tools** | **Options** has the correct connection selected. Refer to "Serial Connection" or "USB Connection".

When installation of ActiveSync is complete on your PC, the ActiveSync Setup Wizard on the PC begins and it begins searching for a connected device.

Because ActiveSync is already installed on your mobile device, your first synchronization process begins automatically when you finish setting up your PC in the ActiveSync wizard and, using the USB cable, connect your mobile device to the PC.

## Serial Connection

Tap the  | **Settings** | **Control Panel** | **PC Connection** on the MX8. Tap the **Change Connection** button. From the popup list, choose

COM 1 @ 57600

*Note: The default is USB. LXE does not recommend using serial ActiveSync at 115 Kb/s.*

This will set up the MX8 to use COM 1. Tap OK and ensure the check box for "Enable direct connections to the desktop computer" is checked.

Tap OK to return to the Control Panel.

## USB Connection


Tap the  | **Settings** | **Control Panel** | **PC Connection** on the MX8. Tap the Change Connection button. From the popup list, choose

USB Default

This will set up the MX8 to use the USB configuration. Tap OK and ensure the check box for "Enable direct connections to the desktop computer" is checked.

Tap OK to return to Settings.

## **Connect -- Initial Install Process**

Connect the correct\*\* cable to the PC (the host) and the MX8 (the client). Tap the  | **Programs** | **Communication** | **Connect** icon on the MX8.

The MX8 connection is made using  | **Programs** | **Communication** | **ActiveSync**.

\*\* Cables for initial ActiveSync Configuration:

USB Client to PC/Laptop	MX8A051MULTICBLUSB
Serial Client to PC/Laptop	MX8A055MULTICBLDA9F

When the desktop/laptop computer and the MX8 successfully connect, the initial ActiveSync process is complete.

---

## **Change Connection Parameters**

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

<b>Option</b>	<b>Description</b>
USB (Default)	This will set up the MX8 to use the USB port direct.
COM1 @ 57600	This will set up the MX8 to use COM 1 direct at 57600 baud

- Tap OK and ensure the check box for “Enable direct connections to the desktop computer” is checked.
- Tap OK to return to Settings.
- Select Scanner and ensure the integrated scanner is set to a port that is different than the “Connect” port (COM 1).

---

## Backup MX8 Files

Use the following process to backup data files from the MX8 to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

---

### Prerequisites

Initial ActiveSync partnership between the MX8 and the target PC has been completed. After the partnership has been established with the mobile device and the host computer, ActiveSync can be performed over Serial, USB, or radio (RF).



**Figure 3-38 ActiveSync Connection Settings on a Windows PC**

### MX8 and PC Partnership

An ActiveSync partnership between the PC and MX8 has been established. See section “Initial Setup”.

### Serial Port Transfer

- A PC with an available serial port and an MX8 with a serial cable. The desktop or laptop PC must be running Windows 95, 98, NT, 2000 or XP.
- “Allow serial cable or infrared connection to this COM port” is checked.
- LXE recommends using the MX8 multipurpose RS-232 and Power cable listed in the following section titled “Connect”.

### USB Transfer

- A PC with an available USB port and an MX8 with a USB cable. The desktop or laptop PC must be running Windows 98 SR2, Windows 2000 or Windows XP.
- LXE-specific MX8 multipurpose USB and Power cable as listed in the following section “Connect”.
- “Allow USB connection with this desktop computer” is checked.

### Radio (RF) Transfer

- A PC or laptop with a radio card or wireless connection (requires ActiveSync for wireless transfers).
- The “Allow network (Ethernet) and Remote Access Service (RAS) server connection with this desktop computer” is checked.

---

## Connect

Connect the correct cable to the PC (the host) and the MX8 (the client).

Select "Connect" from  | **Programs** | **Communications** | **Connect**.

Cable, Multipurpose USB and Power	MX8A051MULTICBLUSB
Cable, Multipurpose RS-232 and Power	MX8A055MULTICBLDA9F

*Note:* USB will start automatically when the cable is connected.

---

## Explore

From the ActiveSync Dialog on the Desktop PC, click on the Explore button, which allows you to explore the MX8 from the PC side, with some limitations.

You can copy files to or from the MX8 using drag-and-drop.

You will not be allowed to delete files or copy files out of the \Windows directory on the MX8. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows OS image. This, however, includes most of the files in the \Windows directory).

For example, you can drag the "LXEbook – MX8 User's Guide" from your desktop computer to the My Documents folder on the MX8.

---

## Disconnect

---

### Serial Connection

- Disconnect the cable from the MX8.
- Put the MX8 into suspend by tapping the red Power button.
- Click the status bar icon in the lower right hand corner of the PC's status bar. Then click the Disconnect button.

---

### USB Connection

- Disconnect the cable from the MX8.
- Click the status bar icon in the lower right hand corner of the PC's status bar. Then click the Disconnect button.

**IMPORTANT** - Do not put the MX8 into suspend while connected via USB. The MX8 will be unable to connect to the host PC when it resumes operation.

---

### Radio Connection

- Put the MX8 into Suspend Mode by tapping the red Power button.
- Click the status bar icon in the lower right hand corner of the PC's status bar. Then click the Disconnect button.

---

## Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a mobile device and a PC. A partnership is defined by two objects -- a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership for a unique client can be established to two hosts.

If the MX8 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. (Windows | **Settings** | **Control Panel** | **System** | **Device Name**)

If the cold booted MX8 tries to reestablish the partnership with the same host PC, a new random number is generated for the MX8 and ActiveSync will insist the unique name of the MX8 be changed. If the MX8 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 Troubleshooting

**ActiveSync on the host returns to the Get Connected screen without connecting to the cabled device.**

If the MX8 is connected to a PC by a cable, disconnect the cable from the MX8 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 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.

Try the following to re-establish the connection:

*On the Host (desktop or laptop PC)*

1. Open ActiveSync.
2. Select File | Connection Settings and disable “Allow serial cable or infrared connection to this COM port”.
3. Click OK.
4. Select File | Connection Settings and enable “Allow serial cable or infrared connection to this COM port”.

*On the MX8*

Tap Start | Programs | Communication | Connect to establish an ActiveSync connection to the host.

**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.**

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.

-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 selecting Start | Programs | Communication | Connect on the CE device, the word "CLIENT" appears on the CE 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.

**Drop down list is blank in the ActiveSync dialog box**

The radio link is broken. Make sure that the radio has a valid IP address.

## Utilities

These utilities are pre-loaded by LXE.

*Note: AppLock Administrator Control panel Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels or in LAUNCH.EXE. For example, Keypad Control Panel LaunchApp and RunCmd options.*

---

## LAUNCH.EXE

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

Then, information is added to the Launch.reg file on the internal Flash drive to make the CAB file auto-launch at startup. The CAB file can update the registry (Launch.REG) 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 installation/executable file. Then 3 values are added:

**FileName** is the name of the CAB file, with the path (usually `\System`)

**Installed** is a DWORD value of 0, which changes to 1 once auto-launch installs the file

**FileCheck** is the name of a file to look for to determine if the CAB file is installed.

The value in FileCheck is the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

Three optional fields are also added: **Order**, **Delay**, and **PCMCIA**. These are all DWORD fields, described below.

The auto-launch process goes as follows. The launch utility opens the registry database and reads the list of CAB files to auto-launch. First it looks for **FileName** to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the **Installed** flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it. If the **Installed** flag is set, auto-launch looks for the **FileCheck** file. If it is present, the CAB file is installed, and that registry entry is complete. If the **FileCheck** file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file. Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.

To force execution every time (for example, for **AUTOEXEC.BAT**), use a **FileCheck** of “dummy”, which will never be found, forcing the item to execute.

For persist keys specifying **.EXE** or **.BAT** files, the executing process will be started, and then **Launch** will continue, leaving the loading process to run independently. For other persist keys (including **.CAB** files), **Launch** will wait for the loading process to complete before continuing. This is important, for example, to ensure that a **.CAB** file is installed before the **.EXE** files from the **.CAB** file are run.

The **Order** field is used to force a sequence of events; **Order=0** is first, and **Order=99** is last (note that the order number given here is the decimal equivalent to hexadecimal number 63). Two items which have the same order will be installed in the same pass, but not in a predictable sequence. Note: If the order of loading is not critical, it may be easier to use the `\System\Startup` folder instead; see below.

The **Delay** field is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to **0** if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default radio drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.

Note that the auto-launch process can also launch batch files (\*.BAT), executable files (\*.EXE), registry setting files (\*.REG), or sound files (\*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Registry information is already in the default image for the following <sup>2</sup>:

```

;; ----- autoexec batch file - for users convenience
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AUTOEXEC]
  "FileName"="\System\Autoexec.bat"
  "Installed"=dword:0
  "FileCheck"="ALWAYSEXEC"
  "Order"=dword:50
;; The file name "ALWAYSEXEC" or "dummy" does not really matter as long as there is
;; no file of that name in the directory. You can use any name that you want for this entry
;; as long as it is a non existent file name. The purpose of this value is that if someone
;; wants to only execute this file one time then you would replace the value of FileCheck
;; with the name of a file that would exist the next time a warm boot occurs.

;; special function - makes Launch copy system folders from ATA drive
;; we put it in here so that we control when it happens (esp. for Applock)
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
  "FileName"="COPYFOLDERS"
  "Installed"=dword:0
  "FileCheck"=""
  "Order"=dword:10

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Wifi Utility]
  "FileName"="\Windows\Wifi_Utility.exe"
  "Installed"=dword:0
  "FileCheck"="ALWAYSEXEC"
  "Order"=dword:20

;; ----- Summit radio support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Summit Radio]
  "FileName"="\System\SUMMIT.CAB"
  "Installed"=dword:0
  "FileCheck"="\WINDOWS\SDCCF10G.DLL"
  "Order"=dword:2
  "PCMCIA"=dword:1

; ----- RFTerm support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
  "FileName"="\System\RFTERM.CAB"
  "Installed"=dword:0
  "FileCheck"="\WINDOWS\LXE\RFTERM.EXE"
  "Order"=dword:11

;; run the app after it has loaded and radio is ready
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
  "FileName"="\WINDOWS\LXE\RFTERM.EXE"

```

<sup>2</sup> 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.



```

        "Installed"=dword:0
        "FileCheck"="ALWAYSEXEC"
        "Order"=dword:40
        "Delay"=dword:1

;; ----- Avalanche support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
    "FileCheck"="\System\avalanche\model.dat"
    "Installed"=dword:0
    "Order"=dword:4
    "FileName"="\System\LXEAVA.CAB"

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
    "Order"=dword:5
    "FileName"="\System\Avalanche\Avainit.exe"
    "FileCheck"="ALWAYSEXEC"
    "Installed"=dword:0

;; ----- Applock support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockInstall]
    "FileName"="\System\AppLock.CAB"
    "Installed"=dword:0
    "FileCheck"="\WINDOWS\APLOCK.EXE"
    "Order"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockPrep]
    "FileName"="\windows\AppLockPrep.exe"
    "Installed"=dword:0
    "FileCheck"="ALWAYSEXEC"
    "Order"=dword:1
    "Delay"=dword:2

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLock]
    "FileName"="\windows\AppLock.exe"
    "Installed"=dword:0
    "FileCheck"="ALWAYSEXEC"
    "Order"=dword:63

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\KbdLocks]
    "FileName"="\windows\KbdLocks.exe"
    "Installed"=dword:0
    "FileCheck"="ALWAYSEXEC"
    "Order"=dword:62

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Bluetooth]
    "FileName"="\System\Bluetooth.CAB"
    "FileCheck"="ALWAYSEXEC"
    "Installed"=dword:0
    "Order"=dword:30

```

When you are installing your custom CAB file to the mobile device's operating system, refer to the default image segments that are commented with "... RFTerm ..." to see the expected Registry format.

One special key is included to force the system folders (Desktop, Fonts, Programs, etc.) to copy from the internal ATA card (\System) to the \Windows directory. This is implemented as a persist key so the sequence of startup events can be controlled (especially for AppLock). The filename is a special internal trigger for the Launch utility, to activate the **CopyFolders** function. *DO NOT EDIT OR ALTER THIS KEY, OR IT MAY NO LONGER FUNCTION.* You may however change the **Order** or **Delay** values if necessary for a particular startup sequence.

```

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
    "FileName"="COPYFOLDERS"

```

```
"FileCheck"=""
"Order"=dword:0F
```

To have files (CAB, EXE, REG, or WAV files) loaded on startup, when sequence of execution is not important, you can put these files in the **\System\Startup folder** (on the internal Flash card). This is parsed by the Launch utility, and these programs are started or executed.

---

## ClearHive.EXE

Command line utility which causes the Registry to be reset to original factory settings. The command is not case-sensitive. Run **\Windows\ClearHive.exe** using the virtual keypad or Soft Input Panel (SIP). Tap Enter or OK.

Passwords are lost upon reset to factory settings. If a password is set, that password must be entered to begin the ClearHive reset process.

---

## GrabTime.EXE

*Note: This utility affects the behavior of GrabTime at warmboot. After a coldboot, GrabTime is disabled.*

The MX8 has a GrabTime utility which can automatically synchronize the MX8 with a worldwide time server (via an Internet connection) at boot up. By default, GrabTime for time synchronization at boot up is Off.

To enable GrabTime to run automatically at boot up, run **\Windows\grabtime.exe** and perform a warm boot (Enter + Power). For more detail, see *LAUNCH.EXE*, earlier in this chapter.

---

## Synchronize with a local time server

- Use ActiveSync to copy **GrabTime.ini** from the **My Device | Windows** folder on the MX8 to the host PC.
- Edit GrabTime.ini (on the host PC) to add the local time server's domain name to the beginning of the list of servers. You can then optionally delete the remainder of the list.
- Copy the modified GrabTime.ini to the **My Device | System** folder on the MX8.
- The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. Each time the mobile device is cold booted, the Windows/GrabTime.ini file is replaced with the default version and the System/GrabTime.ini file is not.

---

## RegEditor.EXE



Before using REGEDITOR.EXE, please refer to commercially available Microsoft Power Tools for Windows manuals. For example Microsoft Windows Registry Guide, Second edition.

The Registry Editor allows viewing, searching for items and changing settings in the registry (Launch.REG). The registry contains information about how the mobile device runs. LXE recommends **caution** when inspecting and editing the Registry as making incorrect changes can damage the mobile device operating system. LXE recommends making a backup copy of the registry before viewing or *carefully* making changes to the registry.

---

## RegDump.EXE

Double-tapping the RegDump.EXE file causes the contents of the Registry to be copied to an ASCII text file (Reg.txt) in the My Documents folder.

---

## 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.

## Wavelink Avalanche Enabler Configuration

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

---

## Briefly . . .

The Wavelink Avalanche Enabler installation file is loaded on the mobile device by LXE; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

*Note: On LXE mobile devices with integrated scanners, the Scanner Wedge has primary control of the serial ports and must be configured properly to allow the Enabler to access the serial ports.*

---

## Enabler Install Process

- Doubletap the Avalanche Enabler CAB file in the System folder. The filename is LXE\_MX8\_ENABLER.CAB.
- Warm boot the mobile device.

---

## Enabler Uninstall Process

To remove the LXE Avalanche Enabler from a Windows CE mobile device:

- Delete the Avalanche folder located in the System folder.
- Warm boot the mobile device.

The Avalanche folder cannot be deleted while the Enabler is running. See *Stop the Enabler Service*. If sharing errors occur while attempting to delete the Avalanche folder, warm boot the mobile device, immediately delete the Avalanche folder, and then perform another warm boot.

### Orphaned Packages

To prevent the enabler from restoring parameters, delete orphaned packages through the Avalanche Mobility Center (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details and instruction).

## Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Avalanche MC Console:

1. Open the Enabler Settings Panels by tapping the Avalanche icon on the desktop.
2. Select File | Settings. Enter the password.
3. Select the Startup/Shutdown tab.
4. Select the “Do not monitor or launch Enabler” parameter to prevent automatic monitoring upon startup.
5. Select Stop Monitoring for an immediate shutdown of all enabler update functionality upon exiting the user interface.
6. Click the OK button to save the changes.
7. Reboot the device if necessary.

---

## Update Monitoring Overview

There are three methods by which the Enabler on an LXE device can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server and the LXE device.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server and the mobile device.
- Wirelessly via the 2.4GHz network card and an access point

After installing the Enabler on the mobile unit, a reboot is required for the Enabler to begin normal functionality. Following a mobile device reboot, the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network. The designation of the mobile device to the Avalanche Mobility Center Manager is `LXE_MX8`.

The Enabler running on LXE Windows CE devices will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the LXE scanner applet in the Control Panel).

The wireless connection is made using the default client interface on the mobile device therefore the device must be actively communicating with the network for this method to succeed. If a Mobile Device Server is found, the Enabler will automatically attempt to apply all wireless and network settings from the active profile. When configured to download available packages, the Enabler will also automatically download and process all available packages.

---

## Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the Enabler will attempt to apply all network and wireless settings contained in the active profile. The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler. These local parameters cannot be overridden from the Avalanche Mobility Center Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE Units

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Avalanche icon on the desktop.
2. Select File | Settings. Enter the password.
3. Select the Adapters tab.
4. Choose settings for the “Use Manual Settings” parameter.
5. Choose settings for “Manage Network Settings”, “Manage Wireless Settings” and “Use Avalanche Network Profile”.
6. Tap the OK button to save the changes.
7. Reboot the device.

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

## Enabler Configuration

Avalanche Icon



The Enabler user interface application is launched by clicking:

either the Avalanche icon on the desktop or Taskbar

or

selecting Avalanche from the Programs menu.

The opening screen presents the user with the connection status and a navigation menu.




**Figure 3-39 Avalanche Enabler Opening Screen**

File	View	Help
Connect	Updates	Adapter Info
Abort	Programs	About
Settings	Icons	
Scan Config	List	
Exit	Details	
	Launchable	
	All Packages	
	Time on Taskbar	
	Device Status	

### File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the mobile device immediately upon a successful connection.
Abort	Stop transmission.

Settings	<p>The Settings option under the File menu allows the user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected. The default password is</p> <p style="text-align: center;"><b>system</b></p> <p>The password is not case-sensitive.</p>
Scan Config	<p><i>Note: LXE does not support the Scan Configuration feature on Windows CE devices.</i> The Scan Config option under the File menu allows the user to configure Enabler settings using a special barcode that can be created using the Avalanche Management Console utilities. Refer to the <i>Wavelink Avalanche Mobility Center User's Guide</i> for details.</p>
Exit	<p>The Exit option is password protected. The default password is</p> <p style="text-align: center;"><b>leave</b></p> <p>The password is not case-sensitive.</p> <p>If changes were made on the Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed:</p> <div data-bbox="818 806 1154 1003" style="text-align: center;">  </div> <p>Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.</p>

## Avalanche Update using File | Settings

### Access: Start | Avalanche | File | Settings

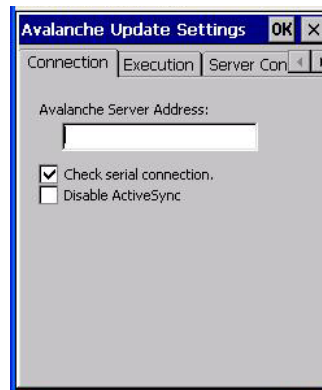
Use these menu options to setup the Avalanche Enabler on the mobile device. LXE recommends changing and then saving the changes (reboot) before connecting to the network.

Alternatively, the Mobile Device Server can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details – available on the Wavelink Avalanche website).

## Menu Options

Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF are used to check for the presence of the Mobile Device Server.
Execution	<i>Unavailable in this release.</i> LXE recommends using AppLock, which is resident on each Windows CE mobile device. See Chapter 6 - AppLock.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Startup/Shutdown	Set options for Enabler program startup or shutdown.
Scan Config	This option allows the user to configure Enabler settings using a special barcode that is created by the Avalanche Mobility Center Console. <i>Not currently supported by LXE.</i>
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.



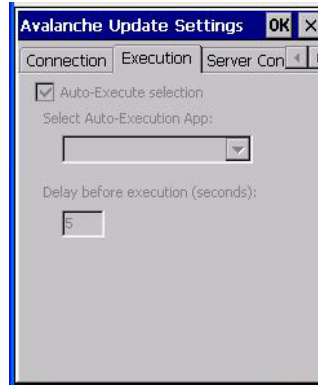
**Connection Tab****Figure 3-40 Avalanche Enabler Connection Options**

Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the mobile device.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.

## Execution Tab

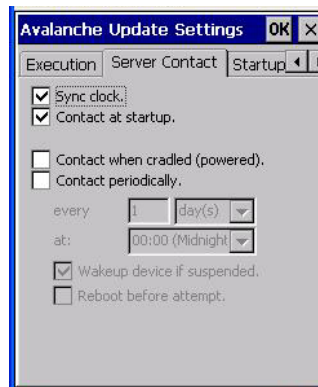
Note the dimmed options on this panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.

Unavailable in this release. LXE recommends using AppLock. See *Chapter 6 – AppLock*.



**Figure 3-41 Avalanche Enabler Execution Options (Dimmed)**

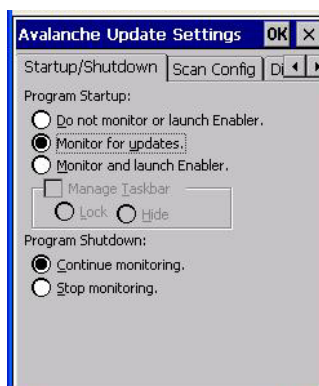
Auto-Execute Selection	An application that has been installed with the Avalanche Mobility Center Console can be run automatically following each reboot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Mobility Center Console.
Delay before execution	Time delay before launching Auto-Execute application.

**Server Contact Tab****Figure 3-42 Avalanche Enabler Server Contact Options**

Sync Clock	Reset the time on mobile computer based on the time on the Mobile Device Server.
Contact at startup	Connect to the Mobile Device Server when the Enabler is accessed.
Contact when cradled	Initiate connection to the Mobile Device Server based on a docking event. <i>Not available on the MX8.</i>
Contact Periodically	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can 'wakeup' and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.

### Startup/Shutdown Tab

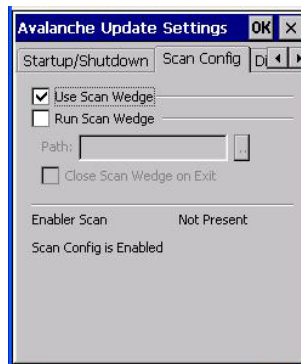
**LXE recommends using AppLock for this function.** AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in *Chapter 6 AppLock*.



**Figure 3-43 Avalanche Enabler Startup / Shutdown Options**

Do not monitor or launch Enabler	When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
Monitor for updates	Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Manage Taskbar (Lock or Hide)	Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.
Program Shutdown (Continue or Stop monitoring)	The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

### Scan Config Tab



*Note: Scan Config functionality is a standard option of the Wavelink Avalanche System but is not currently supported by LXE on Windows CE devices.*

**Figure 3-44 Avalanche Enabler Scan Config Option**

### Display Tab



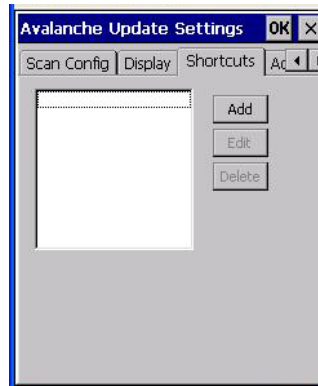
**Figure 3-45 Avalanche Enabler Window Display Options**

The user interface (Update Window Display) for the Enabler can be configured to dynamically change based on the status of the connection with the Mobile Device Server.

At startup	Half screen, Hidden or Full screen. Default is Half screen.
On connect	As is, Half screen, full screen, Locked full screen. Default is As is.
Normal	Half screen, Hidden or As is. Default is As is.

## Shortcuts Tab

**LXE recommends using AppLock for this function.** AppLock is resident on each LXE mobile device with a Windows OS.



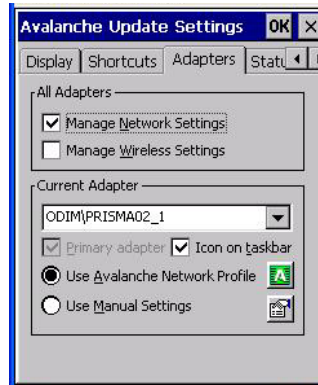
**Figure 3-46 Avalanche Enabler Application Shortcuts**

Configure shortcuts to other applications on the mobile device. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

LXE recommends using AppLock for this function. See *Chapter 6 - AppLock* for instruction.

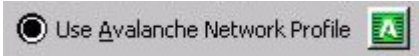

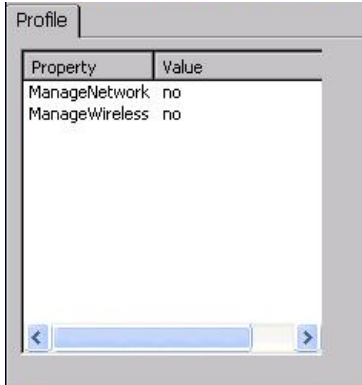
## Adapters Tab



*Note: LXE recommends the user review the network settings configuration utilities and the default values in [Chapter 5 – Wireless Network Configuration](#) before setting All Adapters to Enable in the Adapters applet.*



**Figure 3-47 Avalanche Enabler Adapters Options - Network**

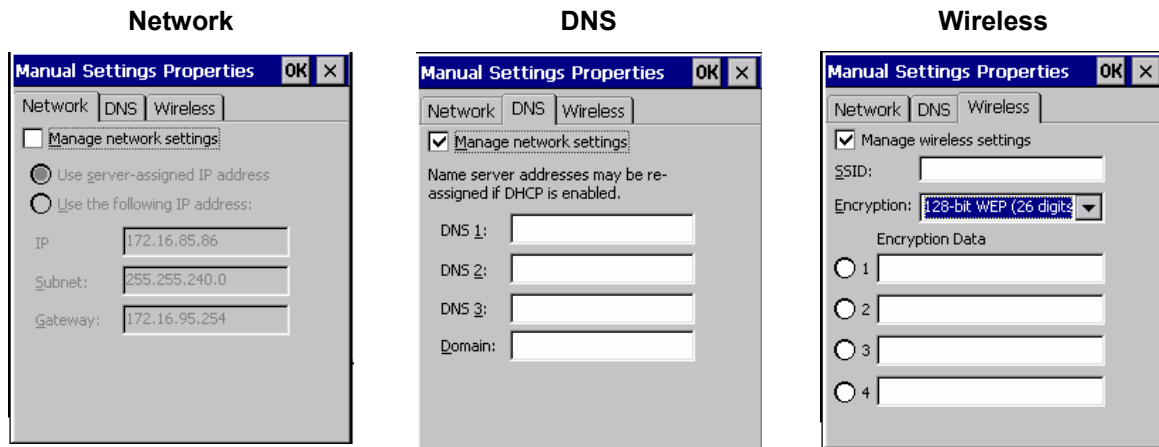
Manage Network Setting	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Management Console and is disabled by default. This parameter setting <b>does not apply to Summit Clients only</b> .
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.

Use Avalanche Network Profile	<p>The Enabler will apply all network settings sent to it by the Avalanche Mobility Center Console.</p> 
<p>Avalanche Icon</p> 	<p>Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.</p>  <p><b>Figure 3-48 Avalanche Network Profile Displayed</b></p>

Use Manual Settings	<p>When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche Mobility Center Console and use only the network settings on the mobile device.</p> 
<p>Properties Icon</p> 	<p>Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:</p>

*Note: A reboot may be required after enabling or disabling these options.*





For device-specific descriptions of these Enabler parameters, refer to Chapter 5 “Wireless Network Configuration”.

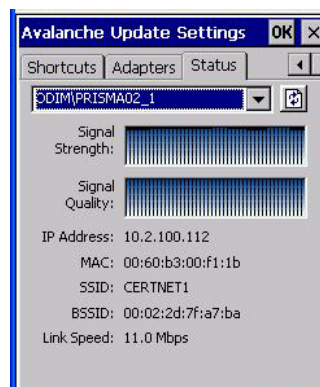
LXE does **not** recommend enabling **Manage Wireless Settings**.

**Figure 3-49 Manual Settings Properties Panels**

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global **Manage wireless settings** and **Manage network settings** options are enabled on the Adapters panel (see Figure titled *Avalanche Enabler Adapters Options – Network*). Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

### Status Tab

The Status panel displays the current status of the mobile device network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button. When tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



**Figure 3-50 Status Display**

Link speed indicates the speed at which the signal is being sent from the adapter to the mobile device. Speed is dependent on signal strength.

## Troubleshooting

### Cold Boot

If a device managed by Avalanche is cold-booted, a warmboot MUST be performed following the coldboot. Failure to perform the warmboot will leave the device in an undetermined configuration and it may not perform as expected. If the intention is to stop using Avalanche to manage the device configuration, please see *Enabler Uninstall Process* earlier in this section.

## 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 LXEAPI.ZIP, 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 LXEAPI, 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 (on the accessories CD) is now included for Microsoft Embedded Visual C++ 4.0 (which is available free on the Microsoft website).

## Clearing Registry Settings

Run ClearHive.exe application. This application will put all registry settings back to LXE factory defaults. The Touch Recalibration screen will appear after the system boots up.

---

## Reflash the Mobile Device

*Note:* When reflashing, LXE recommends using a SD Flash card that is greater than 64MB. Files to be loaded on the Flash card are: OSImage.NB0, BLImage.NB0, MX8Update.exe

The MX8 starts the operating system upon every warm boot or cold boot. If available, always perform MX8 updates when there is a fully charged backup battery and/or a dependable external power source connected to the MX8.

The bootloader and OS are written to onboard flash using the utility MX8Update.EXE.

---

## Preparation

LXE recommends that installation of the Mini SD Flash card be performed on a clean, well-lit surface.



**Figure 3-51 SD Card Location**

Place the mobile device in Suspend Mode and remove the main battery pack.

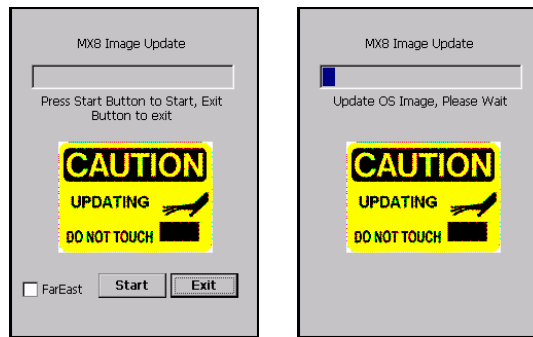
Lift the rubber barrier and pull the Mini SD card out of the slot. Do not remove the rubber barrier.

---

## Procedure

*Note:* If the image to be updated is a Far East Language image (48M), check the FarEast checkbox before updating to a Simplified Chinese, Traditional Chinese, Korean or Japanese version of the OS. The update process may take between 6 and 10 minutes when FarEast is checked.

8. Place the Mini SD flash card with new image files on it into the SD slot. The label on the SD card is facing up.
9. Launch MX8UPDATE.EXE in My Device | Storage Card.
  - **Important:** If a failure occurs during the update, DO NOT COLD BOOT. Follow the instructions on the screen to Exit the update utility. Restart the update utility.
10. Tap **Start** to start the update. Tap **Exit** to exit without updating.




**Figure 3-52 MX8 Image Update**

When the flash update is complete, remove the SD card (if desired), replace the rubber barrier and replace the main battery. The unit automatically performs a cold boot.

## Command Line Interface

### Notes

- My Device\System is a priority searching location for the source file, so if My Device\Storage Card is an intended source, make sure there is no corresponding file in My Device\Storage Card.
- If main battery life is less than 50%, there will be a message box popup to warn user. The application will wait for user's confirmation before proceeding to update.
- In case of update error, the application will not reboot the system, instead, it will show the error message on screen and wait for user's confirmation to proceed.
- If available, always perform MX8 updates when there is a fully charged backup battery and/or a dependable external power source connected to the MX8.

<b>Warning</b> 	<p>If the application displays “Update OS Image Failed” or “Update Boot Loader Image Failed”, <b>do not cold boot</b> the system manually. Perform a warm boot, then try reflashing again. Cold booting will cause an MX8 system crash, since there is no valid image in the system.</p>
---	--

Place new image files on a Mini SD card or in the System Folder.

Launch the MX8Update.exe from another application using the following format:

**MX8Update.exe -[F|L]**

Use -F for Far East Language Image(48M), -L for Latin Language Image (40M).

**-path** Specifies the path where the image files are located. Example: MX8Update -path\storage\remote. If the path parameter is not present, MX8Update searches in My Device\System then \Storage Card for the image files.

**-auto** When this command line option is specified, the update is started automatically. No user interaction is required. The Start button is dimmed.

**-fe** Repartitions the on-board flash to a 50MB partition for the OS image.

When the automatic flash update is complete, replace the rubber barrier and replace the main battery.

## Chapter 4 Scanner

### Introduction

**Access:**  | [Settings](#) | [Control Panel](#) | [Scanner](#)

Set scanner keyboard wedge parameters, enable or disable symbologies from being scanned, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Scanner parameters apply to the MX8 integrated scanner/imager *only*. Barcode manipulation parameters apply to barcodes scanned by the MX8 integrated scanner/imager engine.

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



Integrated Scanner Programming Guide and the **factory defaults** barcodes. After scanning the scanner-engine-specific barcode to reset all scanner parameters to factory default settings (i.e. Reset All, Set Factory Defaults, Default Settings, etc.), the next step is to open the Control Panel Scanner Properties panel. Tap the OK button and close the Scanner panel. This action will synchronize all scanner formats.

The MX8 may have a Symbol laser scan engine (Start | Settings | Control Panel | About):

- [Symbol SE955-I000WR](#)

or one of two Imagers:

- [Intermec EV-15 Imager](#)
- [Hand Held Products 5380SF 2D Imager](#)

The integrated scan engine activates when the Scan button on the front of the MX8 is depressed or when the trigger on an installed trigger handle is depressed.



Please refer to the *Integrated Scanner Programming Guide* for instruction on configuring specific scanner/imager parameters by using the MX8 to scan engine-specific setup barcodes in the guide.

## Barcode Processing Overview

*Note: Steps 1-7 describe the barcode manipulation. Steps 8-12 describe how the manipulated data is built. Step 13 describes how the manipulated data is output.*

The complete sequence of barcode processing is as follows:

1. Scanned barcode is tested for a **code ID**. If one is found, it is stripped from the data, and the settings for the symbology specified are used. Otherwise, the **All** symbology settings are used.
2. If symbology is **disabled**, the scan is rejected.
3. If the **length** of data (minus the code ID) is out of specified **Min/Max** range, the scan is rejected.
4. Strip **leading** data bytes unconditionally.
5. Strip **trailing** data bytes unconditionally.
6. Parse for, and strip if found, **Barcode Data** strings.
7. Replace any **control characters** with string, as configured.
8. Add **prefix** string to output buffer.
9. If **Code ID** is *\*not\** stripped, add saved **code ID** from above to output buffer.
10. Add processed **barcode** string from above to output buffer.
11. Add **suffix** string to output buffer.
12. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
13. If key output is enabled, start the process to output keys. If control characters are encountered:
  - If **Translate All** is set, key is translated to CTRL + char, and output.
  - If **Translate All** is not set, and key has a valid VK code, key is output.
  - Otherwise, key is ignored (not output).

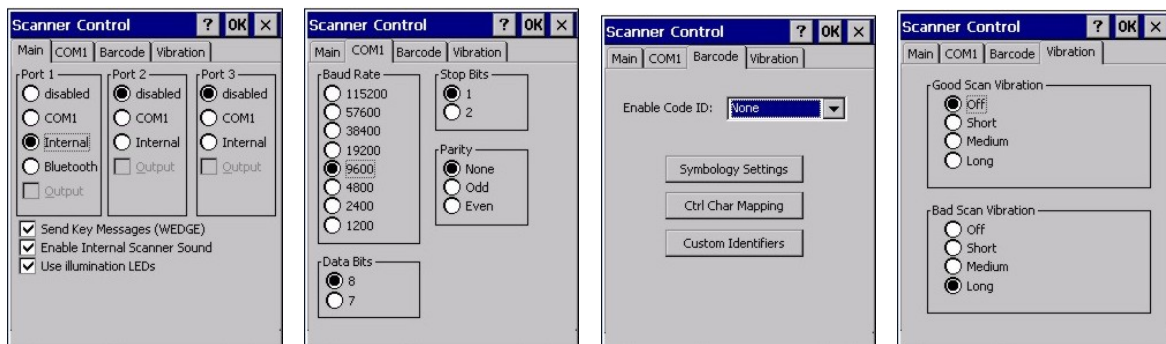
The data is ready to be read by applications.

See *Barcode Processing Examples* at the end of the *Barcode Tab* section.

See *Valid VK Codes for CE*.

## Factory Default Settings

Factory Default Settings	
<b>Main</b>	
Port 1	Internal
Port 2	Disabled
Port 3	Disabled
Send key messages (WEDGE)	Enabled
Enable Internal Scanner Sound	Enabled
Use Illumination LEDs	Enabled
<b>COM1 Port (external serial port)</b>	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
<b>Barcode</b>	
Enable Code ID	None
<b>Vibration</b>	
Good Scan Vibration	Off
Bad Scan Vibration	Long



**Figure 4-1 Scanner Control Panels**

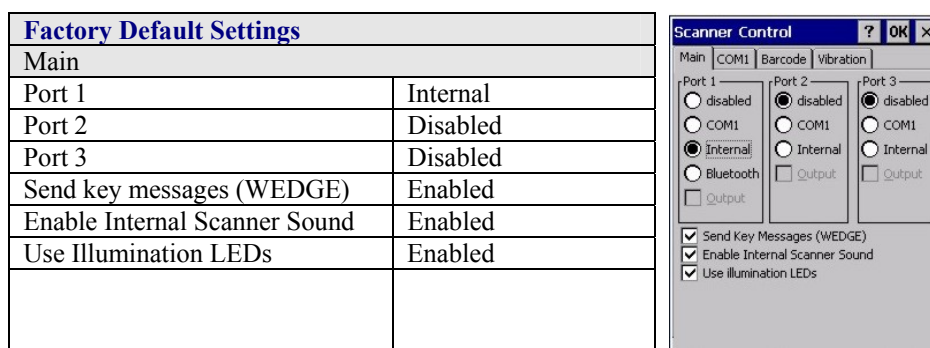
If “Send Key Messages ...” is checked any data scan is converted to keystrokes and sent to the active window. When this box is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using “Wedge”.

Disable “Enable Internal Scanner Sound” when you want an application, not the scan engine or the CE operating system, to control scanner audible notifications. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Disable “Use Illumination LEDs” when the integrated imager does not have illumination LEDs.

## Main Tab

Access:  | Settings | Control Panel | Scanner | Main tab



**Figure 4-2 Scanner Control / Main**

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

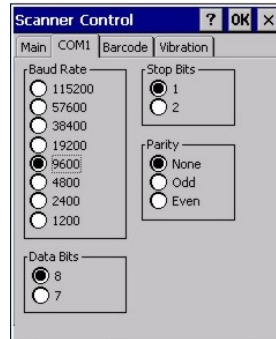
Parameter	Function
Port	<p>Port 1 – Internal. Radio button allows scanner input/output on Port 1 (scan key or trigger).</p> <p>Port 2 – Output is enabled when COM1 is enabled on this port.</p> <p>Port 3 - Output is enabled when COM1 is enabled on this port.</p>
Send Key Messages (WEDGE)	<p>When Send Key Messages (WEDGE) 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”.</p>
Enable Internal Scanner Sound	<p>The default is Enabled. Functionality of the internal scanner driver engine includes audible tones on good scan (at the maximum db supported by the speaker) and failed scan. If enabled, Good Scan / Bad Scan Vibration provides a tactile response on a scan event.</p> <p>Disable this parameter when good scan/bad scan sounds are to be handled by alternate means e.g. application-controlled sound files.</p> <p>Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from an external scanner, and then the rejection of scanned barcode data by the processing causes a bad scan beep from the MX8 on the same data.</p>
Use Illumination LEDs	<p>The default setting is Enabled. Integrated imager may use illumination LEDs when scanning a barcode.</p>



## COM1 Tab

Access:  | Settings | Control Panel | Scanner | COM1 tab

Factory Default Settings	
COM1 Port (external serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8



**Figure 4-3 Scanner Control / COM1**

Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

If these values are changed, the default values are restored after a cold boot or reflashing.

*Note:* COM1 does not support 5V switchable power on Pin 9 for tethered scanners.

## Barcode Tab

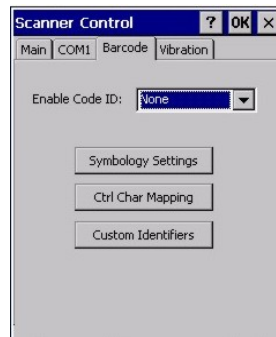
**Access:**  | **Settings | Control Panel | Scanner | Barcode tab**

The Scanner application (Wedge) can only enable or disable the processing of a barcode inside the Wedge software.

The Scanner application enables or disables the Code ID that may be scanned.

Enabling or disabling a specific barcode symbology is done manually using the configuration barcode in the *Integrated Scanner Programming Guide* (available on the LXE Manuals CD and the LXE ServicePass website).

Choose an option in the Enable Code ID drop-down box: None, AIM ID, Symbol ID, or Custom ID.



**Figure 4-4 Scanner Control / Barcode tab**

## Buttons

Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

See Also: *Barcode Processing Overview* earlier in this chapter.

## Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed. If the scanner being configured is not an integrated scanner, the scanner driver expects that the setting has been programmed into the scanner externally, and that the data will be coming in with the specified Code ID attached.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

### Options

None	Programs the internal scanner to disable transmission of a Code ID. The only entry in the Symbology popup list is All.
AIM	Programs the internal scanner to transmit the AIM ID with each barcode. The combo box in the Symbology control panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.
Symbol	Programs the internal scanner to transmit the Symbol ID with each barcode. The combo box in the Symbology control panel is loaded with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.  <i>Note: The Symbol entry may not appear on mobile devices with integrated imagers (e.g. EV-15 Imager).</i>
Custom	Does not change the scanner's Code ID transmission setting. The combo box in the Symbology control panel is loaded with any configured Custom Code IDs.

### Notes

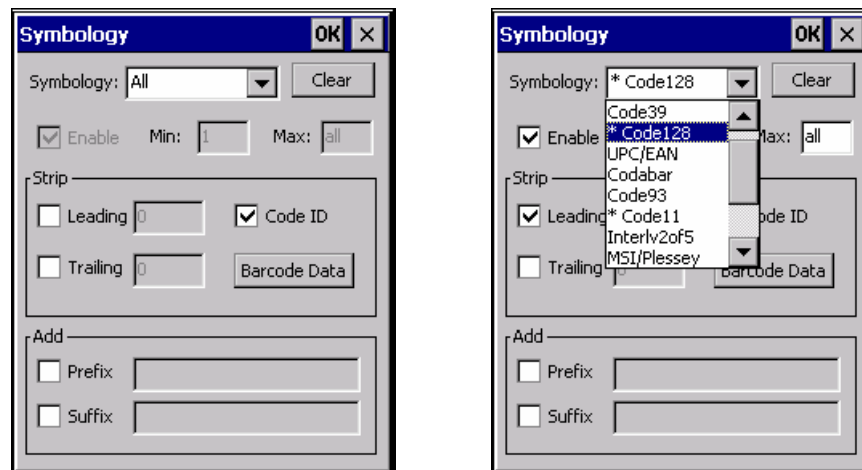
- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the barcode data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e. treated as a Code ID).
- UPC/EAN Codes only: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to AIM or Symbol, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 'JA1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID : JA1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- The external scanner operation cannot be controlled by the MX8 scanner driver; therefore, a 'good' beep may be sounded from the external scanner even if a barcode from an external scanner is rejected because of the configuration specified. The MX8 will still generate a 'bad' scan beep, to indicate the barcode has been rejected.

## Barcode – Symbology Settings

The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured. The features available on the Symbology Settings dialog include the ability to individually enable or disable a barcode from scanning, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode.

The Symbology drop-down box contains all symbologies **supported on the MX8**. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is tapped. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.



**Figure 4-5 Barcode Tab / Symbology Settings**

**Clear** This button will erase any programmed overrides, returning to the default settings for the selected symbology. If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (\*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix and Suffix

*Note: When **Enable Code ID** is set to **None** on the Barcode tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Barcode tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as code IDs.*

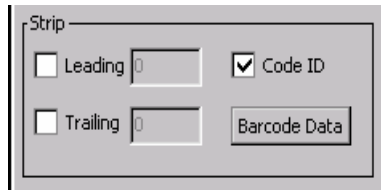
If a specific symbology's settings have been configured, a star (\*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults. If a particular symbology has been configured, the entire set of parameters from that

symbolologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two. If a symbology has not been configured (does not have an \* next to it) the settings for “All” are used which is not necessarily the defaults.

### Parameters

Enable	<p>This checkbox enables (checked) or disables (unchecked) the symbology field.</p> <p>The scanner driver searches the beginning of the barcode data for the type of ID specified in the Barcode tab – Enable Code ID field (AIM or Symbol) plus any custom identifiers.</p> <p>When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed. If the symbology is disabled, all other fields on this dialog are grayed.</p> <p>When there are <i>no customized settings</i>, and the Enable checkbox is unchecked (All is selected and no other settings are customized) a confirmation dialog is presented to the user “You are about to disable all scan input – Is this what you want to do?”. Tap the Yes button or the No button. Tap the X button to close the dialog without making a decision.</p> <p>If there <i>are customized settings</i>, uncheck the Enable checkbox for the All symbology. This results in disabling all symbolologies except the customized ones.</p>
Min	<p>This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed. Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.</p>
Max	<p>This field specifies the maximum length that the barcode data (not including Code ID) can be to be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999). If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length will be used instead.</p>

### Strip Leading/Trailing Control



**Figure 4-6 Symbology / Strip Leading / Trailing**

This group of controls determines what data is removed from the barcode before the data is buffered for the application. If all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.

If the total number being stripped is greater than the number of characters in the barcode data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

- |                 |  |
|-----------------|--|
| <b>Leading</b>  | This strips the number of characters specified from the beginning of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default.  |
| <b>Trailing</b> | This strips the number of characters specified from the end of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default.  |
| <b>Code ID</b>  | Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise). |

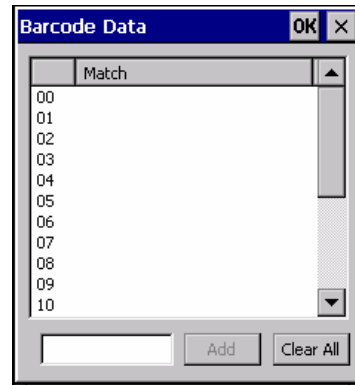
### Barcode Data Match List

#### **Barcode Data**

This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.

To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap the OK button to store any additions, deletions or changes.



**Figure 4-7 Symbology / Barcode Data Match List**

### Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Tap the <b>Add</b> button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The <b>Add</b> button changes to <b>Insert</b> . Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The <b>Add</b> button changes to <b>Replace</b> . When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The <b>Clear All</b> button changes to a <b>Remove</b> button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

#### **Notes**

- Prefix and Suffix data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a 'good' beep will still emit, since barcode data was read from the scanner.

## Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ABC and AB, in that order, incoming data with ABC will match first, and the AB will have no effect.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard \* is not specified, the string is assumed to strip from the beginning of the barcode data. The string ABC\* strips off the prefix ABC. The string \*XYZ will strip off the suffix XYZ. The string ABC\*XYZ will strip both prefix and suffix together. More than one \* in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first \* is used in parsing to match the string.)
- The question mark wildcard ? may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The Barcode Data is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of Strip: Code ID in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the barcode data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.



### Add Prefix/Suffix Control

See Also: *Barcode Processing Overview* earlier in this chapter.

 A screenshot of a software control panel titled "Add". It contains two rows of controls. The first row has a checkbox labeled "Prefix" followed by a text input field. The second row has a checkbox labeled "Suffix" followed by another text input field. The entire panel is enclosed in a rectangular border.

**Figure 4-8 Symbology / Prefix and Suffix Control**

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see the “Hat Encoding” section in Appendix B for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

**Add Prefix** To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the prefix is added for any symbology that has not been specifically configured.

**Add Suffix** To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the suffix is added for any symbology that has not been specifically configured.

See “Hat Encoding” and “Decimal-Hexadecimal Chart” in Appendix B “Technical Specifications”.

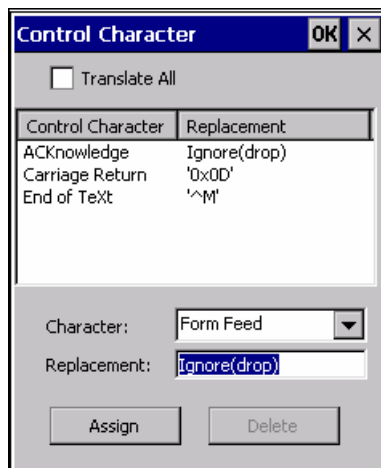
*Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. <F1>), arrow keys, Page up, Page down, Home, and End.*

---

## Barcode – Ctrl Char Mapping

See Also: *Barcode Processing Overview* earlier in this chapter.

The Ctrl Char Mapping button activates a dialog to define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.



**Figure 4-9 Barcode Tab / Ctrl Char Mapping**

See “Hat Encoding” and “Decimal-Hexadecimal Chart” at the end of Appendix B “Technical Specifications”.

## Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Translate All	This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a keystroke equivalent is dropped.
Character	This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplay the default Ignore (drop) in the Replacement edit control.
Replacement	The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.  For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.  The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.
List Box	The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.
Delete	This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

## Barcode – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard AIM or Symbol IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

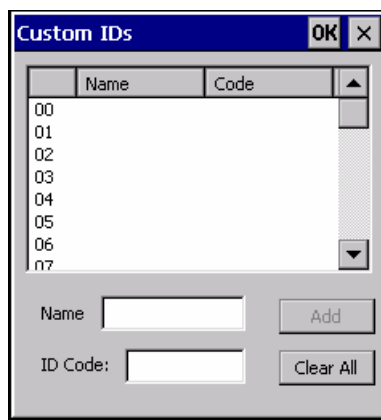
These are called “custom” Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data. The dialog below allows the custom Code IDs to be configured.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if **Enable Code ID** is set to **AIM** or **Symbol**), or to replace the list of standard code IDs (if **Enable Code ID** is set to **Custom**).

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

*Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.*

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*



**Figure 4-10 Barcode Tab / Custom Identifiers**

After adding, changing and removing items from the Custom IDs list, tap the OK button to save changes and return to the Barcode panel.

### Parameters

- Name** text box Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the **Name** and **ID Code** may have the same value. **Name** is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.
- ID Code** text box ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

### Buttons

Add	Entering data into both the Name and ID Code fields enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The <b>Add</b> button changes to <b>Insert</b> . Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The <b>Clear All</b> button changes to a <b>Remove</b> button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

### Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a barcode is converted to the text 'STX'.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	'^M'	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	'\I'	Value 0x09 in a barcode is converted to the text '^I'.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	'0x0A'	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '0x0A'	Value 0x0C is a barcode is converted to text '0x0A'

## Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	<b>Symbology</b>				
	<b>All</b>	<b>EAN-128 (I1)</b>	<b>EAN-13 (I0)</b>	<b>Intrlv 2 of 5 (IIO)</b>	<b>Code93</b>
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

<b>Barcode Symbology</b>	<b>Raw Scanner Data</b>	<b>Resulting Data</b>
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< rejected > (too short)
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< rejected > (too long)
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< rejected > (disabled)
Code-93	]G0444444	< rejected > (disabled)
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< rejected > (too short)

Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

## Length Based Barcode Stripping

Use this procedure to create symbology rules for two barcodes with the same symbology but with different discrete lengths. This procedure is not applicable for barcodes with variable lengths (falling between a maximum value and a minimum value).

### **Example 1:**

- A normal AIM or Symbol symbology role can be created for the desired barcode ID.
- Next, a custom barcode symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

### **Example 2:**

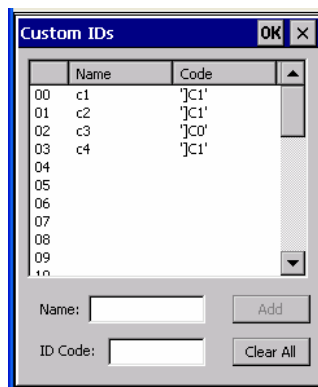
For the purposes of this example, the following sample barcode parameters will be used – EAN128 and Code128 barcodes. Some of the barcodes start with ‘00’ and some start with ‘01’. The barcodes are different lengths.

- 34 character length with first two characters = “01” (strip first 2 and last 18)
- 26 character length with first two characters = “01” (strip first 2 and last 10)
- 24 character length with first two characters = “01” (strip first 2 and last 8). This 24 character barcode is CODE128.
- 20 character length with first two characters = “00” (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN128 barcode and 0 for Code128 barcode.

- c1 = Code = ‘]C1’
- c2 = Code = ‘]C1’
- c3 = Code = ‘]C0’ (24 character barcode is CODE128)
- c4 = Code = ‘]C1’

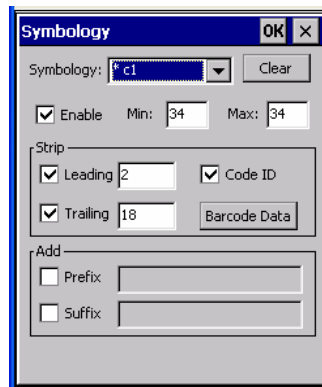


**AIM Custom IDs**

AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

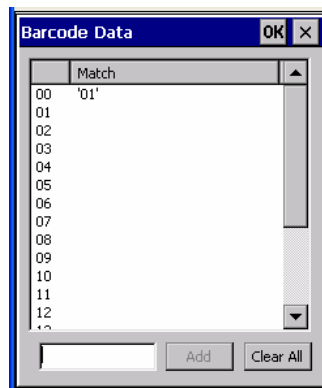
Add the AIM custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.



### AIM Custom Setup for C1

Click the Barcode Data button. Click the Add button.

Add the data for the match codes.



### Barcode Match Data for C1

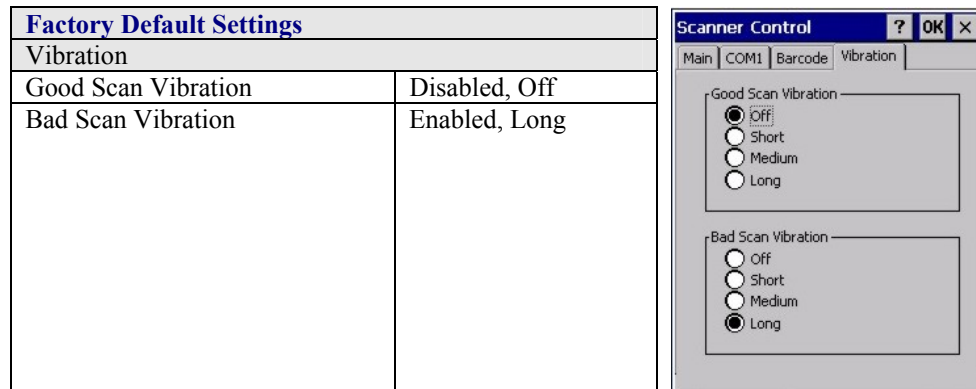
Refer to the previous section *BarcodeData Match List* for instruction.

Scan a barcode and examine the result.



## Vibration Tab

Access:  | Settings | Control Panel | Scanner | Vibration tab



**Figure 4-11 Scanner Control / Vibration tab**

Enable short, medium or long duration when a tactile response is desired on a good scan, bad scan or both event is desired. Scan sounds are accompanied by a tactile response when the internal scanner Sound parameter is enabled.

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



## Chapter 5 Wireless Network Configuration

### Introduction

(Summit 1.3.11) The MX8 mobile device has a wireless client that can be configured for no encryption, WEP encryption or WPA security, no authentication and all authentications listed below.

Certificates are necessary for many of the WPA authentications. Please refer to the *Certificates* section at the end of this chapter for more information on generating and installing certificates.

### Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys
- The Summit profile settings for Auth Type, EAP Type and Encryption depend on the security option chosen.

Wireless Security Options Supported
No Security
WEP
LEAP
EAP-FAST
PEAP-MSCHAP
WPA/LEAP
WPA-PSK
PEAP-GTC
EAP-TLS



Please refer to the *LXE Security Primer* to prepare the Authentication Server and Access Point for wireless communication. The document is available on the LXE Manuals CD and the LXE ServicePass website.



Date/Time

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

## Summit Client Configuration



Summit Client Utility Icon

*Note:* Terminology used on your screen displays may be different than those shown in the figures in this chapter. Contact your LXE representative for Summit driver updates as they become available.

Start the Summit Client configuration by tapping the Summit Client Utility icon on the desktop. You can also start the Summit Client utility by tapping **Start | Programs | Summit | SCU**.

**Important:** After adding a new profile or changing parameters of an existing profile, tap Start | Suspend. When the device Resumes, saved changes are applied.

---

## Summit Client Utility

**Access:** **Start | Programs | Summit | SCU** or **SCU Icon on Desktop** or **SCU Icon in Taskbar**



**Figure 5-1 Summit Client Utility (SCU)**

The **Main** tab provides information, the Admin Login and active config (profile) selection.

Profile specific parameters are found on the **Profile** tab. The parameters on this tab can be set to unique values for each profile.

The **Status** tab contains information on the current connection.

The **Diags** tab provides utilities to troubleshoot the client (network device).

Global parameters are found on the **Global** tab. The values for these parameters apply to all profiles.

*Note:* A password is required before making changes to Summit client profile parameters. A password is not required to switch from one profile to another.

---


## Help

Help is available by clicking the **?** button in the title bar on most SCU screens.

SCU Help may also be accessed by selecting **Start | Help** and tapping the Summit Client Utility link. The SCU does not have to be open to view the help information using this option.

---

## Summit Tray Icon


The Summit tray icon  provides access to the SCU and is a visual indicator of link status.


The Summit tray icon is displayed when:


- The Summit radio is installed and active.
- The Windows Zero Config utility is not active.
- The Tray Icon setting is On.


Tap the icon to launch the Summit Configuration Utility.


Use the tray icon to view the link status:

 Summit client is not currently associated or authenticated to an Access Point.

 The signal strength for the currently associated/authenticated Access Point is -80 dBm or weaker.

 The signal strength for the currently associated/authenticated Access Point is stronger than -80dBm but not stronger than -60 dBm.

 The signal strength for the currently associated/authenticated Access Point is stronger than -60 dBm but not stronger than -40 dBm.

 The signal strength for the currently associated/authenticated Access Point is stronger than -40 dBm.

## Main Tab

Factory Default Settings	
<b>Main</b>	
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI



**Figure 5-2 SCU – Main Tab**

The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (the radio is an 802.11 b/g radio)
- Regulatory Domain
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc).

The **Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module. See *Wireless Zero Config Utility* later in this chapter for Wireless Zero Config instruction.

The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

## [Admin Login](#)

To login to Administrator mode, tap the **Admin login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the Admin Logout button, or a navigation button (X or OK), to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.



**Figure 5-3 Main Tab – Enter Admin Password**

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap OK. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global tab.

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile tab.
- View the global parameter settings on the Global tab.
- View the current connection details on the Status tab.
- View radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags tab.

After Admin login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile tab.
- Edit global parameters on the Global tabs.
- Enable/disable the Summit tray icon in the taskbar.

## Profile Tab

*Note: Tap the **Commit** button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!*

Factory Default Settings	
Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	BG Rates Full
Auth Type	Open
EAP type	None
Encryption	None



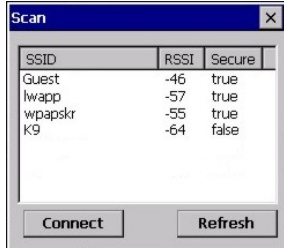
**Figure 5-4 SCU – ProfileTab**

When logged in as an Admin (see *Admin Login*), use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin.

## Buttons

Button	Function
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see <i>Profile Parameters</i> ) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.



Button	Function
Scan	<p>Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers.</p> <p>If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.</p> <div style="text-align: center;">  </div> <p><b>Figure 5-5 SCU – Scan</b></p> <p>If you are logged in as an Admin, tap an SSID in the list and tap the Connect button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as “_1” if a profile with the SSID as its name exists already).</p>
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

*Note:* *Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.*

**Important** – The settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security type chosen. Please refer to *Wireless Security* later in this Summit Client Utility section to determine the proper settings for the security type implemented on the wireless LAN.

### Profile Parameters

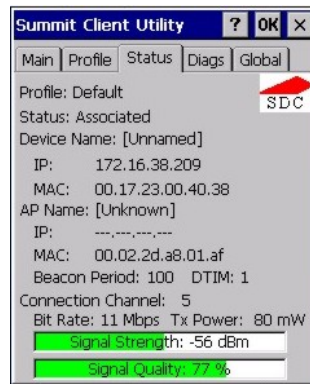
Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).

Parameter	Default	Explanation
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain.  Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device.  Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Radio Mode	BG Rates Full	Specify 802.11g and/or 802.11b when communicating with the Access Point.  Options are: B rates only, BG Rates full, G rates only, BG optimized.
Auth Type	Open	802.11 authentication type used when associating with the Access Point.  Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point.  Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, or EAP-TLS.  <i>Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.</i>
Encryption	None	Type of encryption to be used to protect transmitted data.  Options are: None, Manual WEP, Auto WEP, WPA PSK, WPA TKIP, WPA2 PSK, WPA2 AES, CCKM TKIP, CKIP Manual, CKIP Auto, Manual WEP CKIP, or Auto WEP CKIP.  <i>Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.</i>

---

## Status Tab

This screen displays information on the current profile and wireless connection. Information cannot be edited or changed on the Status panel.



**Figure 5-6 SCU – Status Tab**

The panel displays:

- Profile being used.
- The status of the network connection (down, associated, authenticated, etc.).
- The client name, IP address and MAC address.
- The name, IP address and MAC address of the Access Point maintaining the connection to the network.
- Channel currently being used for wireless traffic.
- Beacon period – The time between AP beacons in kilomicroseconds (1 kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Current transmit power in mW.
- Rate in Mbps.
- Signal strength (RSSI) and signal quality (changes with network activity). Signal quality is a measure of the clarity of the signal and is displayed as a percentage.

*Note:* After completing radio configuration, it is good practice to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

## Diags Tab

The Diags panel can be used for troubleshooting network traffic and wireless connectivity issues for the IP address shown. Admin login is required for the (Re)connect button function.



**Figure 5-7 SCU – Diags Tab**

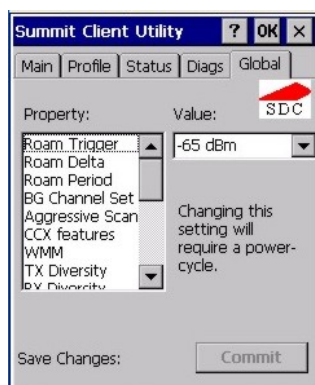
## Buttons

Button	Function
(Re)connect	Tap this button to apply, or reapply, the current config profile and attempt to associate or authenticate to the wireless LAN. Activity is logged in the Diagnostic Output text box on the lower part of the panel.
Release/Renew	Release the current IP address to obtain a new IP address. This option renews the IP address when applicable. Activity is logged in the Diagnostic Output text box. If a fixed IP address has been assigned to the wireless device, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed.
Start Ping	Tap the text box and type an IP address to Ping. Tap the Start Ping button to start pinging the IP address. The button name changes to Stop Ping. Tap Stop Ping to end the pinging process. The pinging process ends when any other button on this panel is tapped or a different menu tab is selected. Ping results are displayed in the Diagnostic Output text box.
Diagnostics	<p>Tapping this button begins an attempt to (re)connect to the wireless LAN. This option provides more data in the Diagnostics Output text box than the (Re)connect option. The data dump includes client state, profile settings, global settings, and a list of access points by SSID broadcasting in the wireless device's immediate area. The text file created, <code>_sdc_diag</code>, is placed in the Windows folder. It is overwritten when Diagnostics is run again. Not available in all releases.</p> <p>Tap the <b>Save To .... button</b> to save the Diagnostics log to a TXT file in the My Device folder (the default folder).</p>

## Global Tab

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

*Note: Tap the **Commit** button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!*



Factory Default Settings	
RX Diversity	On-Start on Main
TX Diversity	On
Roam Trigger	-65 dBm
Roam Delta	10 dBm
Roam Period	10 sec.
BG Channel Set	Full
Aggressive Scan	On
Frag Threshold	2346
RTS Threshold	2347
Ping Payload	32 bytes
Ping Timeout	5000
Ping Delay ms	1000
LED	Off
Hide Passwords	Off
Auth Timeout	8 seconds
Admin Password	SUMMIT or blank
Certs Path	System
CCX	Off
WMM	Off
Tray Icon	On

**Figure 5-8 SCU – Global Tab**

## Custom Parameter Option

LXE does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

## Global Parameters

Parameter	Default	Function
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).

Parameter	Default	Function
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	10 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	10 sec	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Parameter	Default	Function
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Hide Password	Off	If On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT or blank	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the Windows folder path currently exists before assigning the path in this parameter. See sections titled <i>Root Certificates</i> and <i>User Certificates</i> later in this chapter for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
CCX or CCX Features	Off	Use of Cisco Compatible Extensions (CCX) radio management and Access Point specified maximum transmit power features. Options are: On, Off
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off

---

Parameter	Default	Function
Auth Timeout	8 seconds	<p>Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail.</p> <p>If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed.</p> <p>If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials.</p> <p>Options are: An integer from 3 to 60.</p>

*Note:* Tap the **Commit** button to save changes. If this panel is closed before tapping the **Commit** button, changes are not saved!



## Summit Wireless Security

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameter settings than are listed in these instructions. Please see your System Administrator for complete information about your network and its wireless security requirements.

Default profile	LXE recommends editing the Default profile instead of creating new profiles. <b>Important:</b> Perform a Warm boot (using the Suspend/Resume key sequence) after changing parameters to save the changed parameters in the registry.
Switching profiles	Successfully connecting after switching from one profile to another may take up to 30 seconds from the moment the “Is not authenticated” or “Is not Associated” messages are displayed.
Adding, changing or renaming profiles	LXE recommends performing a Warm boot function (using the Suspend/Resume key sequence) after tapping the Commit button.

*Note:* The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the Config tab. The reminder feature may not be present in all versions. Contact your LXE representative for version upgrades.

### Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers two choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the mobile device can access the network.
- The Username and Password are left blank on the Credentials screen. When the mobile device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

*Note:* It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

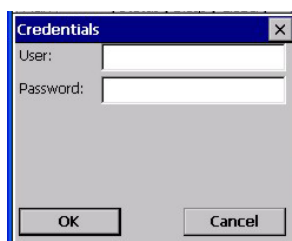
#### How to: Use Stored Credentials

1. After completing the other entries in the profile, tap the the Credentials button.
2. Enter the Username and Password on the Credentials screen and tap the OK button.
3. Tap the Commit button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
6. For EAP-TLS, also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the Validate server and Use MS store checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
10. If using EAP-FAST and manual PAC provisioning, input the PAC filename and password.
11. Tap the OK button then the Commit button.
12. Verify the device is authenticated by reviewing the Status tab. When the device is properly configured, the Status tab indicates the device is Authenticated and the method used.

*Note: More details are provided in the appropriate Summit Wireless Security section following in this chapter. If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.*

#### How to: Use Sign On Screen

1. After completing the other entries in the profile, tap the Credentials button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or WPA/LEAP.
2. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
3. For EAP-TLS, also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the Validate server and Use MS store checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
7. Tap the OK button then the Commit button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Tap the OK button.



**Figure 5-9 Sign-On Screen**

Verify the device is authenticated by reviewing the **Status** tab. When the device is properly configured, the Status tab indicates the device is Authenticated and the method used.

The sign-on screen is displayed after a reboot for each of the listed protocols.

*Note: Complete details are provided in the appropriate Summit Wireless Security section following in this chapter.*

*If a user enters invalid credentials and taps **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.*

*If the user taps the **Cancel** button, the device does not associate. The user is not prompted again for credentials until the device is rebooted, the radio is disabled then enabled, the **Reconnect** button on the Diags tag is tapped or the profile is modified and the **Commit** button is tapped.*

## Windows Certificate Store vs. Certs Path

*Note: It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

### User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store. To generate the user certificate, follow the instructions in *Generating a User Certificate for the Mobile Device*, later in this chapter.

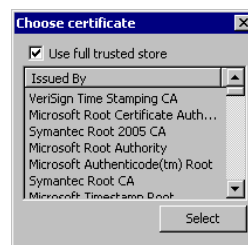
Import the user certificate into the Windows certificate store by following the instructions in *Installing a User Certificate on the Mobile Device*, later in this chapter. A Root CA certificate is also needed for EAP-TLS. Refer to the section below.

### Root CA Certificates

Root CA certificates are required for PEAP/MSCHAP, PEAP/GTC, and EAP-TLS. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

#### How To: Use Windows Certificate Store

1. Follow the instructions later in this chapter for *Downloading a Root CA Certificate* to a PC.
2. To import the certificate into the Windows store, follow the instructions for *Installing a Root CA Certificate on the Mobile Device* later in this chapter.
3. When completing the Credentials screen for the desired authentication, be sure to check the Use MS store checkbox after checking the Validate server checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to Step #8.
5. Otherwise, to select a specific certificate tap the Browse (...) button.



**Figure 5-10 Choose Certificate**

6. Uncheck the Use full trusted store checkbox.
7. Select the desired certificate and tap the Select button to return the selected certificate to the CA Cert textbox.
8. Tap OK to exit the Credentials screen and then Commit to save the profile changes.

#### How To: Use the Certs Path

1. Follow the instructions later in this chapter for *Downloading a Root CA Certificate* to a PC.
2. Copy the certificate to the specified Windows folder on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after warmboot.

3. When completing the Credentials screen for the desired authentication, do not check the Use MS store checkbox after checking the Validate server checkbox.
4. Enter the certificate name in the CA Cert textbox.
5. Tap OK to exit the Credentials screen and then Commit to save the profile changes.

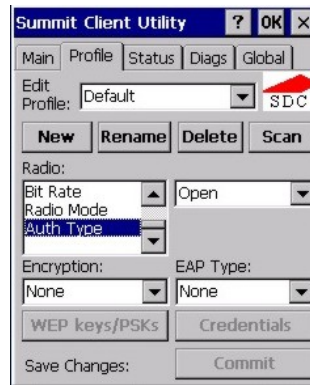
---

## No Security

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-11 Configure a Summit Profile with No Security**

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to None.

Tap the **Commit** button to save the new profile configuration.

Perform a **Suspend/Resume** function to connect using the new profile configuration.

*Note: LXE recommends performing a Suspend/Resume function each time the Commit button is tapped.*

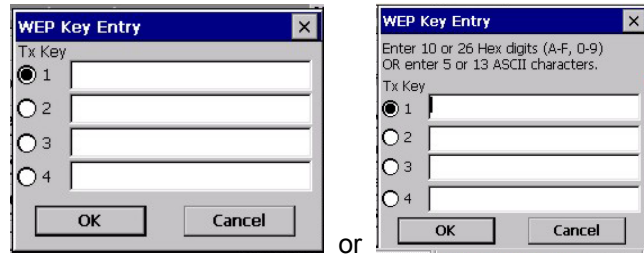
## WEP Keys

Please see your System Administrator for complete information about your network WEP key requirements.

To connect using WEP, use the following minimum required profile options..

- Auth Type = Open
- EAP Type = None
- Encryption = Manual WEP

Tap the **WEP keys/PSK Keys** button. The WEP Key Entry text entry box appears.



**Figure 5-12 Summit WEP Keys**

Enter the **WEP key**. If there are more than one set of keys, tap the radio button in front of the Key to be used.

WEP keys may be entered in Hex or ASCII format. For previous versions of the SCU, if the WEP key entry does not offer a choice between Hex and ASCII, the key must be in Hex (refer to the Hex Key Format segment that follows).

Once configured, tap **OK** then tap the **Commit** button. Ensure the correct Active Config is selected on the Main tab and warm boot. The SCU Main tab shows the device is associated after the radio connects to the network.

### Hex Key Format

Valid keys are 10 (for 40 bit encryption) or 26 (for 128 bit encryption) hexadecimal characters (0-9, A-F). Enter the key(s) and tap **OK**.

### ASCII Key Format

Valid keys are 5 (for 40 bit encryption) or 13 (for 128 bit encryption) alphanumeric characters. Enter the key(s) and tap **OK**.

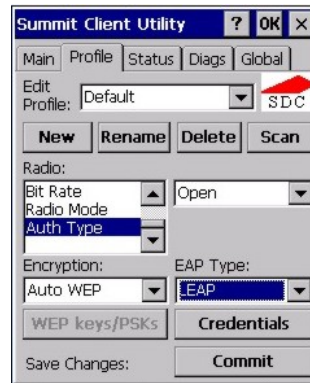
## LEAP w/o WPA Authentication

If the Cisco/CCX certified Access Point (AP) is configured for open authentication, set the Auth Type client parameter to **Open**.

If the AP is configured for network EAP only, set the Auth Type client parameter to **LEAP**.

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK. Tap the **Profile** tab.



**Figure 5-13 Configure a Summit Profile for LEAP w/o WPA**

Enter the **SSID** of the Access Point assigned to this profile.

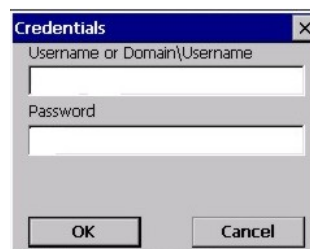
Set **Auth Type** to Open.

Set **EAP Type** to LEAP.

Set **Encryption** to Auto WEP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



**Figure 5-14 LEAP Credentials Dialog**

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired.

Enter the **Password**, if desired. Tap **OK**.

Tap the **Commit** button to save the new profile configuration. Perform a **warm boot** to connect using the new profile configuration.

See Also: *WPA/LEAP Authentication* later in this section to configure the client for WPA LEAP.

See Also: *Sign-on vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

## EAP-FAST Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-15 Configure a Summit Profile for EAP-FAST**

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to EAP-FAST.

Set **Encryption** to WPA TKIP.

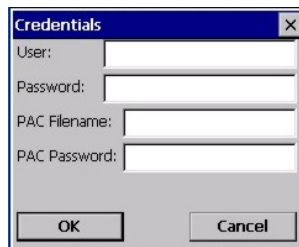
To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server.

The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the client device. Please refer to the *LXE Security Primer* for more information on the RADIUS server configuration.

To use Stored Credentials, tap the **Credentials** button.



**Figure 5-16 Summit EAP-FAST Credentials**

Enter the **Username** in the Credentials popup text entry box, if desired.

Enter the **Password**, if desired. Tap **OK**.

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the mobile device. The same username/password must be used to authenticate each time. When using automatic PAC provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

For manual PAC provisioning, the PAC filename and password must be entered. The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be Read Only.

Tap OK then tap Commit to save the new profile configuration. Ensure the correct Active Profile is selected on the Main tab and perform a warmboot (or Suspend/Resume) function.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

## PEAP/MSCHAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-17 Configure a Summit Profile for PEAP/MSCHAP**

Enter the **SSID** of the Access Point assigned to this profile. Set **Auth Type** to Open. Set **EAP Type** to PEAP-MSCHAP.

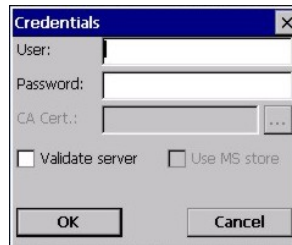
Set **Encryption** to WPA TKIP.



To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

Enter the **Username** or Domain\Username in the Credentials popup text entry box, if desired. Enter the **Password**, if desired. Leave the CA Certificate Filename blank for now. Tap **OK**. Tap **Commit**.



**Figure 5-18 PEAP/MSCHAP Credentials**

*Note:* The date must be properly set on the device to authenticate a certificate.

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [ . . . ] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit**.

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

## WPA/LEAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-19 Configure a Summit Profile with LEAP for WPA TKIP**

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open. Set **EAP Type** to LEAP. Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



**Figure 5-20 LEAP Credentials**

Enter the **Username** in the Credentials popup text entry box, if desired. Enter the **Password**, if desired. Tap **OK**.

Tap the **Commit** button to save the new profile configuration.

Perform a **warm boot** (or Suspend/Resume) to connect using the new profile configuration.

See Also: *LEAP w/o WPA* earlier in this section to configure the client for LEAP without WPA.

See Also: *Sign-on vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

## WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-21 Configure a Summit Profile with WPA PSK Encryption**

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to WPA PSK.

Tap the **WEP keys/PSK Keys** button.



**Figure 5-22 Summit PSK Entry Dialog**

Enter the Passphrase in the **PSK Entry** popup text entry box. This value can be a 64 hex character or an 8-63 byte ASCII value. Tap **OK**

Tap the **Commit** button to save the new profile configuration.

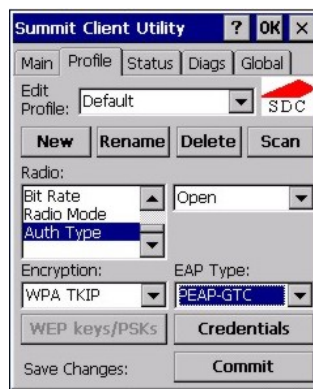
Perform a **warm boot** (or Suspend/Resume) to connect using the new profile configuration.

## PEAP/GTC Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-23 Configure a Summit Profile with PEAP/GTC**

Enter the **SSID** of the Access Point assigned to this profile.

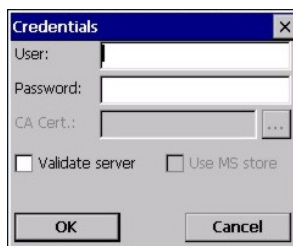
Set **Auth Type** to Open.

Set **EAP Type** to PEAP-GTC.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



**Figure 5-24 PEAP/GTC Credentials**

*Note:* The date must be properly set on the device to authenticate a certificate.

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [ . . . ] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit**.

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

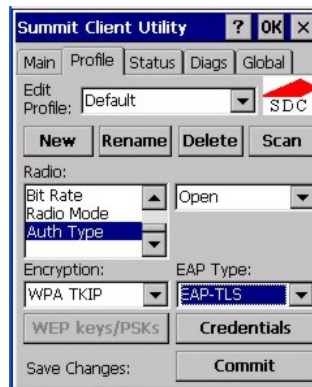
---

## EAP-TLS Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Profile** tab.



**Figure 5-25 Configure a Summit Profile with EAP-TLS**

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

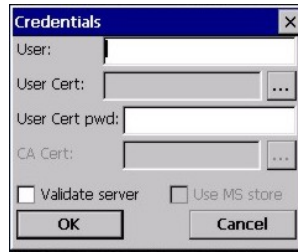
Set **EAP Type** to EAP-TLS.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network. If the username and password are left blank during setup, see *Sign-On vs. Stored Credentials* earlier in this chapter.

*Note:* The date must be properly set on the device to authenticate a certificate.



**Figure 5-26 EAP-TLS Credentials Dialog**

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [ . . . ] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit**.

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using EAP-TLS for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

---

## Wireless Zero Config Utility and the Summit Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the Wireless Zero Config application is enabled and the MX8 is not connected to a network.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network.



***LXE recommends using the Summit Client Utility to manage wireless connectivity.***

To use Wireless Zero Config, first open the Summit Client Utility.

1. Select ThirdPartyConfig in the Active Profile drop down box.
2. A message appears that a Power Cycle is required to make settings activate properly.
3. Tap OK.
4. Tap the Power button to place the MX8 in Suspend, then tap the Power button to wake the MX8 from Suspend mode.

The Wireless Zero Config utility begins.

## Certificates

	Please refer to the <i>LXE Security Primer</i> to prepare the Authentication Server and Access Point for communication.
 Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

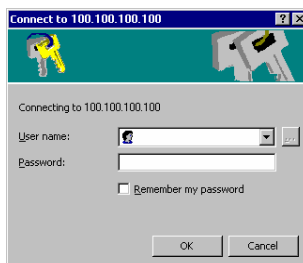
## Root Certificates

### Download a Root CA Certificate

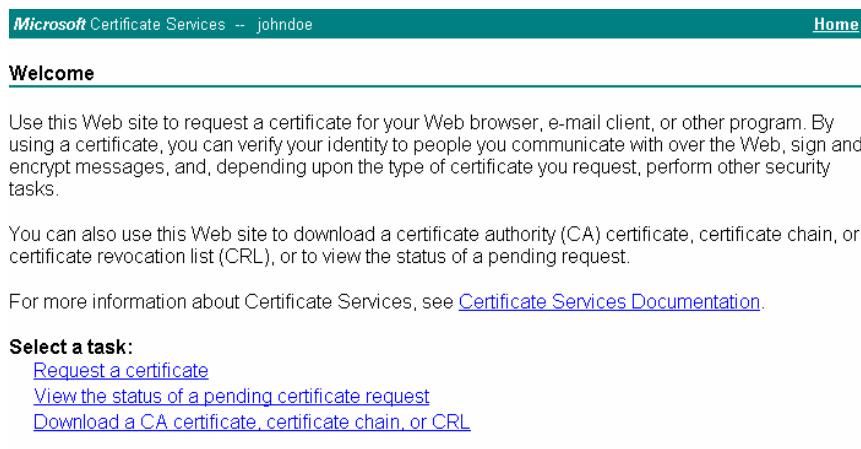
The easiest way to get the root CA certificate is to **use a browser on a desktop PC** to navigate to the CA (Certificate Authority). To request the root CA certificate, **open a browser to**

`http://<CA IP address>/certsrv`

Sign into the CA with any valid username and password.



**Figure 5-27 Logon to Certificate Authority**

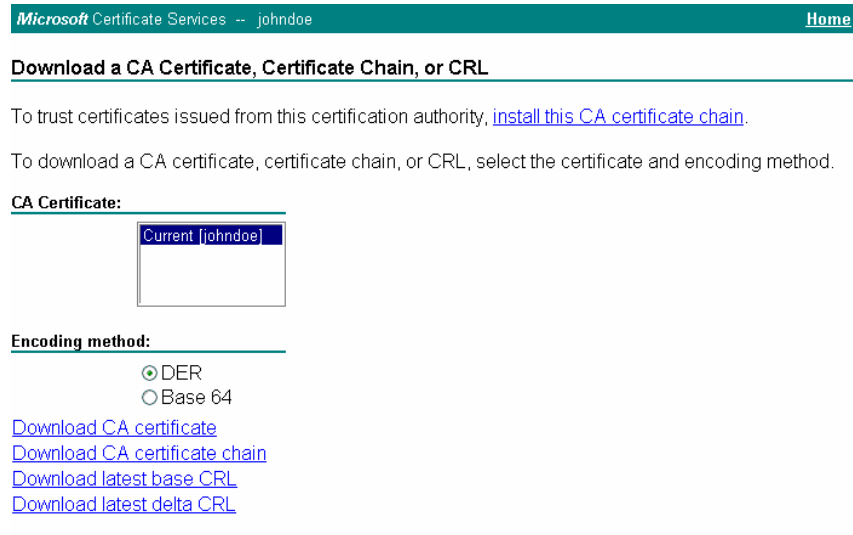


**Figure 5-28 Certificate Services Welcome Screen**

Tap the **Download a CA certificate, certificate chain or CRL** task link.



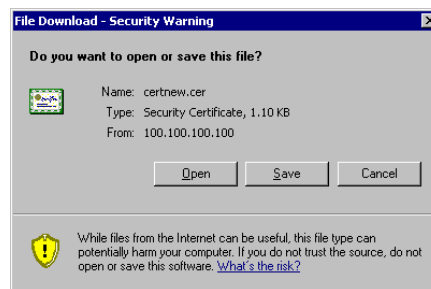
Make sure the correct root **CA certificate** is selected in the list box.



**Figure 5-29 Download CA Certificate Screen**

Tap the **DER** button.

To download the CA certificate, tap on the **Download CA certificate** link.

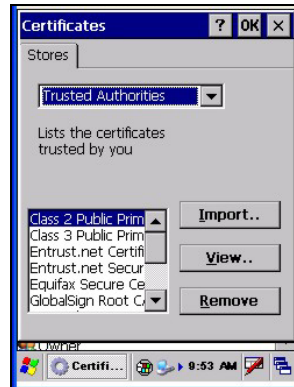


**Figure 5-30 Download CA Certificate Save to Desktop**

Tap the **Save** button and save the certificate to the desktop PC. Keep track of the name and location of the certificate as the certificate file name and file location is required in later steps.

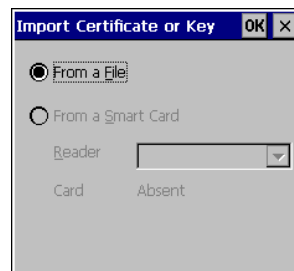
## Installing a Root CA Certificate on the Mobile Device

Copy the certificate file from the desktop PC to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.



**Figure 5-31 Certificate Stores**

Tap the **Import** button.



**Figure 5-32 Import Certificate From a File**

Make sure **From a File** is selected and tap OK.



**Figure 5-33 Browsing to Certificate Location**

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

Tap **OK** to import the certificate.

Once the certificate is installed, return to the proper authentication section, described later in this chapter.

## User Certificates

### Generating a User Certificate for the MX8

The easiest way to get the user certificate is to **use a browser on a PC** to navigate to the CA. To request the user certificate, open a browser to

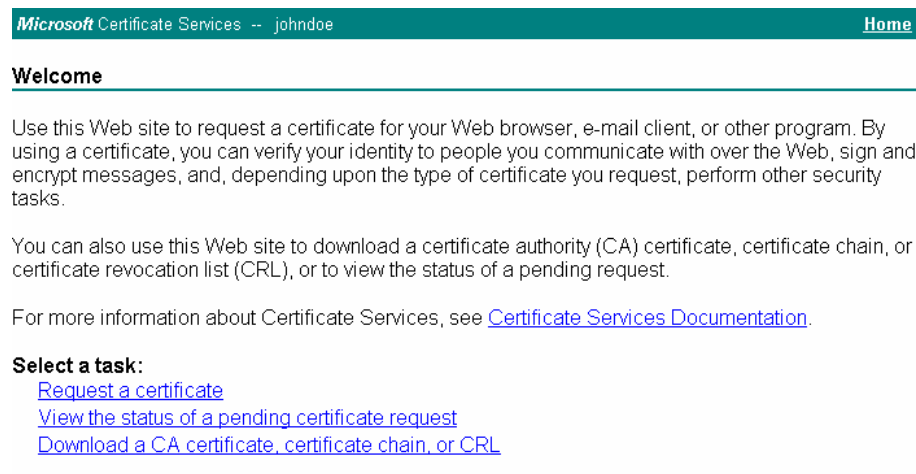
`http://<CA IP address>/certsrv`

Sign into the CA with the username of the user certificate required.



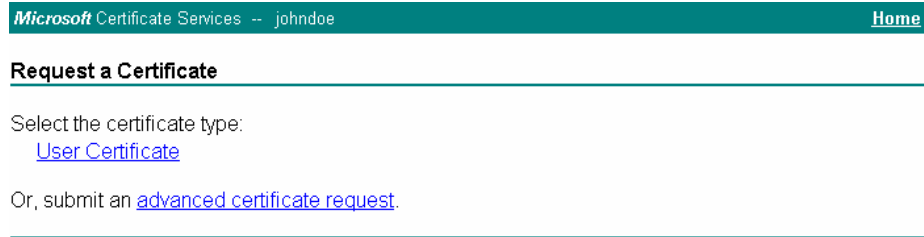
**Figure 5-34 Logon to Certificate Authority**

This process saves a user certificate and a separate private key file. Windows CE devices such as the MX8 require the private key to be saved as a separate file rather than including the private key in the user certificate.



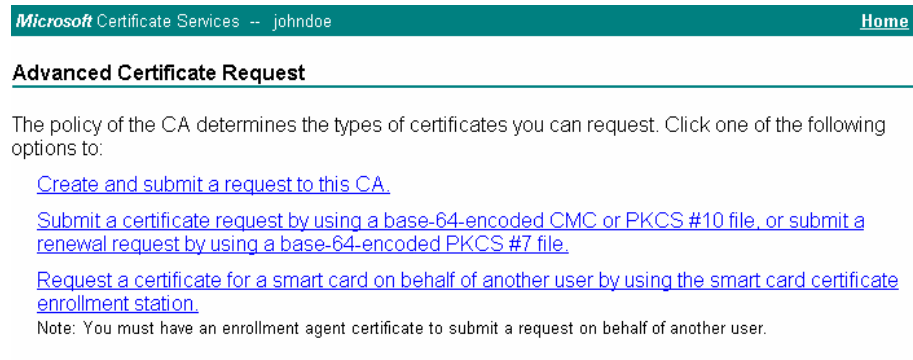
**Figure 5-35 Certificate Services Welcome Screen**

Tap the **Request a certificate** task link.



**Figure 5-36 Request a Certificate Type**

Tap on the **advanced certificate request** link.



**Figure 5-37 Advanced Certificate Request Screen**

Tap on the **Create and submit a request to this CA** link.

Microsoft Certificate Services -- johndoe [Home](#)

### Advanced Certificate Request

---

**Certificate Template:**

User

**Key Options:**

Create new key set    Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage:  Exchange

Key Size: 1024   Min: 384   Max: 16384   (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name    User specified key container name

Mark keys as exportable

Export keys to file

Full path name: user1key.pvk

Enable strong private key protection

Store certificate in the local computer certificate store  
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Additional Options:**

Request Format:  CMC    PKCS10

Hash Algorithm: SHA-1  
*Only used to sign request.*

Save request to a file

Attributes:

Friendly Name:

**Figure 5-38 Advanced Certificate Details**

For the Certificate Template, select **User**.

Check the **Mark keys as exportable** and the **Export keys to file** checkboxes.

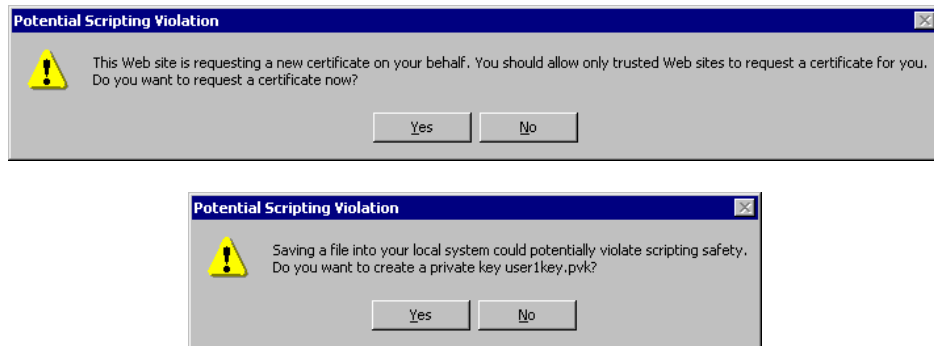
Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.



Be sure to note the name used for the private key file, for example MX8USER.PVK. The certificate file created later in this process must be given the same name, for example, MX8USER.CER.

*DO NOT* check “Enable strong private key protection”.

Make any other desired changes and tap the **Submit** button.



**Figure 5-39 Script Warnings**

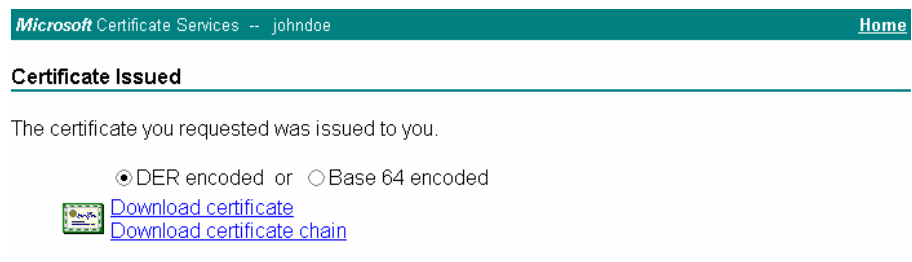
If any script notifications occur, tap the **Yes** button to continue the certificate request.



**Figure 5-40 Script Warnings**

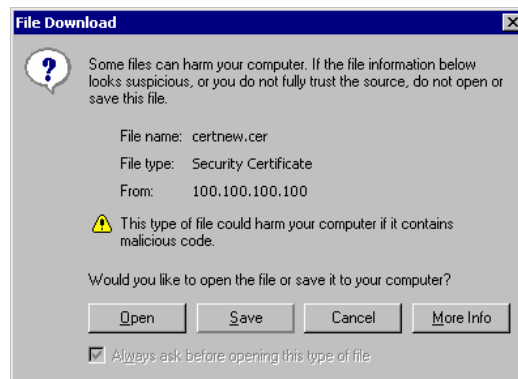
When prompted for the private key password:

- Tap **None** if you do not wish to use a password, *or*
- Enter and confirm your desired password then tap **OK**.



**Figure 5-41 User Certificate Issued**

Tap the **Download certificate** link.



**Figure 5-42 Download Certificate Security Warning**

Tap **Save** to download and store the user certificate **to the PC**. Keep track of the name and location of the certificate as the file name and location is required in later steps. The private key file is also downloaded and saved during this process.



Be sure to use the same name for the certificate file as was used for the private key file. For example, if the private key was saved as MX8USER.PVK then the certificate file created must be given the same name, for example, MX8USER.CER.



### Installing a User Certificate on the MX8 (WPA-TLS Only)

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

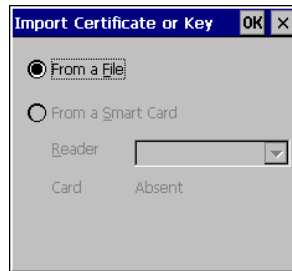


Select **My Certificates** from the pull down list.



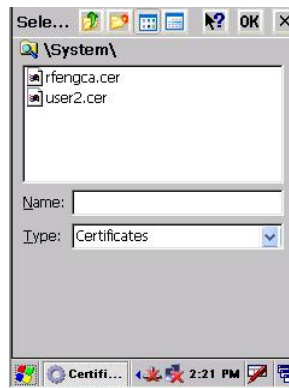
**Figure 5-43 My Certificates Stores**

Tap the **Import** button.



**Figure 5-44 Import User Certificate**

Make sure **From a File** is selected and tap OK.



**Figure 5-45 Browsing to Certificate Location**

Using the explorer buttons, browse to the location on the mobile device where you copied the certificate, select the certificate desired and tap OK.

Tap **Yes** to import the certificate. The certificate is now shown in the list.

Highlight the certificate you just imported and tap the **View. .** button.

From the Field pull down menu, select **Private Key**.

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen.

Tap **import**.



**Figure 5-46 Browsing to Private Key Location**

Using the explorer buttons, browse to the location where you copied the private key file, change the **Type** pull down list to **Private Keys**, select the certificate desired and tap **OK**.

Tap on **View** to see the certificate details again.

The private key should now say "Present". If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example MX8USER.CER for the certificate and MX8USER.PVK for the private key file. If the file names are not the same, rename the private key file and import it again.



## Chapter 6 AppLock

### Introduction

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

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

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

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified application is automatically launched and runs in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold boot, the Administrator may need to reconfigure the AppLock parameters.

*Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.*

AppLock is updated periodically as new options become available. Contact your LXE representative for assistance, downloads and update availability.

## Setup a New Device

Prerequisites:

- The touch panel must be enabled. Refer to the (*Start | Settings | Control Panel | Handheld | Misc |* ) Touch Panel Disabled setting.
- An MX8 default input method (Input Panel, Transcriber, or custom input method) is assigned.

LXE CE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

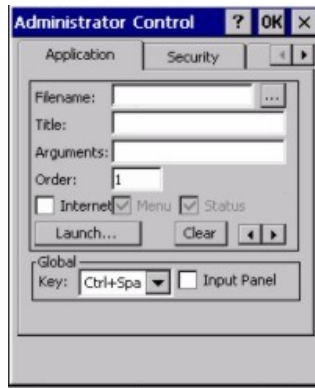
Briefly, the process to configure a new device is as follows:

1. Insert a fully charged battery and press the Power button. See Chapter 1 – Introduction for instruction.
2. Connect an external power source to the device (if required). See Chapter 1 – Introduction for instruction.
3. Adjust screen display, audio volume and other parameters if desired. Install accessories (e.g. handstrap, stylus). See Chapter 1 – Introduction for instruction.
4. Tap Start | Settings | Control Panel | Administration icon.
5. Assign a Switch Key (hotkey) sequence for AppLock. See Security Panel.
6. Assign an application on the Application tab screen. More than one application can be assigned. See Application Panel.
7. Assign a password on the Security tab screen. See Security Panel.
8. Select a view level on the Status tab screen, if desired. See Status Panel.
9. Tap OK.
10. Press the Switch Key sequence to launch AppLock and lock the configured application(s).

The device is now in end-user mode.

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

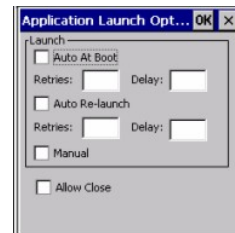
*Note:* AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.



Application Panel



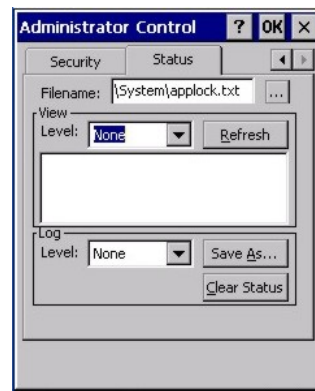
End User Switchpad



Application – Launch Panel



Security Panel



Status Panel

Figure 6-1 AppLock Panels

## 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:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application, or applications, to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	Shift+Ctrl+A
Password	none
Application path and name	none
Application command line	none

## End User Mode

End-user mode locks the end-user into the configured application (or applications). 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 key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE 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 taps 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.



## Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three attempts) 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:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- 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.

---

## AppLock Password Troubleshooting

Can't locate the password that has been set by the administrator? Enter this LXE back door key sequence:

Ctrl+L Ctrl+X Ctrl+E

## End-User Switching Technique

*Note:* The touch screen must be enabled. Refer to Start | Settings | Control Panel | Handheld | Misc | Touch Panel Disabled setting.



**Figure 6-2 Switchpad Menu**

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX8 default input method (Input Panel, Transcriber, or custom input method) is activated.

---

## Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the taskbar. The taskbar is always visible on top of the application in focus. *Note:* If only one application is configured and the Input Panel is not enabled, the Switchpad icon is not displayed.

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

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

See Also: *Application Panel | Launch | Manual (Launch) and Allow Close*

---

## Using the Switch Key Sequence

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

See Also: *Application Panel | Global Key*

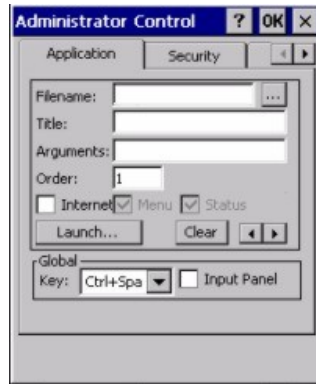
## Multi-Application Configuration

Access:  | Settings | Control Panel | Administration icon

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

*Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.*

## Application Panel



**Figure 6-3 Application Panel**

Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

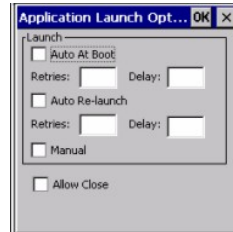
Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the application switcher panel.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.

Option	Explanation
Launch Button	<p>See following section titled Launch Button.</p> <p><i>Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.</i></p>
Global Key	<p>Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.</p>
Global Delay	<p>Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot.</p> <p><i>Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.</i></p>
Input Panel	<p>Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.</p>
Clear Button	<p>Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.</p>
Scroll Buttons	<p>Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.</p>

---

## Launch Button

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



**Figure 6-4 Application Launch Options**

*Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.*

## Auto At Boot

Default is Enabled. Auto At Boot, when enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 (no delay) and a maximum of 999 seconds.

Auto At Boot Retries is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Auto At Boot Delay timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

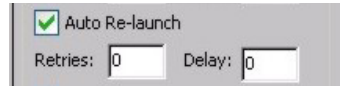
The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

*Note: A Global Delay can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.*

*Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.*

### Auto Re-Launch

Default is Enabled. Auto Re-Launch, when enabled for a specific application, automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.



*Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.*

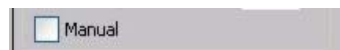
Auto Re-Launch Retries default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Auto Re-Launch Delay timer default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

### Manual (Launch)

Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.



Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

### Allow Close

Default is Disabled. When enabled, the associated application can be closed by the end-user.



This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

### End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

## Security Panel



**Figure 6-5 Security Panel**

### Setting an Activation 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 2<sup>nd</sup> key keypress is an invalid keypress for a hotkey sequence.

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. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the <Ctrl> key is pressed followed by <A>, Ctrl+A is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch user modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

### Setting a Password in the Security Panel

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

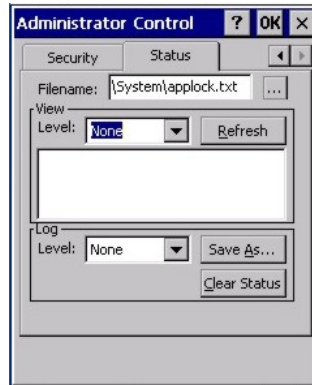
See Also: Passwords and Troubleshooting Multi-Application AppLock



## Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



**Figure 6-6 Status Panel**

Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

## View

The default is None.

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.

## Log

*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 'None'; 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 (default)
- 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.

---

## Troubleshooting AppLock

### The mobile device won't switch from Administration mode to end-user mode.

If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

### The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

## Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter..." is logged at the beginning of the function specified in the message and "Exit..." is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
*****	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete applock.exe from the \Windows directory and reboot the unit. Deleting applock.exe in this manner triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
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

<b>Message</b>	<b>Explanation and/or corrective action</b>	<b>Level</b>
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
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING

<b>Message</b>	<b>Explanation and/or corrective action</b>	<b>Level</b>
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
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

<b>Message</b>	<b>Explanation and/or corrective action</b>	<b>Level</b>
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
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

<b>Message</b>	<b>Explanation and/or corrective action</b>	<b>Level</b>
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
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



Message	Explanation and/or corrective action	Level
Registry read failure at reenter user mode	The registry has to be read when entering user mode if the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. If the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
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

Message	Explanation and/or corrective action	Level
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
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

Message	Explanation and/or corrective action	Level
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

## AppLock Registry Settings

This system application runs at startup via the *launch* feature of LXE Windows CE devices. When the launch feature is installed on the mobile device, the following registry settings are created. The launch feature registry settings are embedded in the mobile device OS image:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Filename=AppLock.exe
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Installed=
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\FileCheck=
```

AppLock registry settings identify the application that is going to be locked and any parameters that are needed by the application. These registry settings are as follows:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Administration\\AppName
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppCommandLine=
```

In addition to the registry settings needed to specify the application, additional registry settings are needed to store the configuration options for AppLock. These options include, among others, the administrator's password and hotkey.

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\HotKey=
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\EP=
```



## Appendix A Key Maps

### Introduction

#### Remember :

“Sticky” keys are also known as “second” function keys.

**Ctl/Ctrl, Alt, Shft, Blue and Orange keys are “sticky keys”. Sticky keys do not need to be held down before pressing the next (or desired) key. It is valid to use combined modifiers on specific keys.**

*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.*

### 32-Key Numeric-Alpha Keypad

When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shft sticky key or the Caps key sequence (Blue+Tab) for upper case alphabetic characters.

Pressing the Alph key forces “Alpha” mode for the 2,3,4,5,6,7,8, and 9 keys. The 1 and 0 keys continue to place a 1 and 0 into the text field.

To create a combination of numbers and letters before pressing Enter, remember to tap the Alph key to toggle between Alpha and Numeric mode.

When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.

To Get This MX8 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
Power / Suspend							Power 3
Field Exit (default VK_PAUSE)	MAP				MAP		Diamond#1 MAP=Mappable
= or (	x	x			MAP		Diamond#2 Default is MAP MAP=Mappable
! or )	x	x			MAP		Diamond#3 Default is MAP MAP=Mappable
Volume Adjust Mode		x					Scan Key 4
Display Backlight Brightness Adjust Mode	x						Scan Key 5
Toggle Blue Mode							Blue
Toggle Orange Mode							Orange
Toggle Shift Mode							Shft

<sup>3</sup> Tapping the Power key when in any sticky mode (Blue, Orange, Shift, etc) either turns the device On (when Off) or places it in Suspend (when active).

<sup>4</sup> Orange+Scan enters Volume Adjust Mode. Use Up Arrow and Down Arrow to adjust volume. Press any other key but Up Arrow or Down Arrow to exit Adjust Mode.

<sup>5</sup> Blue+Scan enters Backlight Brightness Adjust Mode. Use the Up Arrow and Down Arrow to adjust brightness. Press any other key but Up Arrow or Down Arrow to exit Adjust Mode.

To Get This MX8 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctrl	Alt	Shft	Alpha	
Toggle Alpha Mode							Alph
Alt Mode							Alt
Control Mode							Ctrl
Scan Mode							Scan Key
Esc	x						Alt
Space							Spc
Enter							Enter
CapsLock (Toggle)	x						Tab
Back Space		x					Spc
Tab							Tab
BackTab		x					Tab
Up Arrow							Up Arrow
Down Arrow							Down Arrow
Right Arrow	x						Up Arrow
Left Arrow	x						Down Arrow
Insert		x					Ctrl
Delete							Del
Home					x		Down Arrow
End					x		Up Arrow
Page Up		x					Up Arrow
Page Down		x					Down Arrow
F1							F1
F2							F2
F3							F3
F4							F4
F5							F5
F6		x					F1
F7		x					F2
F8		x					F3
F9		x					F4
F10		x					F5
F11	x						F1
F12	x						F2
F13	x						F3
F14	x						F4
F15	x						F5
F16					x		F1
F17					x		F2
F18					x		F3
F19					x		F4
F20					x		F5
F21		x			x		F1

To Get This MX8 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
F22		x			x		F2
F23		x			x		F3
F24		x			x		F4
a						x	2
b						x	22
c						x	222
d						x	3
e						x	33
f						x	333
g						x	4
h						x	44
i						x	444
j						x	5
k						x	55
l						x	555
m						x	6
n						x	66
o						x	666
p						x	7
q						x	77
r						x	777
s						x	7777
t						x	8
u						x	88
v						x	888
w						x	9
x						x	99
y						x	999
z						x	9999
A					x	x	2
B					x	x	22
C					x	x	222
D					x	x	3
E					x	x	33
F					x	x	333
G					x	x	4
H					x	x	44
I					x	x	444
J					x	x	5
K					x	x	55
L					x	x	555
M					x	x	6

To Get This MX8 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
N					x	x	66
O					x	x	666
P					x	x	7
Q					x	x	77
R					x	x	777
S					x	x	7777
T					x	x	8
U					x	x	88
V					x	x	888
W					x	x	9
X					x	x	99
Y					x	x	999
Z					x	x	9999
1							1
2							2
3							3
4							4
5							5
6							6
7							7
8							8
9							9
0							0
. (period)		x					DEL
<	x						7
[	x	x					2 or 2
]	x	x					3 or 3
>	x						8
=		x					Diamond#2
{	x						4
}	x						5
/	x						1
-	x						Spc
+	x						Del
* (asterisk)		x			x		8 or Diamond#1
: (colon)		x					0
; (semicolon)	x						0



To Get This MX8 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
. (period)		x					Del
?		x					8
` (accent)	x						6
_ (underscore)		x					7
, (comma)		x					6
' (apostrophe)		x					Alph
~ (tilde)	x						9
\		x					1
		x					Alt
“	x						Alph
!		x			x		Diamond#3 or 1
@		x			x		2 or 5
#		x			x		3 or 4
\$		x			x		9 or 4
%					x		5
^	x				x		6 or Ctrl
&					x		7
(	x				x		Diamond#2 or 9
)	x				x		Diamond#3 or 0 (zero)

## Creating Custom Key Maps

Prerequisite: LXE MX8 SDK CD [MX8A505CE50SDK]

### Introduction

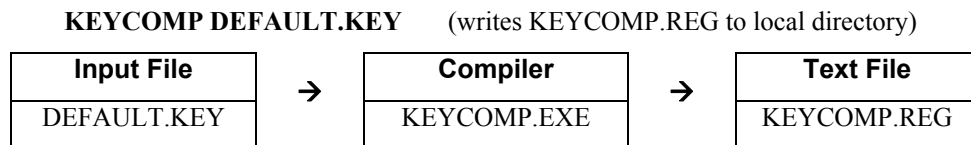
A command-line compiler called KEYCOMP.EXE is provided on the MX8 SDK CD. Using this compiler, the System Administrator can convert a sample default key map text file into a custom key map text file which, when loaded onto the mobile device, can be chosen by the user to replace the default mobile device keymap and then switched back when they are finished using the customized keys.

**IMPORTANT – The keycomp utility included with the MX8 SDK is not the same as the one included with the MX3X SDK. This one only generates maps for the MX8.**

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 can use either hex or decimal, but the desktop one used over ActiveSync that a developer may use requires hex.*

Example:



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; as cold booting returns 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 **Default** 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.

---

## Keymap Source Format

The source file **DEFAULT.KEY** is supplied with the keymap compiler. This is the commented source for the default keymap **Default**. 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.

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 **Default** 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]
MAPDESC=Default
MAPNAME=00000409
MAPCNT=5
MAPCOLS=10
MAPROWS=8
ALGOR=MX8
```

MAPDESC	Name of this map. This is what appears in the popup menu in the keyboard control panel.
MAPNAME	ID code of this map, for use with the internal Win32 APIs (which require a numeric value).
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 MX8 [ MX8 is $\text{scancode} = ((\text{column} \ll 3) + \text{row})$ ]

*Note:* The field MAPDESC needs to be unique, but MAPNAME does not.

---

### SPECIAL Section

Not applicable to MX8. Retained in .key file for compiler compatibility.

```
.
[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_NORMAL32
;;;;;;;;;;;;;
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_NORMAL32	(MX8 only) no modifiers, 32-key map
MAP_ORANGE32	(MX8 only) orange modifier, 32-key map
MAP_BLUE32	(MX8 only) blue modifier, 32-key map
MAP_SHIFT32	(MX8 only) shift modifier, 32-key map
MAP_ORANGESHIFT	(MX8 only) shift-orange modifier, 32-key map

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 <b>(not on MX8)</b>
MAP_CONTR (or) MAP_CONTRAST	special keymap for contrast adjustment <b>(not on MX8)</b>
MAP_BRITE (or) MAP_BRIGHT	special keymap for brightness adjustment <b>(not on MX8)</b>

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','l','@',' ', 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
KY_ALPHA	Alpha mode key

Note that specifying the power button in a different location will affect suspend/resume functions.

---

## 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 value is valid: SCAN1.

**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 than 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 MX8 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 8-digits all numerics

```



```

;;-----
[General]
MAPDESC=Default
MAPNAME=00000409
MAPCNT=13
MAPCOLS=5
MAPROWS=16
ALGOR=NA

;;-----
;; ...Not used for MX8
;; ...included in the MX8 map for compatibility
;;   with other compiler...
;; 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 unmodified keys on the MX8
;; 32-key keypad
;;-----
[Map]
MAP=MAP_NORMAL32
;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_F3
COL0ROW1=VK_F2
COL0ROW2=VK_F1
COL0ROW3=VK_DOWN
COL0ROW4=VK_TAB
COL0ROW5=open
COL0ROW6=open
COL0ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=ACTION+SCAN1
COL1ROW3=KY_BLUE
COL1ROW4=VK_RETURN
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=VK_F4
COL2ROW1=VK_F5
COL2ROW2=KY_PROG1
COL2ROW3=VK_UP
COL2ROW4=VK_SHIFT
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open

```

```

;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;
COL4ROW0=' 1 '
COL4ROW1=' 4 '
COL4ROW2=' 7 '
COL4ROW3=VK_MENU
COL4ROW4=KY_PROG2
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_CONTROL
;;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;
COL6ROW0=' 2 '
COL6ROW1=' 5 '
COL6ROW2=' 8 '
COL6ROW3=' 0 '
COL6ROW4=KY_PROG3
COL6ROW5=open
COL6ROW6=open
COL6ROW7=ACTION+KY_ALPHA
;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;
COL8ROW0=' 3 '
COL8ROW1=' 6 '
COL8ROW2=' 9 '
COL8ROW3=VK_SPACE
COL8ROW4=KY_ORANGE
COL8ROW5=open
COL8ROW6=open
COL8ROW7=VK_DELETE
;;;;;;;;;;;;;
COL9ROW0=open
COL9ROW1=open
COL9ROW2=open
COL9ROW3=open

```

```

COL9ROW4=open
COL9ROW5=open
COL9ROW6=open
COL9ROW7=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 modified with ORANGE
;; on the MX8 32-key keypad
;;-----
[Map]
MAP=MAP_ORANGE32
;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_F8
COL0ROW1=VK_F7
COL0ROW2=VK_F6
COL0ROW3=VK_NEXT
COL0ROW4=SHIFT+VK_TAB
COL0ROW5=open
COL0ROW6=open
COL0ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=CHANGE+MAP_VOLUME
COL1ROW3=open
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=VK_F9
COL2ROW1=VK_F10
COL2ROW2=SHIFT+'8'
COL2ROW3=VK_PRIOR
COL2ROW4=open
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=VK_BACKSLASH
COL4ROW1=SHIFT+'3'
COL4ROW2=SHIFT+VK_HYPHEN
COL4ROW3=SHIFT+VK_BACKSLASH
COL4ROW4=VK_EQUAL
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_INSERT

```

```

;;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;
COL6ROW0=VK_LBRACKET
COL6ROW1=SHIFT+'2'
COL6ROW2=SHIFT+VK_SLASH
COL6ROW3=SHIFT+VK_SEMICOLON
COL6ROW4=SHIFT+'1'
COL6ROW5=open
COL6ROW6=open
COL6ROW7=VK_APOSTROPHE
;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;
COL8ROW0=VK_RBRACKET
COL8ROW1=VK_COMMA
COL8ROW2=SHIFT+'4'
COL8ROW3=VK_BACK
COL8ROW4=open
COL8ROW5=open
COL8ROW6=open
COL8ROW7=VK_PERIOD
;;;;;;;;;;;;;
COL9ROW0=open
COL9ROW1=open
COL9ROW2=open
COL9ROW3=open
COL9ROW4=open
COL9ROW5=open
COL9ROW6=open
COL9ROW7=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 on the MX8 32-key keypad
;; modified with BLUE
;;-----
[Map]
MAP=MAP_BLUE32
;;;;;;;;;;;;;
COL0ROW0=VK_F13
COL0ROW1=VK_F12
COL0ROW2=VK_F11

```

```

COL0ROW3=VK_LEFT
COL0ROW4=VK_CAPITAL
COL0ROW5=open
COL0ROW6=open
COL0ROW7=open
;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=CHANGE+MAP_BRIGHT
COL1ROW3=open
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;
COL2ROW0=VK_F14
COL2ROW1=VK_F15
COL2ROW2=KY_PROG1B
COL2ROW3=VK_RIGHT
COL2ROW4=open
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;
COL4ROW0=VK_SLASH
COL4ROW1=open
COL4ROW2=open
COL4ROW3=VK_ESCAPE
COL4ROW4=SHIFT+'9'
COL4ROW5=open
COL4ROW6=open
COL4ROW7=SHIFT+'6'
;;;;;;;;;;
COL5ROW0=open
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;
COL6ROW0=open
COL6ROW1=open
COL6ROW2=open
COL6ROW3=open
COL6ROW4=SHIFT+'0'
COL6ROW5=open
COL6ROW6=open
COL6ROW7=SHIFT+VK_APOSTROPHE
    
```

```

;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;
COL8ROW0=open
COL8ROW1=open
COL8ROW2=open
COL8ROW3=VK_HYPHEN
COL8ROW4=open
COL8ROW5=open
COL8ROW6=open
COL8ROW7=SHIFT+VK_EQUAL
;;;;;;;;;;;;;
COL9ROW0=open
COL9ROW1=open
COL9ROW2=open
COL9ROW3=open
COL9ROW4=open
COL9ROW5=open
COL9ROW6=open
COL9ROW7=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 on the MX8 32-key keypad
;; modified with SHIFT
;;-----
[Map]
MAP=MAP_SHIFT32
;;;;;;;;;;;;;
COL0ROW0=VK_F18
COL0ROW1=VK_F17
COL0ROW2=VK_F16
COL0ROW3=VK_HOME
COL0ROW4=open
COL0ROW5=open
COL0ROW6=open
COL0ROW7=open
;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=open
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0=VK_F19
COL2ROW1=VK_F20
COL2ROW2=KY_PROG1S

```

```

COL2ROW3=VK_END
COL2ROW4=open
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=SHIFT+' 1 '
COL4ROW1=SHIFT+' 4 '
COL4ROW2=SHIFT+' 7 '
COL4ROW3=open
COL4ROW4=KY_PROG2S
COL4ROW5=open
COL4ROW6=open
COL4ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=SHIFT+' 2 '
COL6ROW1=SHIFT+' 5 '
COL6ROW2=SHIFT+' 8 '
COL6ROW3=SHIFT+' 0 '
COL6ROW4=KY_PROG3S
COL6ROW5=open
COL6ROW6=open
COL6ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;
COL8ROW0=SHIFT+' 3 '
COL8ROW1=SHIFT+' 6 '
COL8ROW2=SHIFT+' 9 '
COL8ROW3=VK_SPACE
COL8ROW4=open
COL8ROW5=open
COL8ROW6=open
COL8ROW7=open
    
```

```

;;;;;;;;;;;;;
COL9ROW0=open
COL9ROW1=open
COL9ROW2=open
COL9ROW3=open
COL9ROW4=open
COL9ROW5=open
COL9ROW6=open
COL9ROW7=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_ORANGESHFT
;;;;;;;;;;;;;
COL0ROW0=VK_F23
COL0ROW1=VK_F22
COL0ROW2=VK_F21
COL0ROW3=open
COL0ROW4=open
COL0ROW5=open
COL0ROW6=open
COL0ROW7=open
;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=open
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0=VK_F24
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=open
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=open
COL4ROW3=open

```



```

COL4ROW4=open
COL4ROW5=open
COL4ROW6=open
COL4ROW7=open
;;;;;;;;;;
COL5ROW0=open
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=open
COL6ROW7=open
;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
    
```

## Output File

```

[HKEY_CURRENT_USER\Keyboard Layout\Keymaps\Default]
"HKL"="00000409"
"Head"=hex: 05,0A,08,50,00,00,FF,13,03,0A,FF,FF,40,48,50,58

;; Normal32
"Map4"=hex:\
    72,71,70,28,09,00,00,00,00,00,8C,F3,0D,00,00,00,\
    73,74,E9,26,10,00,00,00,00,00,00,00,00,00,00,\
    31,34,37,12,ED,00,00,11,00,00,00,00,00,00,00,\
    32,35,38,30,EF,00,00,F1,00,00,00,00,00,00,00,\
    33,36,39,20,F2,00,00,2E,00,00,00,00,00,00,00
"Flag4"=hex:\
    00,00,00,00,00,00,00,00,00,00,00,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,A0,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Orange32
"Map5"=hex:\
    77,76,75,22,09,00,00,00,00,00,00,00,00,00,00,\
    78,79,38,21,00,00,00,00,00,00,00,00,00,00,00,\
    DC,33,BD,DC,BB,00,00,2D,00,00,00,00,00,00,00,\
    DB,32,BF,BA,31,00,00,DE,00,00,00,00,00,00,00,\
    
```

```

        DD,BC,34,08,00,00,00,00,BE,00,00,00,00,00,00,00
"Flag5"=hex:\
    00,00,00,00,10,00,00,00,00,00,00,00,B5,00,00,00,00,00,\
    00,00,10,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,10,10,10,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,10,10,10,10,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,10,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Blue32
"Map6"=hex:\
    7C,7B,7A,25,14,00,00,00,00,00,00,00,00,00,00,00,\
    7D,7E,EC,27,00,00,00,00,00,00,00,00,00,00,00,00,\
    BF,00,00,1B,39,00,00,36,00,00,00,00,00,00,00,00,\
    00,00,00,00,30,00,00,DE,00,00,00,00,00,00,00,00,\
    00,00,00,BD,00,00,00,BB,00,00,00,00,00,00,00,00
"Flag6"=hex:\
    00,00,00,00,00,00,00,00,00,00,00,00,B7,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,10,00,00,10,00,00,00,00,00,00,00,00,\
    00,00,00,00,10,00,00,10,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,10,00,00,00,00,00,00,00,00

;; Shift32
"Map7"=hex:\
    81,80,7F,24,00,00,00,00,00,00,00,00,00,00,00,00,\
    82,83,EA,23,00,00,00,00,00,00,00,00,00,00,00,00,\
    31,34,37,00,EE,00,00,00,00,00,00,00,00,00,00,00,\
    32,35,38,30,F0,00,00,00,00,00,00,00,00,00,00,00,\
    33,36,39,20,00,00,00,00,00,00,00,00,00,00,00,00
"Flag7"=hex:\
    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,\
    10,10,10,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    10,10,10,10,00,00,00,00,00,00,00,00,00,00,00,00,\
    10,10,10,00,00,00,00,00,00,00,00,00,00,00,00,00

;; ShiftOrange
"Map12"=hex:\
    86,85,84,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    87,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    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,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
"Flag12"=hex:\
    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,\
    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

```

## Appendix B Technical Specifications

### Physical Specifications

Features		Specifications	Comments	
CPU		Intel Xscale operating at 520 MHz	32 bit CPU (with on-chip cache)	
Memory	RAM	128 MB SDRAM 128 MB Strata Flash	20 MB available for programs and data	
Display	LCD	Transmissive Color – optimized for indoor use	Transmissive LCD with touchscreen. Customer Configurable Display LED Backlighting	
Mass Storage	Removable Mini SD card	128MB	Mini SD Card	
PCMCIA Interface		None		
Weights		Unit with radio, battery, SE955 scanner and handle	1 lbs	458g
		Unit with radio, battery, SE955 scanner and handstrap	0.84 lbs	385g
		Battery	2.8 oz	80g
		Radio – 2.4GHz CF 802.11b/g	0.35 oz	9.9g
		Mini SD Card	0.035 oz	1g
External Connectors/Interface		20 pin Multi function port	20 Position multi function IO Connector. Provides cabled connection to external devices such as an audio headset, USB/power connection, RS-232/power connection.	
Dimensions		Length	7.58"	19.2 cm
		Width at display	2.84"	7.2 cm
		Width at handgrip	2.45"	6.2 cm
		Depth at Scanner	1.72"	4.36 cm
		Depth at Battery	1.52"	3.86 cm
Scanner		No Scanner Intermec EV-15 Linear Imager HHP 2 D imager (5300) Symbol SE955 Short Range	Integrated SE955	
Batteries	Main	Li-Ion battery pack 3.7V 3000mAh	In-Unit Chargeable or Externally Chargeable	
	Backup (CMOS)	Internal Nickel Metal Hydride (Ni-MH) 2.4V max.	Automatically charges from main battery during normal operation. Requires AC power for re-charging. Minimal life expectancy is 2 years.	

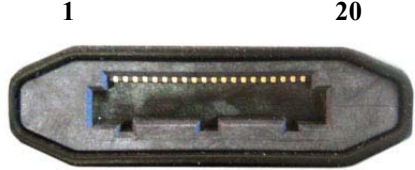
Features		Specifications	Comments
Radio	802.11 b/g LXE	2.4GHz (Compact Flash device in PCMCIA Adapter Card)	Supports diversity. Dynamic control for power management.

## Display Specifications

Feature	Specification
Type	LCD – Active Transmissive Color / LED Backlight
Resolution	320 (Vertical) x 240 (Horizontal) pixels
Size	1/4 VGA portrait
Diagonal Viewing Area	2.8 in (7.12 cm)
Dot Pitch	60 (W)um X 180 (H) um
Dot Size	180 um X 180 um
Color Scale	256 colors

## Pinout I/O Port

Pin No	Pin Description
1	UART_TXD
2	UART_RTS
3	UART_RXD
4	UART_CTS
5	GND
6	USBC_D+
7	USBC_VBUS
8	HS_OUT
9	HS_SLEEVE
10	HS_DETECT
11 to 13	DC_GND
14	UART_DTR
15	UART_DSR
16	USBC_D-
17	HS_MIC
18 to 20	DC_IN



## Environmental Specifications

### MX8

Feature	Specification
Operating Temperature	14°F to 122°F (-10°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
Water and Dust	IP54
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Standards	See “MX8 User’s Guide”, Appendix B.
Contamination	Resistant to exposure to skin oil and other lubricants.
Vibration	Based on MIL Std 810D
ESD	8 kV air, 4kV direct contact

### AC Wall Adapter

Feature	Specification
Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Current Fuse
Input Voltage	100VAC min – 240 VAC max
Input Frequency	50 - 60 Hz
Input Connector	North American wall plug, no ground
Output Connector	AC wall adapter has a 5.5mm barrel connector. This connects to the LXE cables which transition power to the 20 pin D connector.
Output Voltage	+5V, regulated
Output Current	0 Amps min, 3 Amps max
Operating Temperature	32 F to 100° F / -0° C to 40° C  <i>The LXE-approved AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.</i>
Storage Temperature	-40° F to 180° F / -40° C to 80° C (fahrenheit degrees (temperature) = ((centigrade temperature)*9/5)+32)
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

## Radio Specifications

### Summit Client

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Radio Frequencies	2.4 to 2.4897 GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	50 mW max.
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	see Environmental Specifications
Storage Temperature	see Environmental Specifications
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes
Hotswapping	No

### Bluetooth

Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 ft (10 meters) line of sight
Bluetooth Version	2.0 + EDR

## List of Valid VK Codes for CE

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 .

VK_ADD	VK_F3	VK_NUMPAD9
VK_APOSTROPHE	VK_F4	VK_OEM_CLEAR
VK_APPS	VK_F5	VK_OFF
VK_ATTN	VK_F6	VK_PA1
VK_BACK	VK_F7	VK_PAUSE
VK_BACKQUOTE	VK_F8	VK_PERIOD
VK_BACKSLASH	VK_F9	VK_PLAY
VK_BROWSER_BACK	VK_FINAL	VK_PRINT
VK_BROWSER_FAVORITES	VK_HANGUL	VK_PRIOR
VK_BROWSER_FORWARD	VK_HANJA	VK_RBRACKET
VK_BROWSER_HOME	VK_HELP	VK_RBUTTON
VK_BROWSER_REFRESH	VK_HOME	VK_RCONTROL
VK_BROWSER_SEARCH	VK_HYPHEN	VK_RETURN
VK_BROWSER_STOP	VK_INSERT	VK_RIGHT
VK_CANCEL	VK_JUNJA	VK_RMENU
VK_CAPITAL	VK_KANA	VK_RSHIFT
VK_CLEAR	VK_KANJI	VK_RWIN
VK_COMMA	VK_LAUNCH_APP1	VK_SCROLL
VK_CONTROL	VK_LAUNCH_APP2	VK_SELECT
VK_CONVERT	VK_LAUNCH_MAIL	VK_SEMICOLON
VK_CRSEL	VK_LAUNCH_MEDIA_SELECT	VK_SEPARATOR
VK_DECIMAL	VK_LBRACKET	VK_SHIFT
VK_DELETE	VK_LBUTTON	VK_SLASH
VK_DIVIDE	VK_LCONTROL	VK_SLEEP
VK_DOWN	VK_LEFT	VK_SNAPSHOT
VK_END	VK_LMENU	VK_SPACE
VK_EQUAL	VK_LSHIFT	VK_SUBTRACT
VK_EREOF	VK_LWIN	VK_TAB
VK_ESCAPE	VK_MBUTTON	VK_UP
VK_EXECUTE	VK_MEDIA_NEXT_TRACK	VK_VOLUME_DOWN
VK_EXSEL	VK_MEDIA_PLAY_PAUSE	VK_VOLUME_MUTE
VK_F1	VK_MEDIA_PREV_TRACK	VK_VOLUME_UP
VK_F10	VK_MEDIA_STOP	VK_ZOOM
VK_F11	VK_MENU	
VK_F12	VK_MULTIPLY	
VK_F13	VK_NEXT	
VK_F14	VK_NOCONVERT	
VK_F15	VK_NONAME	
VK_F16	VK_NUMLOCK	
VK_F17	VK_NUMPAD0	
VK_F18	VK_NUMPAD1	
VK_F19	VK_NUMPAD2	
VK_F2	VK_NUMPAD3	
VK_F20	VK_NUMPAD4	
VK_F21	VK_NUMPAD5	
VK_F22	VK_NUMPAD6	
VK_F23	VK_NUMPAD7	
VK_F24	VK_NUMPAD8	

## ASCII Control Codes

The following table lists ASCII Control codes in hexadecimal and their corresponding Control-key combinations.

Char	Hex	Control-Key	Control Action	
NUL	0	^@	NULL character	Ctrl-Shift-`
SOH	1	^A	Start Of Heading	VK_CONTROL (0x11) down VK_A (0x41) down WM_CHAR (0x1) VK_A (0x41) up VK_CONTROL (0x11) up
STX	2	^B	Start of TeXt	Ctrl-b
ETX	3	^C	End of TeXt	Ctrl-c
EOT	4	^D	End Of Transmission	Ctrl-d
ENQ	5	^E	ENQuiry	Ctrl-e
ACK	6	^F	ACKnowledge	Ctrl-f
BEL	7	^G	BELL, rings terminal bell	Ctrl-g
BS	8	^H	BackSpace (non-destructive)	Ctrl-h
HT	9	^I	Horizontal Tab (move to next tab position)	Ctrl-i
LF	a	^J	Line Feed	Ctrl-j
VT	b	^K	Vertical Tab	Ctrl-k
FF	c	^L	Form Feed	Ctrl-l
CR	d	^M	Carriage Return	Ctrl-m
SO	e	^N	Shift Out	Ctrl-n
SI	f	^O	Shift In	Ctrl-o
DLE	10	^P	Data Link Escape	Ctrl-p
DC1	11	^Q	Device Control 1, normally XON	Ctrl-q
DC2	12	^R	Device Control 2	Ctrl-r



Char	Hex	Control-Key	Control Action	
DC3	13	^S	Device Control 3, normally XOFF	Ctrl-s
DC4	14	^T	Device Control 4	Ctrl-t
NAK	15	^U	Negative AcKnowledge	Ctrl-u
SYN	16	^V	SYNchronous idle	Ctrl-v
ETB	17	^W	End Transmission Block	Ctrl-w
CAN	17	^X	CANcel line	Ctrl-x
EM	19	^Y	End of Medium	Ctrl-y
SUB	1a	^Z	SUBstitute	Ctrl-z
ESC	1b	^[	ESCape	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1b VK_PACKET up VK_CONTROL up
FS	1c	^\ 	File Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1c VK_PACKET up VK_CONTROL up
GS	1d	^] 	Group Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1d down WM_CHAR (0x1d) up VK_PACKET up VK_CONTROL up

Char	Hex	Control-Key	Control Action	
RS	1e	^^	Record Separator	VK_CONTROL (0x11)down VK_SHIFT (0x10) down WM_CHAR 0x36 down WM_CHAR 0x36 up VK_SHIFT up VK_CONTROL up
US	1f	^_	Unit Separator	VK_CONTROL (0x11) down VK_SHIFT (0x10) down VK_PACKET (0xe7) down WM_CHAR 0x1f VK_PACKET (0xe7) up VK_SHIFT (0x10) up VK_CONTROL (0x11) up

## Index

---

### A

About	
software, hardware, version, network IP	80
About LXE	
software, hardware, version	81
AC External Power Supply, How to	16
AC Power Adapter	
Assembly	16
Accessibility settings	82
Accessories	39
Electrostatic Discharge	11
Installing	11
Activation Key	
AppLock	12
ActiveSync	
Backup Data Files	117
Cables	116
Cold Boot and Loss of Host Re-connection	119
Connect cables	118
Connection, serial or USB	115
Disconnect, how to	119
Explore	118
Help	114
Initial installation	115
instruction	114
IR port transmission	72
partnership prerequisite	117
Setup Wizard	114, 115
Troubleshooting	119
ActiveSync Help	72
Adapters	
Avalanche	137
Admin Hotkey	
AppLock	213
Administration	
AppLock	82
Administrator	
Summit client utility	169
Align	
touchscreen	22
Allow Close	217
Allow PC Connection	106
Alpha Mode LED	55
Alt key function	56
API calls	140
API Routines	66
Appearance options	95
Application Panel	213
AppLock	
EUIE	217

Passwords	211
Setup	207
AppLock Administrator	68
ASCII Control Codes in hex	258
Asian fonts	99
Assemble	
Audio connection	19
Headset and microphone	19
RS232 connection	18
USB connection	17
assign key sequences to Diamond keys	100
Audible verification signals	47
Audio Cable	
Install	19
audio codecs	47
Audio headset interface	46
Audio support	47
Audio Volume settings	24
Audio/Microphone Connector	254
Auto hide	76
Auto-reconnect, Bluetooth	90
Autorun files at startup	71
Avalanche Enabler installation	125
Avalanche update settings	130

---

### B

Background and Window colors	95
Backlight display timer	22
Backlight properties	95
Backlight timers	95
Backup Battery	
Low	60
Nickel Metal Hydride	45
Time Limit	61
Backup Data Files	117
Backup software	67
Barcode	
Enable or Disable	148
Barcode – Symbology Settings	150
Barcode Data Match list	153
Barcode processing overview	144
Barcode Tab	148
Batteries	254
battery	
trickle charging	15
Battery	
Backup, details	61
charge before using	15
Charger	63
Charging	45
Check status and power reading	15

Compartment.....	15	Clear registry settings .....	140
Critical Suspend state.....	61	Client	
Hotswapping .....	61	and Network Setup.....	26
Important.....	3	Code ID, Enable .....	149
Life Approximate.....	60	Code IDs.....	158
Lithium-Ion (Li-Ion).....	45, 60	Cold Boot.....	48
Low .....	61	COLDBOOT.EXE.....	124
Main.....	60	COM Ports.....	143
Main Battery Pack, details .....	60	Configurations.....	46
Publication .....	62	COM1 port settings .....	147
Safety .....	62	Command Prompt.....	74
status .....	60	Commit button	
status LED.....	15	Global.....	175
Battery Auto Turn Off .....	95	Profile.....	170
Battery Power Scheme.....	23	Components.....	5
Battery voltage and status display .....	83	Computer Friendly Name .....	89
Baud Rate .....	143	Connect	
Bluetooth		ActiveSync.....	72
barcode reader setup.....	33	Connect External PS.....	16
devices .....	32	Connect Using .....	106
Initial Use.....	29	Connection	
LXEZ Pairing specification.....	52	Avalanche .....	131
Options.....	29	Contact LXE .....	39
Settings tab.....	88	Control Char mapping .....	148
Subsequent Use.....	31	Control characters.....	157
Bluetooth control panel .....	84	Control Panel options .....	78
Bluetooth Properties panel.....	87	Controls, Physical.....	48
Bluetooth Settings, Chart.....	88	Copyrights .....	112
Boot loader .....	67	Core Logic .....	43
		CPU .....	253
		CPU Xscale .....	43
		Create a dialup, direct, or VPN connection .....	103
		Create Connection option .....	103
		Ctrl Char Mapping.....	156
		Ctrl key function.....	56
		Cumulative mode timers.....	107
		Current Time .....	93
		Custom identifier .....	148
		Custom Identifiers .....	158
		Custom Key Mapping.....	236
		Custom parameter option.....	175
		Customize dates, times, currency .....	108
		<b>D</b>	
		Data Bits .....	143
		Data entry	
		keypad.....	36
		laser scanner.....	38
		stylus .....	37
		virtual keyboard .....	36
		Data entry .....	36
		Date and Time default settings .....	93
		Daylight Savings .....	93
		DEFAULT.KEY.....	237
		Desktop.....	69
		Device Name and description.....	112

Diagnostics .....	174
Diags tab	
Summit .....	174
Dialing properties .....	94
Diamond keys .....	54
Digital certificates .....	91
Dimensions .....	254
Disable Summit Client .....	73
Discover and Query .....	85
Display .....	253
Avalanche .....	135
Features .....	59
Pixels .....	59
Specifications .....	254
Display Backlight Timer .....	59
display owner notes .....	22
Display properties .....	95
Display Timer .....	59
Double-click sensitivity for stylus taps .....	102

**E**

EAP-FAST Authentication, Summit .....	185
Edit Diamond key parameters .....	54
Enable Code ID .....	149
Enable Code ID drop-down box .....	148
Enable Internal Scanner sound .....	146
Enable or Disable specific symbology .....	148
Enabler	
communication .....	128
Network adapter status, link speed .....	140
Enabler Configuration .....	128
Enabler installation .....	125
Enabler passwords .....	129
Enabler Uninstall Process .....	125
End user switching	
Touch .....	212
end-user flash card .....	113
Entering Data .....	36
Environmental Specifications .....	255
Error Messages	
AppLock .....	221
EUIE .....	217
EV-15 linear imager .....	47
Example	
Barcode processing .....	160
Execution	
Avalanche .....	132
Expand Control Panel .....	77
External Auto Turn Off .....	95
External Connector/Interface .....	253
External modem	
not supported .....	66
External PS .....	16

**F**

Factory Default Settings	
Summit Client .....	175
Factory Default, reset registry to .....	140
Features .....	2
MX8 .....	1
Flash .....	253
Flash and Reflash .....	141
Fonts and keymaps .....	99
Forms entry .....	36
Function	
2 <sup>nd</sup> Key .....	57
Alt Key .....	56
CapsLock Mode .....	58
Ctrl Key .....	56
Shft Key .....	56

**G**

General system parameter .....	111
Getting Help .....	39
Getting Started .....	11
Getting the Most from Your Batteries .....	62
Global parameters .....	175
Glossary .....	39
Good scan Bad scan .....	146
GrabTime utility .....	124

**H**

Handle	
Installation .....	13
Handling Batteries .....	62
Handstrap .....	8
Handstrap, Install .....	14
Hardware	
Configuration .....	43
Help .....	39
HHP 5380SF 2D imager .....	47
HKEY_LOCAL_MACHINE .....	80, 81
Hotkey	
AppLock .....	218
Hotswapping	
allowed for Main Battery .....	61
hotswapping not allowed	
flash cards .....	50
radio .....	45
scanners .....	47
HyperTerminal	
ActiveSync .....	120

**I**

Icons	
Desktop .....	69
Idle Time .....	95

IEC IP54 .....	255
Inbox	
Outlook .....	74
Input panel	
virtual keyboard .....	36
Input Panel properties .....	96
Install ActiveSync on Desktop or Laptop.....	115
Install MX8 LXEbook .....	25
Integrated barcode scanner port.....	47
Internal modems	
not supported by LXE .....	94
Internal SD flash card and port.....	50
Internet connectivity .....	97
Internet Explorer.....	74
AppLock .....	217
Radio card and ISP required .....	74
Internet popup blocker.....	97
Internet privacy.....	97
Internet Security .....	97
IO Components.....	43

---

## J

Java Option.....	66
JEM-CE .....	68

---

## K

key repeat delay and rate .....	99
Keyboard	
Onscreen only .....	96
KEYCOMP compiler .....	257
KEYCOMP.EXE.....	236
Keymap	
32-key Keymap.....	231
Keypad	
and entering data.....	36
Keypad Shortcuts.....	21

---

## L

LAUNCH.EXE.....	121
LEAP without WPA Authentication, Summit.....	184
LED	
Alpha mode.....	55
Battery Status .....	60
Li-Ion battery life.....	15
List of configured ActiveSync connections.....	106
Logging	
AppLock .....	220
Loss of Host Re-connection.....	119
Low Battery Warning .....	61
LXE Manuals CD .....	39
LXE Security Primer .....	165, 194
LXE ServicePass .....	39
LXEbook – MX8 Users Guide .....	25

---

## M

MAC address .....	80, 81
Main.....	143
Main Battery Pack .....	45
Main tab	
Summit.....	168
Mappable Diamond Keys .....	54
Mass Storage .....	253
Match list.....	153
Match list rules .....	154
Media Player.....	75
Memory .....	253
allocate for programs or storage.....	112
Memory installed.....	111
Memory system parameter .....	111
Menu Options	
Start.....	71
Microphone adjustment.....	19
Microsoft File Viewers and password protected files .....	71
MiniSD Card	
Storage .....	50
Mixer record gain .....	101
Mode	
Off.....	52
On.....	51
Suspend.....	52
Mode Key Functions .....	58
Modes	
AppLock .....	210
MX8 Multi-Charger	
described .....	63
My Certificates .....	27
My Device	
Folders .....	70

---

## N

Network driver properties.....	103
Network Profile	
Avalanche .....	138, 139
No Security	
Summit.....	182

---

## O

Off Mode .....	52
ON Mode characteristics .....	51
Operating Temperature	
MX8 .....	255
US AC to DC .....	255
Optional	
Software .....	68
Optional Software	
RFTerm.....	68
WaveLink Avalanche Enabler .....	68

Orange and Blue keys .....	57
Owner	
Identification .....	104
Network ID and password.....	104
Notes .....	104
Owner information .....	22

---

**P**

Parity .....	143
Password.....	105
AppLock .....	211
At Power On .....	105
Passwords	
AppLock Save As .....	220
Passwords lost at cold boot.....	124
PEAP MSCHAP Authentication, Summit.....	186
Pen Stylus	
and data entry .....	37
Pen Stylus Pressure limit .....	59
Permanent storage of drivers and utilities.....	113
Physical Specifications .....	253
Pin 9 power unavailable .....	143
Pistol Grip Handle .....	13
Power key .....	48
Power key location .....	20
Power Mode Properties .....	107
Power Modes .....	51
Power Off	
schemes.....	23
Power Port 1 while asleep.....	145
Power Supply	
Battery Pack .....	45
Prefix and Suffix Control .....	155
Pre-loaded Files .....	66
Private key install .....	28
Processor speed .....	43
processor type.....	111
Profile buttons .....	170
Profile parameters	
Summit.....	171
Programmable Keys .....	54
Prompt	
Command.....	74
Proprietary boot loader .....	67
Protective Film .....	25
Putting it all Together .....	13

---

**Q**

Quick Start Instructions .....	11
--------------------------------	----

---

**R**

Reboot, How to.....	48
Recalibration.....	110

Reflash the Mobile Device .....	141
Reflash, Automatic .....	142
Reflash, Manual .....	141
REGEDIT.EXE .....	124
Regional settings, defaults .....	108
Registry and save settings.....	49
Registry content	
back up location .....	113
REGLOAD.EXE .....	125
Release/Renew button .....	174
Remove a program.....	108
Reset to Factory Default, How to .....	49
Review System and mobile device data and revision levels.....	111
RFTerm .....	26, 68
Root CA Certificates	
Generating.....	194
Installing on mobile device .....	196
RS-232 and Power port.....	46

---

**S**

Save settings .....	49
Scan Status LED .....	55
Scanner	
Main tab .....	146
Port.....	146
Send Key Messages .....	146
WEDGE .....	146
Scanner Aperture identify type.....	7
Scanner Control Characters Tab.....	157
Scanner engine type.....	254
Scanner LED, functioning .....	38
Scanner, factory defaults .....	143
Scanning	
and data entry .....	38
Schemes tab .....	107
Screwdriver	
Phillips, for handstrap .....	14
SD card interface .....	2, 44
SD Cards	
Install and remove.....	50
SE955 .....	143
SE955 laser scanner.....	47
Second key function, described .....	57
Security Panel	
AppLock .....	218
Select a font .....	99
Select a key map .....	99
Send Key Messages and Wedge.....	145, 146
Set Owner information .....	22
Set time zone .....	22
Settings Menu	
Status tab.....	140
Setup	
AppLock .....	207
Setup new device	

AppLock .....208  
 Setup Software.....65  
 Shift key function .....56  
 Shortcuts  
     Avalanche .....136  
 Show Clock .....76  
 Shutdown time limits.....61  
 Soft Keyboard.....96  
 Software  
     and Files .....66  
     Applications .....67  
     Load .....66  
     supported by the MX8.....66  
 Sounds and Volume default values.....112  
 speaker .....47  
 Speaker location .....24  
 Special functions.....56  
 SSID .....171  
 Standard keys  
     functions.....56  
 Start Menu  
     Shutdown .....69  
 Start Menu, described .....71  
 Start Ping .....174  
 Startup and shutdown  
     Avalanche .....134  
 Static screen protector .....59  
 Status  
     Avalanche .....139  
 Status Panel  
     AppLock .....219  
 Stereo and mono settings for headsets .....101  
 Sticky keys.....56  
 Stop Bits .....143  
 Stop the Enabler Service.....126  
 Storage Temperature  
     MX8 .....255  
     US AC to DC .....255  
 Stored certificates .....91  
 Storing MiniSD Cards .....50  
 Strip Leading and Trailing Control.....152  
 Stylus  
     and data entry .....37  
 Stylus pressure.....59  
 Stylus sensitivity.....110  
 Summit  
     EAP-FAST Authentication .....185  
     LEAP without WPA Authentication .....184  
     No Security .....182  
     PEAP GTC Authentication .....190, 191  
     PEAP MSCHAP Authentication.....186  
     startup.....26  
     WEP keys .....183  
     WPA LEAP Authentication .....188  
     WPA PSK Authentication.....189  
 Summit Client.....73  
 Summit Client configuration .....166  
 Summit client utility .....166

Summit client utility (SCU)  
     Diags tab .....174  
     Global tab .....175  
     Profile tab .....170  
     Status tab .....173  
 Suspend button .....69  
 Suspend mode.....52  
 Suspend Mode  
     How to.....20  
 Suspend mode and ActiveSync .....48  
 Switch applications  
     Multi AppLock.....12  
 Symbology.....150  
     strip leading strip trailing .....152  
 Symbology settings.....148  
 System Configuration .....65  
 System Hardware Configuration .....43  
 System Memory.....44  
 System Status LED.....55

---

**T**

Taskbar defaults.....76  
 Technical specifications  
     bootloader .....67  
     version control .....67  
 Technical Specifications.....253  
 Terminal Emulation parameters .....26  
 Tethered scanners .....38  
 Tile.....95  
 Time Zone .....93  
 Timer  
     battery power timer .....22  
     cumulative effect.....23  
     external power timer .....22  
 Touch Screen and Keypad Shortcuts .....21  
 Touch Screen and the Stylus.....21  
 Touchscreen.....59  
     adjustment .....22  
     and data entry .....37  
 Transcriber.....76  
 Translate All .....157  
 Translate control codes.....157  
 Transmissive Display .....59  
 Trigger Handle.....7  
 Troubleshooting  
     AppLock .....220  
 Troubleshooting  
     ActiveSync .....119  
     AppLock Password .....211  
     Coldboot.....124  
     Password, screensaver.....105  
 turbo mode switching .....43

---

**U**

Uninstall a program .....108



Update monitoring .....	126
USB Client and Power port .....	46
User access	
power up password.....	105
User Certificate on the MX8.....	203
User Certificates	
Generating.....	198
User certificates and private keys .....	27
User-specific application version information... 80, 81	
Utilities	
Coldboot.....	124
Launch .....	121
Regedit .....	124
Regload .....	125

---

**W**

Version control .....	67
Version window information.....	80, 81
Vibration	
Good scan and bad scan .....	146
Vibration tab	
Scanner.....	163
Video Subsystem .....	44
View	
Display .....	59
Virtual keyboard	
Input panel .....	36
Virtual Keyboard.....	96
VK_Code List.....	257
Voice	
Accessories .....	39
Voice data .....	38
Volume	
adjust audio volume .....	24
using the keypad .....	24
Volume and Sounds default values.....	112
Volume control.....	47
Volume Mixer .....	101

---

**W**

Wake the device from Suspend .....	69
Warm Boot .....	48
Warning	
Low Battery .....	61
Warnings and Labels	
Laser Scanner.....	38
Wavelink Avalanche Enabler installation.....	125
Wedge.....	145, 146
Weights.....	253
WEP Keys	
Summit.....	183
When to use this guide.....	3
Where is the --- .....	24, 48
Where is the --- .....	38
Where is the --- .....	43
Windows CE on-line Help.....	65, 124
Windows Explorer .....	76
Windows OS version.....	111
Wireless communication .....	64
Wireless network configuration.....	165
Wireless Security	
Summit Client .....	179
Wireless Zero Config Utility	
Summit Client .....	73, 193
WLAN Networks.....	26
WLAN Profiles.....	26
WordPad .....	75
WPA LEAP Authentication, Summit.....	188
WPA PSK Authentication, Summit.....	189
WZC icon .....	73, 193

