

MX7 Reference Guide

(Microsoft® Windows® CE 5.0 Equipped)



Copyright © 2008 by LXE Inc.
All Rights Reserved
E-EQ-MX7RG-G



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 © 2008 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.

Odyssey Client © Copyright 2002-2006 Funk Software, Inc. All rights reserved. **Odyssey®** and **Funk®** are registered trademarks of Funk Software, 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.

Wavelink®, the Wavelink logo and tagline, **Wavelink Studio™**, **Avalanche Management Console™**, **Mobile Manager™**, 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.

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.

PSC® is a registered trademark of PSC Inc., 959 Terry Street, Eugene, OR 97402. The PSC logo is a trademark of PSC. PSC is owned (Apr 2007) by **DATALOGIC™** S.p.A, Via Candini, 2, 40012 Lippo di Calderara di Reno, Bologna, Italy.

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 © 2008 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.

Revision Notice

Chapter 1 – Introduction	Revised “Features”. Updated Accessories.
Chapter 2 – Physical Description and Layout	Added MX7 Cold Storage.
Chapter 3 – System Configuration	Revised “Control Panel Options” to add “WiFi”. Revised “Wavelink Avalanche Enabler Configuration”. Added “eXpress Scan”. Added “LXE Connect”.
Chapter 4 – Scanner	Updated Scanner Control Barcode tab panel.
Chapter 5 – Wireless Network Configuration	Revised the following sections: “Introduction”, “Summit Radio”, “Summit Client Utility”, “Main Tab”. Revised Profile Tab parameter: “Radio Mode”. Revised Global Tab parameters: “TX Diversity”, “Rx Diversity”. Added Global Mode parameter: “DFS Channels”.
Appendix B – Technical Specifications	Revised “Network Device Specifications”.



Table of Contents

CHAPTER 1 INTRODUCTION	1
Overview	1
Features	2
Important Battery Information	3
When to Use This Guide	3
Document Conventions	4
Components	5
Front	5
Back	6
Scanner / Imager Aperture	7
Continuous Scan Mode	7
AC Adapter	7
I/O Port and Cables	8
Handle and Handstrap	9
Quick Start	10
Troubleshooting	11
Entering the Multi AppLock Activation Key	11
Hotkey (Activation hotkey)	11
Touch	11
Hardware Setup	12
Installing Trigger Handle (Optional)	12
Inserting the Main Battery	13
About Lithium-Ion Batteries	13
Installing the Handstrap	14
Connecting an External Power Supply (Optional)	15
Putting it all together	15
Assembling the AC Power Adapter	15
Connecting the Multipurpose USB / Power Cable	16
Connecting the Multipurpose RS-232 / Power Cable	16
Connecting to a Printer Interface Cable	17
Connecting the Audio Cable and a Headset	17
Adjust Microphone and Secure the Cable	18
Entering Data	18
Power Key	19
Tapping the Touchscreen with a Stylus	20
Keypad Shortcuts	20
Software Setup	21
Touchscreen Calibration	21
Set Time Zone (Optional)	21
Enter Owner Information (Optional)	21
Set the Display Backlight Timer	22
Set the MX7 Power Schemes Timers	22
Set The Audio Speaker Volume	23
Using the Keypad	23
Using the Touchscreen	23
Applying the Protective Film to the Display	24
Copy the MX7 LX Ebook to the MX7 (Optional)	24
Client and Network Setup	25
Terminal Emulation Setup	25
Installing User Certificates and Private Keys	26

User Certificate	27
Private Key	28
Bluetooth	29
Initial Use.....	29
Settings Tab Bluetooth Options	30
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
MX7 with Label	33
MX7 without Label	34
Bluetooth Beep and LED Indications.....	34
Bluetooth Printer Setup	35
Entering Data.....	36
Using the Keypad.....	36
Using the Input Panel or Virtual Keyboard	36
Using the Stylus	37
Using the Integrated Barcode Scanner or Imager	38
Barcode Scanner	38
2D Imager	38
Scan Status LED	39
Tethered Scanners.....	39
Bluetooth Scanners and Printers	39
Voice Data	39
Saving Changes to the Registry.....	40
Getting Help.....	41
Manuals.....	41
Accessories	41

CHAPTER 2 PHYSICAL DESCRIPTION AND LAYOUT **45**

Hardware Configuration.....	45
System Hardware	45
Central Processing Unit	45
Core Logic	45
System Memory	46
Internal SD Memory Card.....	46
Video Subsystem	46
Power Supply	47
Main Battery Pack.....	47
Backup Battery.....	47
Client Ports	47
802.11b/g	47
COM Port.....	48
RS-232 Serial Port	48
USB Client Port	48
Audio Connection	48
Audio Support.....	49

Speaker.....	49
Volume Control.....	49
Voice	49
Scanner/Imager Port.....	50
Bluetooth LXEZ Pairing	51
Physical Controls.....	52
Power Key.....	52
Warm Reset.....	52
Cold Reset	52
Flash Cards	53
Flash Card Installation / Removal.....	54
Power Modes.....	55
Primary Events Listing.....	55
On Mode	55
The Display	55
The MX7	56
Suspend Mode.....	56
The MX7	56
Off Mode.....	56
The Keypads.....	57
Using the 55 Key ANSI / CE Keypad.....	58
Using the 32-Key Numeric-Alpha Keypad.....	59
Mappable Diamond Keys.....	60
55 Key Keypad.....	60
32 Key Keypad.....	61
LED Indicators.....	62
System Status	62
Scan Status	62
Alpha Mode (32-key Alph Key)	62
Standard Keys	63
Function Keys	63
Sticky Keys	63
Ctl / Ctrl (Control key)	63
Alt (Alternate key)	63
Shft (Shift key).....	63
Orange and Blue Keys	64
Field Exit.....	64
Mode Key Functions	65
CapsLock Mode	65
55-Key Keypad	65
32-Key Keypad	65
Touchscreen Display.....	66
Display Backlight Timer.....	66
Cleaning the Display and Scan Aperture	66
Power Supply	67
Checking Battery Status.....	67
MX7 Status LED and the Batteries	67
Main Battery Pack.....	67
Battery Hotswapping	68
Low Battery Warning	68
Backup Battery.....	69
Discharging	69
Handling Batteries Safely	69
Battery Maintenance Publication	69
MX7 Multi-Charger (Optional).....	70
Multi-Charger Indicators	71

LED Functions	71
LCD Messages	71
MX7 Cradles (Optional)	72
MX7 Cold Storage	73
Cold Storage Battery	73
Snowflake Decal	73
Heating Elements	73
Recharging Batteries	74
Normal Operation Temperature Ranges	74

CHAPTER 3 SYSTEM CONFIGURATION **75**

Introduction	75
Windows CE 5.0	75
Installed Software	76
Software Load	76
Software Applications	77
Software Backup	77
Version Control	77
Boot Loader	77
Folders Copied at Startup	78
Optional Applications	78
AppLock (Option)	78
Bluetooth (Option)	78
JAVA (Option)	78
LXE RFTerm (Option)	78
Wavelink Avalanche Enabler (Option)	79
Desktop	80
My Device Folders	81
Start Menu Program Options	82
Communication	83
ActiveSync	83
Connect	83
Remote Control	84
LXEConnect	85
Install LXEConnect	85
Using LXEConnect	86
Start / Stop FTP Server	86
Command Prompt	87
Inbox	87
Internet Explorer	87
Media Player	88
Microsoft WordPad	88
Odyssey Client	89
Radio Config Utility	89
Wireless Zero Config Utility and the Odyssey Client	89
Summit Client	90
Certs	90
Wireless Zero Config Utility and the Summit Client	90
Transcriber	91
Windows Explorer	91
Taskbar	92
Advanced Tab	93
Settings Control Panel Options	94
About	96

Accessibility.....	97
Administration – For AppLock.....	97
Battery.....	98
Bluetooth.....	99
Discover Button	100
Bluetooth Devices	101
Bluetooth Device Properties.....	102
Settings.....	103
Options	103
About.....	104
Pairing and Auto-Reconnect	105
Certificates	106
Date/Time	107
Dialing	108
Display	109
Background	109
Appearance	110
Backlight.....	110
Input Panel	111
Internet Options	112
Keyboard.....	114
Keymaps and Fonts	115
Backlight.....	115
Mappable Keys	116
Mixer.....	117
Mouse.....	118
Network and Dialup Connections	119
Create a Connection Option.....	119
Owner.....	120
Password	121
Troubleshooting	121
PC Connection	122
Power	123
Regional Settings	124
Remove Programs	124
Scanner.....	125
Determine Your Scanner Software Version.....	125
Factory Default Settings.....	126
Main Tab.....	127
COM1 Tab	128
Barcode – Advanced - Prefix / Suffix	129
Strip Leading / Strip Trailing Characters	129
Prefix / Suffix.....	129
Interaction between Strip Leading/Trailing and Prefix/Suffix Settings	130
Barcode - Advanced – Ctrl Char Mapping	131
Translate All.....	131
Barcode - Advanced – Scancode Enable	133
Barcode - Advanced – Code ID	134
No Code ID	134
AIM Code ID	134
Symbol Code ID.....	134
Strip Code ID	135
Strip Identifiers from EAN128 Barcodes	135
Adding Codes to the Match List for EAN128 Barcodes	136
Stylus	137
Double Tap.....	137

Calibration.....	137
System.....	138
General.....	138
Memory.....	139
Device Name.....	140
Copyrights.....	140
Volume and Sounds.....	141
Good Scan and Bad Scan Sounds.....	141
SD Flash Cards, CAB Files and Programs.....	142
Access Files on the Flash Card.....	142
ActiveSync / Get Connected Process.....	143
Introduction.....	143
Initial Install.....	144
Install ActiveSync on Desktop/Laptop.....	144
Serial Connection.....	144
USB Connection.....	144
Connect -- Initial Install Process.....	145
Change Connection Parameters.....	145
Connect.....	145
Explore.....	145
Disconnect.....	146
Serial Connection.....	146
USB Connection.....	146
Network Connection.....	146
Backup MX7 Files.....	146
Prerequisites.....	146
MX7 and PC Partnership.....	147
Serial Port Transfer.....	147
USB Transfer.....	147
Wireless Network Transfer.....	147
Cold Boot and Loss of Host Re-connection.....	147
ActiveSync Troubleshooting.....	148
Utilities.....	150
LAUNCH.EXE.....	150
REGEDIT.EXE.....	154
REGLOAD.EXE.....	154
WARMBOOT.EXE.....	154
WAVPLAY.EXE.....	154
Configuring GrabTime.....	154
Synchronize with a local time server.....	154
Configuring CapsLock Behavior.....	155
Configuring IPv6.....	155
Launch App / Launch Command.....	155
Command-line Utility.....	156
COLDBOOT.EXE.....	156
PrtScrn.EXE.....	156
LXE Login Utility.....	157
Installation.....	157
Using the Utility.....	158
Uninstall the LXE Login Utility.....	161
Wavelink Avalanche Enabler Configuration.....	162
Briefly.....	162
Enabler Install Process.....	162
Enabler Uninstall Process.....	162
Stop the Enabler Service.....	163
Update Monitoring Overview.....	163

Mobile Device Wireless and Network Settings	164
Enabler Configuration.....	165
File Menu Options	166
Avalanche Update using File Settings.....	167
Menu Options.....	167
Connection Tab	168
Execution Tab	169
Server Contact Tab.....	170
Startup/Shutdown Tab.....	171
Scan Config Tab.....	172
Display Tab	172
Shortcuts Tab	173
Adapters Tab	174
MX7 and Controlling Wireless Settings.....	176
Status Tab.....	177
Troubleshooting	177
eXpress Scan	178
API Calls	181
Clearing Registry Settings	181
Reflash the Mobile Device	182
Preparation	182
How To	182

CHAPTER 4 SCANNER 183

Introduction	183
Determine Your Scanner Software Version	184
Barcode Processing Overview	185
Factory Default Settings	185
Main Tab	187
COM1 Tab	188
Barcode Tab	189
Buttons	190
Continuous Scan Mode	190
Enable Code ID.....	191
Barcode – Symbology Settings	192
Strip Leading/Trailing Control.....	194
Barcode Data Match List.....	195
Barcode Data Match Edit Buttons	195
Match List Rules	196
Add Prefix/Suffix Control.....	197
Barcode – Ctrl Char Mapping	198
Translate All.....	198
Barcode – Custom Identifiers.....	200
Control Code Replacement Examples.....	201
Barcode Processing Examples	202
Length Based Barcode Stripping	203
Vibration Tab	205

CHAPTER 5 WIRELESS NETWORK CONFIGURATION 207

Introduction	207
Summit Client Configuration	208
Summit Client Utility.....	208
Help.....	208

Summit Tray Icon	209
Main Tab	210
Admin Login	211
Config Tab	212
Buttons	212
Config / Profile Parameters	214
Status Tab	217
Diags Tab	218
Buttons	218
Global or Global Settings Tab	219
Global Parameters	220
Summit Wireless Security	225
Sign-On vs. Stored Credentials	225
Windows Certificate Store vs. Certs Path	227
User Certificates	227
Root CA Certificates	227
No Security	229
WEP Keys	230
LEAP w/o WPA Authentication	231
EAP-FAST Authentication	233
PEAP/MSCHAP Authentication	235
WPA/LEAP Authentication	237
WPA PSK Authentication	238
PEAP/GTC Authentication	239
EAP-TLS Authentication	241
Funk Odyssey Client Configuration	243
Odyssey Client Menu	243
Settings	243
Commands	244
Tools	245
Help	245
Wireless Security	246
Set WEP	246
No Encryption	247
WEP Encryption	248
Set LEAP	250
WEP Authentication for LEAP	251
Set WPA	253
PEAP/MS-CHAP Authentication Configuration	255
Server Authentication	258
PEAP/GTC Authentication Configuration	259
Server Authentication	263
EAP-LEAP Authentication	264
EAP/TLS Authentication Configuration	266
Installing User Certificate	266
Setting EAP/TLS Parameters	269
Validating the Server Certificate	272
WPA/PSK Configuration	273
Trusted Server Configuration	275
Root Certificates	277
Downloading a Root CA Certificate to a PC	277
Installing a Root CA Certificate on the Mobile Device	279
User Certificates	281
Generating a User Certificate for the Mobile Device	281
Installing a User Certificate on the Mobile Device (WPA-TLS Only)	286
IEEE 802.11g Wireless LAN Configuration Utility	290

Wireless Zero Config Utility	292
Odyssey Client	292
Summit Client	293
 CHAPTER 6 APPLOCK	 295
Introduction	295
Determine Your AppLock Version	295
Setup a New Device	296
Administration Mode	298
End User Mode	298
Passwords	299
End-User Switching Technique	300
Using a Stylus Tap	300
Using the Switch Key Sequence	300
Multi-Application Configuration	301
Application Panel	301
Launch Button	303
Auto At Boot	303
Auto Re-Launch	304
Manual (Launch)	304
Allow Close	305
End User Internet Explorer (EUIE)	305
Security Panel	306
Setting an Activation Hotkey	306
Setting a Password in Security Panel	306
Status Panel	307
View	307
Log	308
Save As	308
Troubleshooting AppLock	309
 APPENDIX A KEY MAPS	 311
Introduction	311
55-Key Alphanumeric Keymaps	311
ANSI / CE Keypad	311
5250 Key Map for the 55-Key Keypad	316
32-Key Numeric-Alpha Keypad	317
Creating Custom Key Maps	322
Introduction	322
Keymap Source Format	323
COLxROWx Format	323
GENERAL Section	323
SPECIAL Section	324
MAP Section	324
Keycomp Error Messages	326
Sample Input File	330
Sample Output File	345
 APPENDIX B TECHNICAL SPECIFICATIONS	 347
Physical Specifications	347
Display Specifications	348
Bluetooth	348

Environmental Specifications	349
MX7	349
AC Wall Adapter	349
Network Device Specifications	350
Summit 802.11 b/g	350
Summit 802.11 a/b/g	350
Odyssey Client	350
 APPENDIX C REFERENCE MATERIAL	 351
Introduction	351
AppLock - Single Application Version	352
Determine Your AppLock Version	352
Setup a New Device	353
Administration Mode	354
End User Mode	354
Passwords	355
Password Troubleshooting	355
Application Configuration	356
Administrator Control Panels	356
Control Panel	357
End User Internet Explorer	357
Security Panel	358
Specify an Activation Hotkey	358
Setting a Password	358
Status Panel	359
View	359
Levels	359
Save As	360
AppLock Error Messages	361
AppLock Registry Settings	369
Valid VK Codes for CE	370
ASCII Control Codes	371
Hat Encoding	373
Decimal - Hexadecimal Chart	375
Revision History	377
 INDEX	 379

Illustrations

Figure 1-1 Front of MX7	5
Figure 1-2 Back	6
Figure 1-3 Beam Aperture	7
Figure 1-4 AC Adapter	7
Figure 1-5 I/O Port	8
Figure 1-6 Handle and Handstrap	9
Figure 1-7 MX7 Desktop	10
Figure 1-8 Trigger Handle Attach Points	12
Figure 1-9 Main Battery Pack	13
Figure 1-10 MX7 With Handstrap Installed	14
Figure 1-11 AC/DC 12V External Power Supply	15

Figure 1-12 Connect the USB / Power Cable to the MX7 Port	16
Figure 1-13 Connect the RS-232 / Power Cable to the MX7 Port.....	16
Figure 1-14 Connect to a Printer Interface Cable	17
Figure 1-15 Audio Cable and Headset.....	17
Figure 1-16 Power Key Location.....	19
Figure 1-17 Enter Suspend Mode – Press Enter	19
Figure 1-18 Speaker Location.....	23
Figure 1-19 Volume & Sounds Properties	23
Figure 1-20 Certificate Stores	27
Figure 1-21 View Certificate Details	28
Figure 1-22 Bluetooth Devices Display – Before Discovering Devices.....	29
Figure 1-23 Sample Bluetooth Address Barcode Label.....	33
Figure 1-24 About tab and Bluetooth Address	34
Figure 1-25 Input Panel / Virtual Keyboard	36
Figure 1-26 Laser Scanner Beam on Linear Barcode	38
Figure 1-27 Imager Bracketed Crosshair Target on 2D Barcode	38
Figure 1-28 Scan Status LED	39
Figure 2-1 System Hardware	45
Figure 2-2 COM1 Port.....	48
Figure 2-3 Flash Card Location	53
Figure 2-4 Power Modes – On, Suspend and Off.....	55
Figure 2-5 The 32-key and 55-key Keypads.....	57
Figure 2-6 The ANSI / Batch Keypad	58
Figure 2-7 The 32-Key Keypad	59
Figure 2-8 Mappable Diamond Keys.....	60
Figure 2-9 Touchscreen Display	66
Figure 2-10 LCD Panel and Dome Switch	70
Figure 3-1 Pocket CMD Prompt Screen	87
Figure 3-2 Radio Config Utility Main Menu	89
Figure 3-3 Taskbar General Tab	92
Figure 3-4 Advanced Tab	93
Figure 3-5 System – Accessibility	97
Figure 3-6 System – Battery	98
Figure 3-7 Control Panel - Bluetooth.....	100
Figure 3-8 Discover Bluetooth Devices.....	100
Figure 3-9 Bluetooth Devices Panel	101
Figure 3-10 Bluetooth Device Disconnect / Delete	102
Figure 3-11 Bluetooth Device Properties Menu	102
Figure 3-12 Bluetooth Device Settings Panel	103
Figure 3-13 Bluetooth About Panel	104
Figure 3-14 System – Stored Certificates	106
Figure 3-15 Date/Time Properties.....	107
Figure 3-16 Dialing.....	108
Figure 3-17 Display – Background.....	109
Figure 3-18 Display – Appearance	110
Figure 3-19 Display – Backlight.....	110
Figure 3-20 Input Panel	111
Figure 3-21 Internet Options.....	112
Figure 3-22 Keyboard Properties.....	114
Figure 3-23 Mappable Keys.....	116
Figure 3-24 Mixer.....	117
Figure 3-25 Mouse.....	118
Figure 3-26 Network and Dialup Connections	119
Figure 3-27 Owner Properties.....	120
Figure 3-28 Password	121
Figure 3-29 PC Connection	122

Figure 3-30 Power	123
Figure 3-31 Regional Settings	124
Figure 3-32 Scanner Control Panels	126
Figure 3-33 Scanner Panel - Main	127
Figure 3-34 Scanner Panel – COM1	128
Figure 3-35 Barcode – Advanced – Prefix / Suffix	129
Figure 3-36 Barcode – Advanced – Ctrl Translation	131
Figure 3-37 Barcode – Advanced – Scancode Enable/Disable	133
Figure 3-38 Barcode – Advanced Processing – No Code ID	134
Figure 3-39 Barcode – Advanced Processing – Strip Code ID	135
Figure 3-40 Barcode – Advanced Processing – EAN128 Barcodes	135
Figure 3-41 Stylus - Double-Tap	137
Figure 3-42 Stylus - Calibrate	137
Figure 3-43 System - General	138
Figure 3-44 System - Memory	139
Figure 3-45 System - Device Name	140
Figure 3-46 System - Copyrights	140
Figure 3-47 Volume & Sounds	141
Figure 3-48 ActiveSync Connection Settings on a Windows PC	146
Figure 3-49 LXE Login Utility User Prompt	158
Figure 3-50 Enter / Select Login Name	159
Figure 3-51 Odyssey Client Screen	159
Figure 3-52 Enter the Odyssey Client Username Password	160
Figure 3-53 Odyssey Client Password Screen Cancelled	160
Figure 3-54 Avalanche Enabler Opening Screen	165
Figure 3-55 Avalanche Enabler Connection Options	168
Figure 3-56 Avalanche Enabler Execution Options (Dimmed)	169
Figure 3-57 Avalanche Enabler Server Contact Options	170
Figure 3-58 Avalanche Enabler Startup / Shutdown Options	171
Figure 3-59 Avalanche Enabler Scan Config Option	172
Figure 3-60 Avalanche Enabler Window Display Options	172
Figure 3-61 Avalanche Enabler Application Shortcuts	173
Figure 3-62 Avalanche Enabler Adapters Options - Network	174
Figure 3-63 Avalanche Network Profile Displayed	175
Figure 3-64 Manual Settings Properties Panels	176
Figure 3-65 Status Display	177
Figure 3-66 eXpress Scan Desktop Icon	178
Figure 3-67 eXpress Scan Password Input	178
Figure 3-68 Scan Barcode 1	179
Figure 3-69 Scan Remaining Barcodes	179
Figure 3-70 Configuring Settings	180
Figure 4-1 Scanner Control Panels	184
Figure 4-2 Scanner Control Panels	186
Figure 4-3 Scanner Control / Main	187
Figure 4-4 Scanner Control / COM1	188
Figure 4-5 Scanner Control / Barcode tab	189
Figure 4-6 Barcode Tab / Symbology Settings	192
Figure 4-7 Symbology / Strip Leading / Trailing	194
Figure 4-8 Symbology / Barcode Data Match List	195
Figure 4-9 Symbology / Prefix and Suffix Control	197
Figure 4-10 Barcode Tab / Ctrl Char Mapping	198
Figure 4-11 Barcode Tab / Custom Identifiers	200
Figure 4-12 Vibration Tab	205
Figure 5-1 Summit Client Utility (SCU) Tabs	208
Figure 5-2 Summit Client Utility – Main tab	210
Figure 5-3 Main tab – Enter Admin Password	211

Figure 5-4 Summit Client Utility – Config / Profile tab	212
Figure 5-5 SCU - Scan	213
Figure 5-6 Summit Client Utility – Status tab	217
Figure 5-7 Summit Client Utility – Diags tab	218
Figure 5-8 Summit Client Utility – Global Settings tab	220
Figure 5-9 Sign-On Screen	226
Figure 5-10 Choose Certificate	228
Figure 5-11 Configure a Summit Profile with No Security	229
Figure 5-12 WEP Keys	230
Figure 5-13 Configure a Summit Profile with LEAP w/o WPA	231
Figure 5-14 LEAP Credentials Dialog	232
Figure 5-15 Configure a Summit Profile for EAP-FAST	233
Figure 5-16 Summit EAP-FAST Credentials	234
Figure 5-17 Configure a Summit Profile with PEAP/MSCHAP	235
Figure 5-18 PEAP/MSCHAP Credentials Dialog	236
Figure 5-19 Configure a Summit Profile with LEAP w/ WPA TKIP	237
Figure 5-20 LEAP Credentials Dialog	237
Figure 5-21 Configure a Summit Profile with WPA PSK Encryption	238
Figure 5-22 PSK Entry Dialog	238
Figure 5-23 Configure a Summit Profile with PEAP/GTC	239
Figure 5-24 PEAP/GTC Credentials Dialog	240
Figure 5-25 Configure a Summit Profile with EAP-TLS	241
Figure 5-26 EAP-TLS Credentials Dialog	242
Figure 5-27 Odyssey Client Screens – Settings	243
Figure 5-28 Odyssey Client Screens – Commands	244
Figure 5-29 Odyssey Client Screens – Tools	245
Figure 5-30 Odyssey Client Screens – Help	245
Figure 5-31 Funk Odyssey Client Settings Menu	246
Figure 5-32 Add Network Wizard Screen	247
Figure 5-33 Set Encryption Mode to None	247
Figure 5-34 Set Encryption Mode to WEP	248
Figure 5-35 Setting Static WEP Keys	249
Figure 5-36 Funk Odyssey Client Settings Menu	250
Figure 5-37 Add Network Wizard Screen	250
Figure 5-38 Set Encryption Mode to LEAP	251
Figure 5-39 EAP-LEAP Method	251
Figure 5-40 Create Username and Password Method	252
Figure 5-41 Enter Password for LEAP	252
Figure 5-42 Funk Odyssey Client Settings Menu	253
Figure 5-43 Tap Add to Configure a Profile	253
Figure 5-44 Add Network Wizard Screen	254
Figure 5-45 Set Association Mode to WPA	254
Figure 5-46 Select Method	255
Figure 5-47 User Name for Phase 1 Authentication	255
Figure 5-48 Select EAP-MS-CHAP-V2	256
Figure 5-49 User Name and Password for Phase 2 Authentication	256
Figure 5-50 Connect to New Profile	257
Figure 5-51 Validate Server Certificate	258
Figure 5-52 PEAP/GTC Authentication Configuration	259
Figure 5-53 User Name for Outer Authentication	259
Figure 5-54 Choose Correct Version of PEAP	260
Figure 5-55 EAP-PEAP Credential Choice	260
Figure 5-56 Prompt for Password	261
Figure 5-57 Enter the Profile Password	261
Figure 5-58 Authentication is Successful	262
Figure 5-59 Validate Server Certificate for PEAP/GTC	263

Figure 5-60 EAP-LEAP Method	264
Figure 5-61 Create Username and Password Method.....	264
Figure 5-62 Enter Password for EAP-LEAP	265
Figure 5-63 Install User Certificate	266
Figure 5-64 Install Private Key for Certificate	267
Figure 5-65 Enter Password for Private Key	267
Figure 5-66 Verify User Certificate	268
Figure 5-67 Authenticate a User	269
Figure 5-68 Completed Network Configuration	269
Figure 5-69 Choose the New Profile	270
Figure 5-70 Status is open and authenticated.....	270
Figure 5-71 Settings – Detailed Status Menu Option	271
Figure 5-72 Detailed Status is Displayed – Signal, Authentication, Encryption	271
Figure 5-73 Enable the “Validate server certificate” Checkbox	272
Figure 5-74 Enter Name of Network	273
Figure 5-75 Set the Association Mode to WPA.....	273
Figure 5-76 Connect the MX7 and the AP	274
Figure 5-77 Settings – Trusted Servers Menu Option	275
Figure 5-78 Select a Trusted Root CA.....	275
Figure 5-79 Configuring a Trusted Server Certificate	276
Figure 5-80 Logon to Certificate Authority	277
Figure 5-81 Certificate Services Welcome Screen	277
Figure 5-82 Select Encoding Method before Downloading	278
Figure 5-83 Download CA Certificate Screen.....	278
Figure 5-84 Certificate Stores	279
Figure 5-85 Import the Certificate	279
Figure 5-86 Browse to the Certificate Location on the MX7	280
Figure 5-87 Logon to Certificate Authority	281
Figure 5-88 Certificate Services Welcome Screen	281
Figure 5-89 Request a Certificate Screen	282
Figure 5-90 Advanced Certificate Request Screen	282
Figure 5-91 Advanced Certificate Details	283
Figure 5-92 Script Warnings.....	284
Figure 5-93 Script Warnings.....	284
Figure 5-94 Certificate Issued.....	284
Figure 5-95 Certificate Download Security Warning	285
Figure 5-96 Certificates	286
Figure 5-97 Import Certificate	286
Figure 5-98 Browsing to Certificate Location	287
Figure 5-99 Certificate Listing.....	287
Figure 5-100 Private Key Not Present.....	288
Figure 5-101 Browsing to Private Key Location	288
Figure 5-102 Private Key Present.....	289
Figure 5-103 802.11g WiFi Configuration Utility Menus - Status, CCX, RSSI	290
Figure 5-104 802.11g WiFi Configuration Utility Menus - Conf, About, Save&Exit	291
Figure 6-1 AppLock Screens	297
Figure 6-2 Switchpad Menu.....	300
Figure 6-3 Application Panel – Multi-Application	301
Figure 6-4 Application Launch Options	303
Figure 6-5 Security Panel – Multi-Application.....	306
Figure 6-6 Status Panel – Multi-Application	307

Chapter 1 Introduction

Overview

The LXE® MX7 is a rugged, portable, hand-held Microsoft® Windows® CE 5.0 equipped mobile computer capable of wireless data communications. The mobile device can transmit information using an 802.11 network card and it can store information for later transmission through an RS-232 or USB port.

The mobile device is vertically oriented and features backlighting for the display. The touchscreen display supports graphic features and Windows icons that the Windows CE 5.0 operating system supports. Keypads are available in 55-key alphanumeric and 32-key numeric-alpha versions. Also available is an IBM 5250 55-key keypad overlay.

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. The MX7 Cold Storage (MX7CS) mobile device functions normally in various temperature ranges. A trigger handle is available as an accessory.

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

The MX7 is powered by a 2200 mAh Lithium-Ion main battery pack and an internal NiCd backup battery. The MX7 Bluetooth® module supports LXE Bluetooth printers and scanners.

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”.



Related Manuals

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

- SE824, SE955 and SE1524 scanner barcode reading parameters, refer to Chapter 2 in the “Integrated Scanner Programming Guide”. Note: The SE955 scanner replaced the SE824 scanner on all MX7’s manufactured after July 2006.
- Intermec EV15 linear imager, refer to Chapter 3 in the “Integrated Scanner Programming Guide”.
- HHP 5380SF 2D imager, refer to Chapter 4 in the “Integrated Scanner Programming Guide”.

MX7 Multicharger User’s Guide – contains user, technical and troubleshooting information for the MX7 battery multi-charger.

MX7 Cradle Reference Guide – contains user, technical and troubleshooting information for the MX7 Cradles.

Features



New features affect user interaction and internal operation of the MX7.

The appropriate wireless utility for your device configuration has been pre-installed by LXE. The desktop will display an *Odyssey Client Utility* icon or it will display a *Summit Client Utility* icon for 802.11 configuration and security.

New features affect user interaction and internal operation of the MX7.

The appropriate wireless utility for your device configuration has been pre-installed by LXE.

The desktop will display an *Odyssey Client Utility* icon or it will display a *Summit Client Utility* icon for 802.11 configuration and security.

	Odyssey 	Summit 	Optional?
Summit® Client Utility	-	x	No
Odyssey® Client Utility	x	-	No
Bluetooth® Printers and Scanners	-	x	Yes
400MHz	x	x	No
128MB RAM	x	x	No
128MB Flash	x	x	No
SE955 Laser Scanner	-	x	Yes
EV-15 Linear Imager	x	x	Yes
SE824 Laser Scanner	x	-	Yes
5380SF 2D Imager	-	x	Yes
Windows® CE 5.0	x	x	No
Wavelink Avalanche® Enabler	x	x	Yes
Voice	-	x	Yes
RFTerm®	x	x	Yes
JAVA®	x	x	Yes
AppLock	x	x	Yes
MX7 Cold Storage (MX7CS)	x	x	No

*Note: The LXE Login Utility should be used by Odyssey Clients **only**.*

The MX7 does not have a Bluetooth managed LED.

The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates **or** an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates.


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 MX7 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 MX7 to conserve the main battery and recharge the backup battery.
- When a new battery is installed in the MX7 for the first time (or when the backup battery is completely depleted), the Time and Date reverts to its default values.

Tap  | **Settings** | **Control Panel** | **Date/Time** tab.

Note: Power drain increases substantially in Turbo mode ( | Settings | Control Panel | Power).

See Also: Section titled MX7 Cold Storage in Chapter 2 Physical Description and Layout.

When to Use This Guide

As the reference for LXE's MX7 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 MX7, 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 MX7.

Operation and safety instructions for the general user are contained in the “MX7 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 MX7 components, controls and connectors. Also describes the external power supplies and vehicle mounting options for the MX7.

Chapter 3 “System Configuration” takes you through the CE 5.0 operating system setup and the MX7 file structure. Also describes and explains initial ActiveSync processes, MX7 specific utilities, Avalanche Enabler and the LXE Login Utility.

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 keypress sequences for the keypad. Custom Keymapping instruction is included.

Appendix B “Technical Specifications” lists MX7 technical specifications.

Appendix C “Reference Material” contains parameter programming charts. It also contains the Single Application AppLock information and instruction.

Document Conventions

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

Components

Front

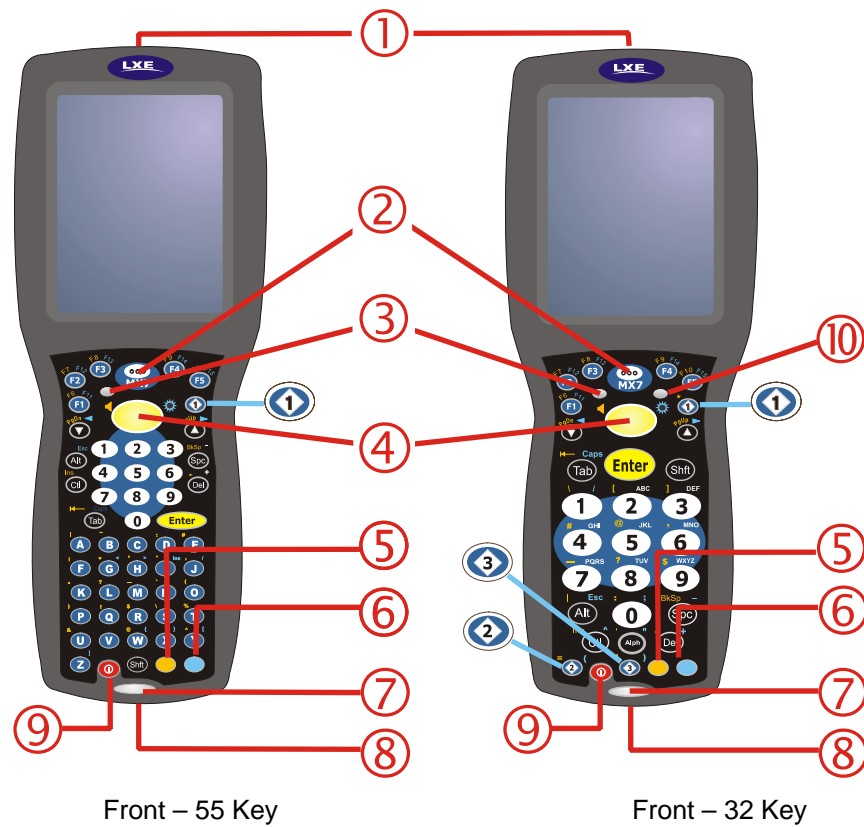



Figure 1-1 Front of MX7

- 1 Scanner/Imager 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” Lock LED
-  Diamond Number Keys

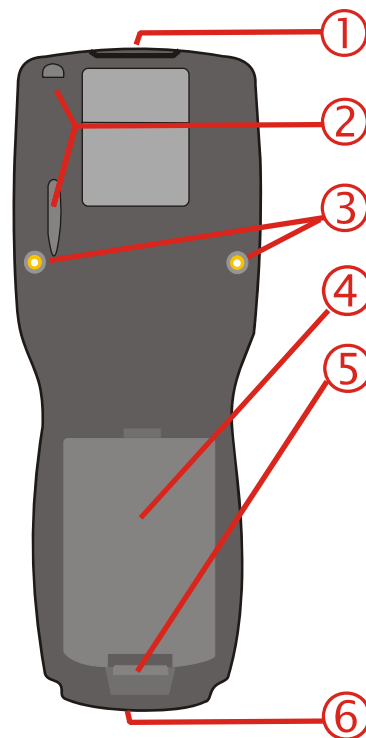
Back

Figure 1-2 Back

1	Scanner/Imager Aperture	4	Main Battery
2	Stylus and Stylus Pocket	5	Battery Fastener
3	Trigger Handle Attach Points	6	Cable Port

Scanner / Imager Aperture

CAUTION: *Never stare directly into the beam aperture. Read the previous section “Laser Warnings and Labels” before using the scanner/imager.*



Figure 1-3 Beam Aperture

Identify the type of integrated imager or laser scanner installed in the MX7 by looking at the type of plastic lens covering the Beam aperture.

- The laser barcode scanner has a red lens protecting the laser engine.
- The No-Scanner option has an opaque lens protecting the MX7 internal components.
- 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.

Continuous Scan Mode

If Continuous Scan Mode has been enabled (default is disabled), the laser is always on and decoding. Refer to *Chapter 4 Scanner*. **Caution:** Laser beam is emitted continuously. Do not stare into the laser beam.

AC Adapter



AC Adapter



AC Power Cable



Figure 1-4 AC Adapter

The LXE-approved AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

I/O Port and Cables

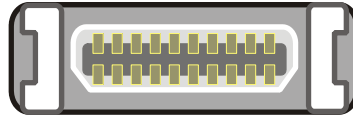


Figure 1-5 I/O Port

Cable: Multipurpose RS-232 and Power

MX7A055MULTICBLDA9F



Cable: Multipurpose USB and Power

MX7A052MULTICBLUSB



Adapter/Cable : Audio

MX7A060ADPTCBLVOICE



Adapter: RS-232 PC port to D9 male

MX7A058ADPTCBLPER



I/O Port Cables

Note: Tethered scanners connected to the MX7 I/O port are not supported by LXE. Tethered scanners connected to the MX7 Cradle I/O ports are supported by LXE.

Handle and Handstrap

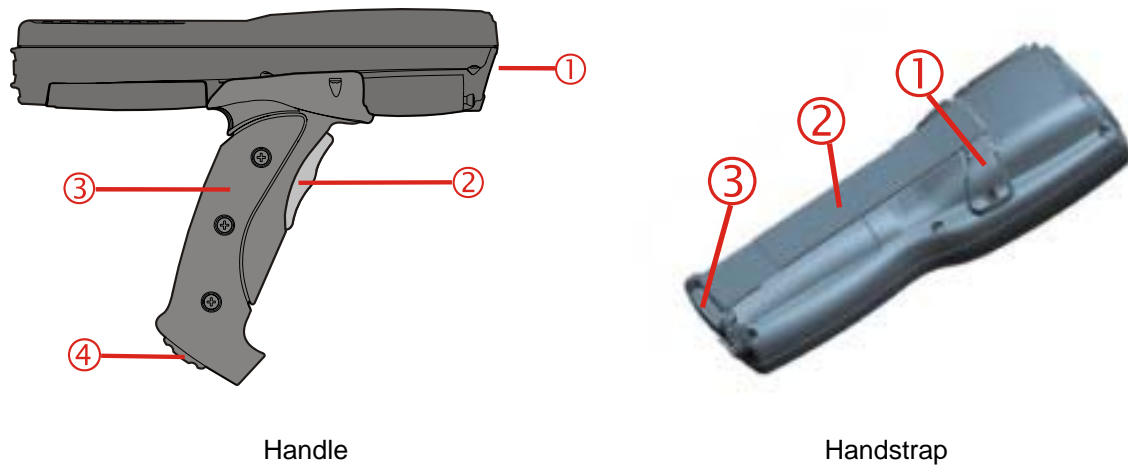


Figure 1-6 Handle and Handstrap

- | | | | |
|---|-------------------------|---|----------------------------|
| 1 | Imager/Scanner Aperture | 1 | Handstrap Retainer Bracket |
| 2 | Trigger | 2 | Handstrap |
| 3 | Handle | 3 | Handstrap Clip |
| 4 | Tether Attach Point | | |

Note: Either the trigger handle is attached to the MX7 or the handstrap is attached, not both. LXE recommends that, in the absence of a trigger handle, the handstrap be used at all times.

LXE pre-installs the handstrap when the MX7 is purchased without a trigger handle.

Quick Start

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

This section's instructions are based on the assumption that your new system is pre-configured and requires only accessory installation (e.g. handstrap) 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, MX7, 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 MX7 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. Client device 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.




MX7 with Odyssey Client



MX7 with Summit Client

Figure 1-7 MX7 Desktop

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

Troubleshooting

Can't calibrate the touch screen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts User access to running programs. Changes or modifications require Administrator access. Refer to "Chapter 6 – AppLock" for setup and processing information.
RFTerm opens and runs upon each cold reset and warm reset.	Tap File Exit to close the RFTerm application.
The Login utility waits for a login name before the MX7 can continue. For devices with an Odyssey Client only.	If the LXE Login Utility has been installed, a login screen is presented to the user after a return from Suspend, a warm reset and a cold reset. Type the login name and tap OK to continue. Tap Cancel to use the previously entered user name. Refer to Chapter 3 "System Configuration", section titled "LXE Login Utility."
MX7 seems to lockup as soon as it is warmbooted.	There may be small delays while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the MX7 startup completes, and Bluetooth relationships establish or re-establish.

Entering the Multi AppLock Activation Key

See Also: Chapter 6 "AppLock".

Hotkey (Activation hotkey)

If the mobile device uses LXE's Multi AppLock to allow the user to switch between 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)

Note: Either the trigger handle is attached to the MX7 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 MX7 can be purchased with a customer-installable trigger handle. The handle is shipped with a wrist strap. The handle enables the user of the MX7 to hold the mobile device comfortably while pointing and activating the scanner / imager with one hand. With the handle installed, the MX7 can balance on a tabletop supported by the nose of the mobile device and the bottom of the handle.

Pressing the trigger on the handle activates the laser scanner / imager. The trigger performs the same function as the Scan key on the keypad. With the handle installed the Scan key on the keypad remains active.

The handle is built of a durable and flexible plastic with a rubber grip that will not detach from the MX7 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. The trigger handle does not contain a battery pack.

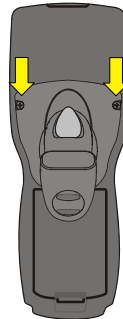


Figure 1-8 Trigger Handle Attach Points

Handle Installation

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

1. Place the MX7, 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 MX7 (as shown above) with the two screws provided.
6. Torque the Pan Head Screws to 3 ± 1 in/lb ($.34\pm .11$ N/m).
7. Test the handle's connection making sure the MX7 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 MX7 is placed in service.

Inserting the Main Battery

Press the Power key after the battery is inserted into the MX7.

Note: On first use the MX7 batteries should be charged with an external power source (i.e. AC Adapter) – 3.5 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 four hours in an LXE Multi-Charger.



Figure 1-9 Main Battery Pack


The MX7 Battery Compartment is located at the bottom of the back of the computer. The battery case serves as the back cover for the battery well for the MX7.

Place the battery in the battery well, making sure the tab on the bottom of the battery pack fits into the slot at the bottom end of the battery well. Push the battery down into the battery well until the tab clicks into place and the battery pack is secure in the battery well.

The backup battery is trickle-charged by the main battery. Whenever possible, use the AC power adapter with the MX7 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 MX7 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 MX7:

100% capacity	2200 mAh minimum
80% capacity	1760 mAh minimum

Deciding when to put a fully charged main battery pack in the MX7 is difficult to quantify because it is very application specific. 1800 mAh may be the cutoff for one customer who uses the mobile device frequently, while 1000 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.

Note: The battery should not be replaced in a dirty, harsh or hazardous environment. When the battery is out of the MX7, any dust or moisture that enters the battery compartment can get into the main unit, potentially causing damage.

Installing the Handstrap

Note: The handstrap cannot be used/installed when the MX7 has the trigger handle installed at the same time.

An elastic hand strap is available for the MX7. Once installed, the hand strap 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: Slide the bottom bracket out and away from the MX7 when replacing the main battery pack.



Figure 1-10 MX7 With Handstrap Installed

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

Installation

1. Place the MX7, with the screen facing down, on a flat stable surface.
2. Attach the handstrap retainer bracket to the MX7 with the screws provided.
3. Slip the Handstrap Clip into the bracket at the base of the MX7.
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 strap over so that the closed loop fastener surfaces mate evenly.
6. Test the strap's connection making sure the MX7 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 MX7 is placed into service again.

Periodically check the handstrap for wear and the connection for tightness. If the handstrap gets worn or damaged, it must be replaced.

Connecting an External Power Supply (Optional)

The MX7 receives AC/DC power from the AC/DC 12V Power Supply. The MX7 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 MX7 follow the steps below in sequence.

1. Plug the 3 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 MX7 power cable connector into the MX7 port until it clicks. The click means the connector is seated firmly.
3. Press the power cable connector pin from the power adapter into the connector on the (USB/Power or RS-232/Power) cable attached to the base of the MX7. AC power is now being supplied to the MX7.

The System LED above the Scan key illuminates when the MX7 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 MX7 to conserve the main battery power and maintain a charge in the backup battery.

Assembling the AC Power Adapter

The LXE-approved AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

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



Figure 1-11 AC/DC 12V External Power Supply

Plug the 3-prong cable into an AC wall outlet. Firmly press the female end of the power cable into the male connector on the power adapter. AC power is now being supplied to the power adapter.

Connecting the Multipurpose USB / Power Cable



Figure 1-12 Connect the USB / Power Cable to the MX7 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 MX7. Release the clips in the connector cable. Test the connection for stability before connecting the B or C connector.
- Connector B Plug the 3-prong cable into an AC wall outlet. Firmly push the power cable connector pin into connector B until you hear a slight click.
- 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

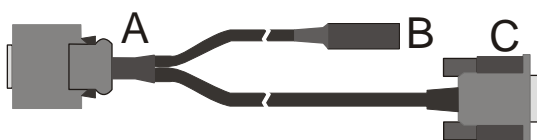


Figure 1-13 Connect the RS-232 / Power Cable to the MX7 Port

- 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 MX7. Release the clips in the connector cable. Test the connection for stability before connecting the B or C connector.
- Connector B Plug the 3-prong cable into an AC wall outlet. Firmly push the power cable connector pin into connector B until you hear a slight click.
- 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 MX7 is securely connected to the serial device.

Connecting to a Printer Interface Cable



Figure 1-14 Connect to a Printer Interface Cable

- 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 MX7. Release the clips in the connector cable. Test the connection for stability before connecting the B or C connector.
- Connector B Align the RS-232 serial cable end carefully to the serial port on the cable from the printer. Press the ends together and hand tighten the screws on either side of the serial cable until it is securely connected to the printer cable.

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 MX7. Use the control panel option “Mixer” to set up mono or stereo headphones. The Summit Client supports mono only.



Figure 1-15 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 MX7. Release the clips in the connector cable. Test the connection for stability before connecting the B connector.
- Connector B Align Connector B 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.

Entering Data

Data is entered into the MX7 by speaking into the headset’s microphone when prompted.

Please contact your System Administrator if assistance is needed with the voice software installed on your MX7.

Power Key

Note: Refer to the section titled “Power Modes” later in this guide for information relating to the power states of the MX7.

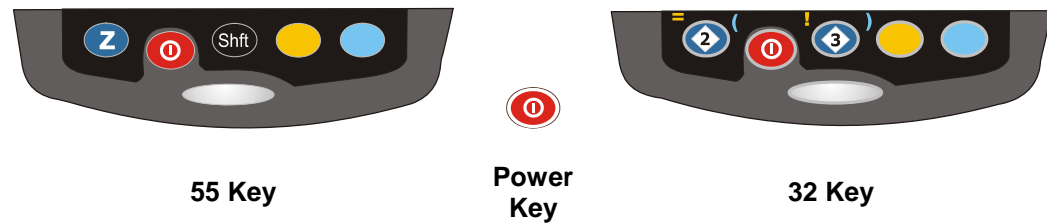


Figure 1-16 Power Key Location

The Power key is located at the bottom of the keypad. When a battery is inserted in the MX7 for the first time press the Power key.

Tapping the Power key places the MX7 immediately in Suspend mode. Tapping the Power key again immediately releases the MX7 from Suspend Mode.

Or

Tap  | **Suspend**.

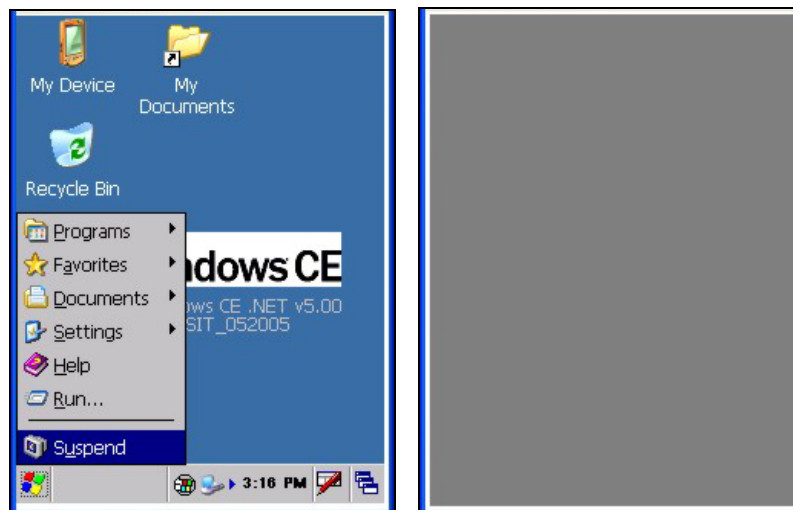


Figure 1-17 Enter Suspend Mode – Press Enter

Please refer to the section titled “Power Key” in Chapter 2 for Reboot options and instruction. See section “LED Indicators” and “System Status LED” later in this guide.

Tapping the Touchscreen with a Stylus

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

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. Place the stylus into the stylus holder on the MX7 when the stylus is not in use.

Like using a mouse to left-click icons on a laptop/desktop computer screen, using the stylus to tap icons on the MX7 display 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.
- Press Shift and an Arrow key to select several files.
- Once you’ve selected a file, press Alt then press Enter to open its Properties dialog.
- Press Del to delete a file.
- To force the Start menu to display, press Ctl and release, press Blue and release, then press Esc (the Alt key).

A stylus replacement kit containing 10 stylus’ can be ordered from LXE. See the section titled “Accessories” for the stylus replacement kit part number.

Software Setup

Touchscreen Calibration

Note: The first time it is used, the MX7 automatically runs the touchscreen calibration program.

If the MX7 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 Cold Reset, the MX7 resets Date and Time to the factory default values.

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.

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 MX7.

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


The first option affects the MX7 when it is running on battery power only. The second option affects the MX7 when it is running on external power (e.g. AC adapter).

The default value for the battery power timer is 5 seconds. The default value for the external power timer is “never” and the checkbox is blank. **The backlight will remain on all the time when both checkboxes are blank.**

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

Set the MX7 Power Schemes Timers

Note: Refer to the section titled “Power Modes” later in this guide for information relating to the power states of the MX7.

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 MX7 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 MX7 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 1-18 Speaker Location

The speaker is located on the front of the device above the MX7 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.

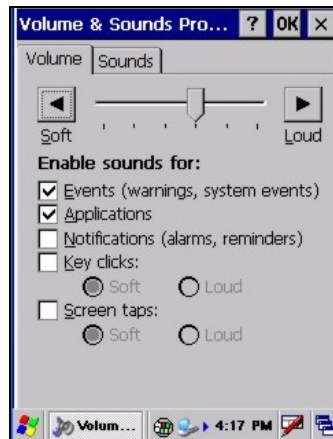


Figure 1-19 Volume & Sounds Properties

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 MX7 LXEbook to the MX7 (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 "MX7 User's Guide" on the LXE Manuals CD.

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

MX7	Windows CE PDF Viewer (pre-installed).
-----	--

First, using your desktop computer download "LXEbook – MX7 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 MX7 to your PC.

When the MX7 and the desktop ActiveSync applications are synchronized, tap Explore on the ActiveSync menu on your PC to display the contents of the MX7 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 MX7.

When the file copy process is finished, disconnect the MX7 from the synchronization equipment and close ActiveSync.

To view the LXEbook on the MX7, select Start / Programs / Microsoft File Viewers / Microsoft PDF Viewer / File / Open. Locate the LXEbook on the MX7 and "open" the file.

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

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 IS 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 MX7 may use either the Funk Odyssey Client or the Summit Client Utility to configure the network card.

When the MX7 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	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.
--	--

Access:  | [Settings](#) | [Control Panel](#) | [Certificates](#)

Prerequisites:

- The MX7 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 reset. For example, the internal flash folder.

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 MX7 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.

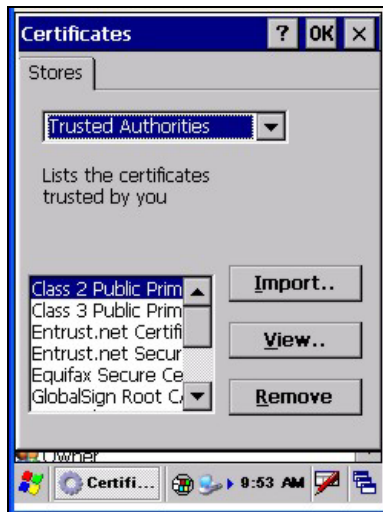


Figure 1-20 Certificate | Stores

Private Key

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

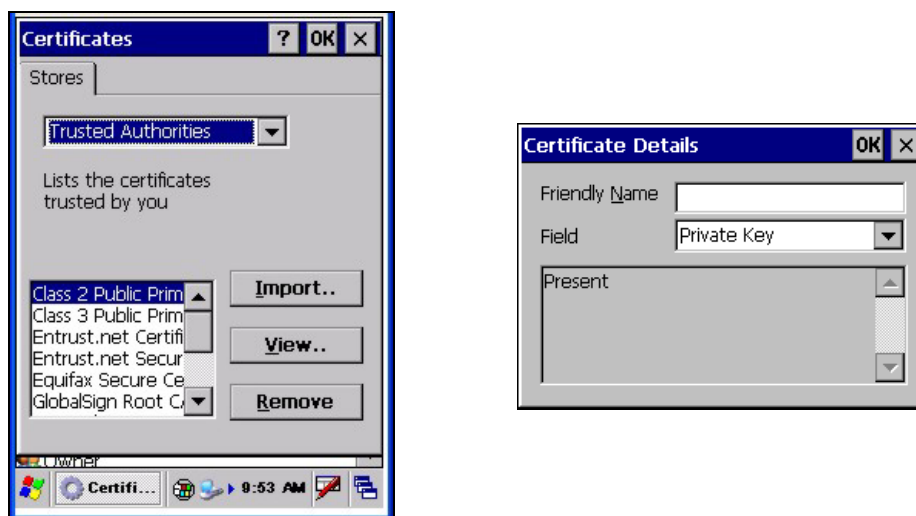


Figure 1-21 View Certificate Details

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

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

The MX7 default Bluetooth hardware setting is Enabled. Bluetooth is an option and may not be available on all devices. The MX7 does not have a Bluetooth managed LED.

The LXE MX7 *Bluetooth®* module is designed to Discover and pair with nearby LXE Bluetooth devices. Non-LXE Bluetooth devices may be discovered but are inaccessible as they are filtered out on the Bluetooth Devices panel and are not displayed.

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.

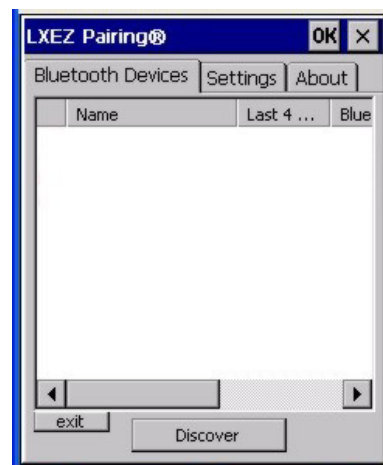


Figure 1-22 Bluetooth Devices Display – Before Discovering Devices

The Bluetooth remote device should be as close as possible, and in direct line of sight, with the MX7 during the pairing process.

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 MX7 default name is determined by the LXE factory installed software version. LXE strongly urges assigning every MX7 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the 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 MX7, 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 MX7. When the Bluetooth devices are disconnected, the device icon has a red background.

Report when connection lost

A dialog box appears on the MX7 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 MX7 display notifying the user a connection between one (or all) of the previously-paired Bluetooth devices is complete. This option is disabled by default.

Tap 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 MX7 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.

Tap 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 MX7 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 MX7 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 MX7 screen notifying the user a Bluetooth device requests to pair with the MX7. This option is disabled by default.

The requesting Bluetooth device does not need to have been Discovered by the MX7 before the pairing request is received.

Tap 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 MX7 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. Tap the Bluetooth Devices tab, if necessary.
2. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
3. The discovered devices are listed in the Bluetooth Devices window.
4. Doubletap a Bluetooth device in the Discovered window to open the Bluetooth device properties menu.
5. Tap Pair as Scanner to set up the MX7 to receive scanner data.
6. Tap Pair as Printer to set up the MX7 to send data to the printer.
7. If paired, tap Disconnect to stop pairing with the device. Tap Delete to remove the device name and data from the MX7 Bluetooth Devices list. Tap OK.
8. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX7 display.
9. Whenever the MX7 returns from Suspend Mode, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the MX7. If the devices cannot connect to the MX7 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 MX7. The System Administrator has also enabled / disabled Bluetooth settings and assigned a Computer Friendly Name for each MX7. See *Chapter 3 System Configuration, Bluetooth control panel applet* and supported Bluetooth printers and scanners.

The Bluetooth taskbar Icon state changes as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the MX7. The MX7 does not have a Bluetooth managed LED.

Taskbar Icon	Legend
	Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
	<p>MX7 is not connected to any Bluetooth device.</p> <p>MX7 is ready to connect with any Bluetooth device.</p> <p>MX7 is out of range of all paired Bluetooth device(s). Connection is inactive.</p>

Note: When an active paired device, not the MX7, enters Suspend Mode, is turned Off or leaves the MX7 Bluetooth scan range, the Bluetooth connection between the paired device and the MX7 is lost. There may be audible or visual signals as paired devices disconnect from the MX7. The Bluetooth remote device should be as close as possible, in direct line of sight, with the MX7 during the pairing process.

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 MX7 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 MX7 using Bluetooth functions.

- The MX7 must have the Bluetooth hardware and software installed. An MX7 operating system upgrade may be required. Contact your LXE representative for details.
- If the MX7 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 MX7 batteries are fully charged. Alternatively, the MX7 may be in a powered cradle or 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 1-23 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 MX7.

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

Important: The MX7 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.

MX7 with Label

If the MX7 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the MX7, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the MX7 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. Tap and hold the stylus on the Bluetooth scanner until the right-mouse-click menu appears.
6. Select Pair as Scanner to pair the MX7 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 MX7 Bluetooth label, if there is no beep and no LED flash from the remote Bluetooth device, the devices are currently paired.

MX7 without Label

If the MX7 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the MX7:

First, locate the MX7 Bluetooth address by tapping Start | Settings | Control Panel | Bluetooth | About tab.

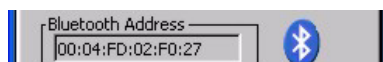


Figure 1-24 About tab and Bluetooth Address

Next, create a Bluetooth address barcode label for the MX7 ¹.

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 MX7 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 MX7 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

Bluetooth Beep and LED Indications

Beep Type from Bluetooth Device	Behavior
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

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

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

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

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the MX7 during the pairing process.

1. Open the LXEZ Pairing Panel (Start | Settings | Control Panel | Bluetooth).
2. Tap Discover. Locate the Bluetooth printer in the discovery panel.
3. Tap and hold the stylus (or doubletap) on the Bluetooth printer until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the MX7 with the Bluetooth managed printer.

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

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

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the MX7 and the printer are currently paired.

Entering Data

You can enter data into the MX7 through several different methods. The scan 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 touchscreen 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 MX7 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 keypresses 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 1-25 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 MX7 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 MX7 for daily use. The touch screen should be calibrated before initial use.

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

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

The stylus can be used in conjunction with the keyboard and Scan button 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 / imager.

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

Using the Integrated Barcode Scanner or Imager

Use the integrated laser scanner to scan linear barcodes.

Use the 5380SF integrated imager to scan 2D barcodes.

Barcode 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 scan aperture towards a barcode and press the Scan button. You will see a red beam strike the barcode. Align the beam so that the barcode is centered within the beam. The laser beam must cross the entire barcode. Move the MX7 towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.

There may be a tactile response combined with the Scan functions.

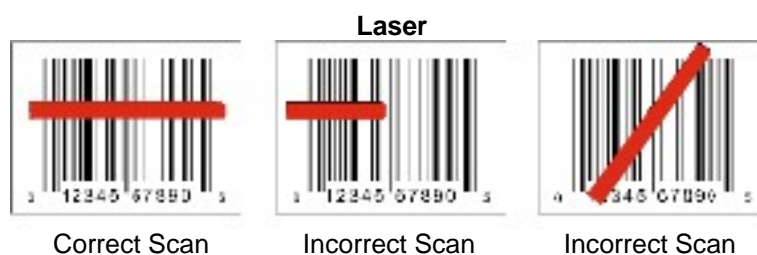


Figure 1-26 Laser Scanner Beam on Linear Barcode

2D Imager



Figure 1-27 Imager Bracketed Crosshair Target on 2D Barcode

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

Move the MX7 towards or away from the barcode until a response is received by the MX7 (beep, tactile response, etc) or the bracketed crosshair times out and disappears.

Scan Status LED



Figure 1-28 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 MX7 beeps or vibrates, indicating a successful scan. If the scan was unsuccessful, 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 successful or unsuccessful read. The scanner / imager is ready to scan again after the Scan key (or trigger on the handle if installed) is released, or after the Scan Status LED turns off following a successful scan.

The Scan Status LED turns amber when scanner/imager programming changes, if any, are being saved. When the LED is off, the MX7 is ready to scan again.

Tethered Scanners

Tethered scanners cabled to the MX7 I/O port are not supported by LXE. Tethered scanners cabled to the MX7 **Cradle** I/O port are supported by LXE, see “MX7 Cradle Reference Guide” for instruction.

Bluetooth Scanners and Printers

Note: Barcode manipulation parameters in Chapter 4 - Scanner are applied to the incoming data resulting from successful barcode scans sent to the MX7 for processing.

Bluetooth scanners are paired to the MX7 wirelessly using the MX7 Bluetooth wireless client. The MX7 does not have a Bluetooth LED.

See previous section *Bluetooth* for more information.




Only LXE Bluetooth scanners and LXE Bluetooth printers are supported by LXE. See *Accessories*.

Voice Data

Data is entered into the MX7 by speaking into the headset's microphone when prompted. Please contact your System Administrator if assistance is needed with the voice software.


Saving Changes to the Registry

The MX7 saves the registry when you:

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

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

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

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

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

MX7 User’s Guide – English
 MX7 User’s Guide – German
 MX7 Cradle Reference Guide
 MX7 Multi-Charger / Analyzer User’s Guide
 LXEbook – MX7 User’s Guide (download to mobile device)
 RFTerm Reference Guide
 LXE Security Primer
 CE API Programmers Guide
 Integrated Scanner Programming 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.

MX7 Mobile Device

MX7 Main Battery , Lithium Ion	R	MX7A380BATT
MX7 Main Battery, Lithium Ion (for Cold Storage MX7CS)	R	MX7A381BATT
5 Unit Main Battery Charger (US power cord), Includes analyzing capabilities	R	MX7A385CHGR5US
5 Unit Main Battery Charger (no power cord), Includes analyzing capabilities	R	MX7A386CHGR5WW
Replacement MX7 Hand Strap	R	MX7A401HANDSTRAP
Carry case for MX7 with no handle, includes shoulder strap	R	MX7A4132CASENHDL
Carry case for MX7 with handle, includes shoulder strap	R	MX7A414CASEHDL
MX7 Voice Application case with belt	R	MX7A404CASEVRNHDL
MX7 Padded handle with rubber overmold and two finger trigger, includes wrist strap	R	MX7A406HANDLE
Holster for MX7 with handle, belt not included	R	MX7A405HOLSTERHDL
Holster for MX7 without handle, belt not included	R	MX7A407HOLSTERNHDL
Holster for MX7 with handle and boot, belt not included	R	MX7A410HLSTRWHDLBOOT
Holster for MX7 without handle, with boot, belt not included	R	MX7A409HOLSTERWBOOT
Holster belt	R	9200L67
Black rubber protective boot , do not use with Desktop Cradle.	R	MX7A488PROTBOOT
Yellow rubber protective boot , do not use with Desktop Cradle.	R	MX7A489PROTBOOTYEL
Carry case for MX7 with Gearkeeper retractor	R	MX7A408RETRACTORCASE
Carry case for MX7 with handle. (For use with Gearkeeper retractor – MX7A412RETRACTORWBLT).	R	MX7A411RTRCORCASEHDL

Gearkeeper retractor with belt. (For use with Carry case for MX7 with handle – MX7A411RTRCORCASEHDL)	R	MX7A412RETRACTORWBLT
MX7 Charge/Comm Interface Cable , USB Client for ActiveSync	R	MX7A052MULTICBLUSB
MX7 Charge/Comm Interface Cable , RS-232 Serial ActiveSync, D9 Female	R	MX7A055MULTICBLDA9F
AC/DC power supply with US power cord for use with MX7 Charge/Comm cables	R	9000A319PSACUS
AC/DC power supply without power cord for use with MX7 Charge/Comm cables	R	9000A302PSACWW
RS-232 Serial Adapter cable , 6in, for use with printers that provide their own source of power.	R	MX7A058ADPTCBLPER
MX7 Headset coiled adapter cable , includes quick disconnect headset connector. A headset is still required.	R	MX7A060ADPTCBLVOICE
MX7 Replacement Stylus , 10-pack	R	MX7A584STYLUS
Large tethered stylus which fit the MX7 carry cases, 5 pack	R	9000A507STYLUS
CD with CE 5.0 API's and LXE API's with documentation for custom application development	R	MX7A504CE50SDK
Touch screen anti-glare anti-reflective protective film , 10 pack	R	MX7A584PROTFILM
Voice Recognition and Headsets		
VoxBrowser™ English and Americas		VOXBROWSER ENG
VoxBrowser™ Rest-of-the-World		VOXBROWSER ROW
Single ear, single headband, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A501SNGBHEADSET
Single ear, dual headband, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A502DUALBHEADSET
Dual ear, behind the head, headset with noise canceling microphone, includes 5 replacement windscreens	R	HX1A503BTHHEADSET
Replacement foam block for 502 dual band headsets, qty 1	R	HX1A504AHSBLOCKFOAM
Replacement head yoke for dual band 502 headset, qty 1	R	HX1A505DUALYOKE
Replacement head yoke for single band 501 headset, qty 1	R	HX1A506SINGLEYOKE
Replacement windscreen for all headset microphones, 10 Pack	R	HX1A508WINDSCREEN10
Replacement windscreen for all headset microphones, 50 Pack	R	HX1A509WINDSCREEN50
Replacement foam ear piece cover for 501 and 502 headsets, 10 pack	R	HX1A510FOAMEAR10
Replacement foam ear piece cover for 501 and 502 headsets, 50 pack	R	HX1A511FOAMEAR50
*** Contact your LXE representative for Voice Recognition and Headset availability.		

Mobile Bluetooth Barcode Readers

LXE Bluetooth Ring Scanner module with laser ring scanner, battery, two hand/wrist straps (large and small)	R	8651A100BTLASERKIT
LXE Bluetooth Ring Scanner module with 1D/2D imager ring scanner, battery, two hand/wrist straps (large and small)	R	8652A100BTIMAGERKIT
Li-Ion Spare Battery for LXE Bluetooth Ring Scanner Module	R	8650A376BTBOHBATTERY
LXE Bluetooth Ring Scanner 8-bay battery charger with US power cord	R	8650A377BTBOHCHGRUS
LXE Bluetooth Ring Scanner single-bay charger with US wall plug	R	8651A379SINGLECHGRUS
PowerScan 7000BT Scanner RS-232 with pointer	R	8700A301SCNRBTSRI
PowerScan 7000BT Base Station, RS232, without universal power supply.	R	8700A501BASERS232
PowerScan 7000BT Base Station Power Supply, Std US, 120V	R	8700A502PSACUS
PowerScan 7000BT, RS232 Cable for Base Station, DB9S, Coil, 8'	R	8700A001CBL8DA9F
PowerScan 7000BT Battery Charger with Power Supply, Four Station, US Std	R	8700A503CHGR4US
PowerScan 7000BT Battery Pack	R	8700A504BATT
Bluetooth Standard Range Fuzzy Logic laser	R	8810A326SCNRBTfZ
Bluetooth Auto Range LORAX laser	R	8820A327SCNRBTfR
Spare battery	R	8800A376BATTERY
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	R	8800A051POWERCORD
Single Slot Universal Battery Charger adapter cup for 8800 Battery	R	8800A377CHGRADPTRCUP
Single slot battery charger with International power supply	R	8800A378CHGR1SLOT
Universal Battery charger 4-Slot Base. Power Supply included, no AC power cord.	R	8800A379CHGRBASE
LS3408 Scanner Holster for Belt	R	8200A501HOLSTRBELT
Mounted Take Up Reel (Mounted applications)	R	8000A501INDREEL
Auto Sense Intellistand, Hands Free Scanning	R	8500A505STANDSMT
CBL ASSY, DA9F, 9ft (cradle to terminal)	R	8500A051CBL9DA9F
Desk Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	R	8800A001CRADLERCMI
Desk Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	R	8800A002CRADLECMI
Forklift Cradle, Radio/Charging, Multi-Interface (requires data cable and power supply)	R	8800A003CRADLEVRCMI
Forklift Cradle, Charge Only, Multi-Interface (requires data cable and power supply)	R	8800A004CRADLEVRCMI
US AC Power Cord (use with 8800A301ACPS and 8800A379CHGRBASE)	R	8800A051POWERCORD
Universal Desktop Power Supply 90-264VAC, 9VDC, 2A, EPS	R	8800A301ACPS
9-60VDC Forklift Power Supply (For Use with Forklift Cradles)	R	8800A302DCPS
Power Cable: Connects DC Power Supply to Forklift Cradle	R	8800A052DCPWRCABLE
Forklift Rugged Scanner Holder with RAM mount (all metal with cloth padding)	R	8800A005STAND

MX7 Cradles

Cradle Power Supply , AC/DC, US, with power cord	R	9000A321PSACUS
Cradle Power Supply , AC/DC, WW, without power cord	R	9000A322PSACWW
Cradle , Desktop with spare battery charging	R	MX7A388DESKCRADLEWW
MX7 Passive vehicle cradle . Does not support charging or communication. U-Bracket kit included.	R	MX7A007VMCRADLE
RAM mount kit for MX7 Passive Vehicle Bracket. This kit does NOT include the Cradle. Attaches to U-Bracket.	R	MX7A001RAMBRKT
MX7 Main Battery , Lithium Ion	R	MX7A380BATT
Black rubber protective boot , designed for Desktop Cradle use.	R	MX7A490PROTBOOTBLK
Yellow rubber protective boot , designed for Desktop Cradle use.	R	MX7A491PROTBOOTYEL
MX7 Charge/Comm Interface Cable , USB Client for ActiveSync	R	MX7A052MULTICBLUSB
MX7 Charge/Comm Interface Cable , RS-232 Serial ActiveSync, D9 Female	R	MX7A055MULTICBLDA9F
RS-232 Serial Adapter Cable , 6 in., for use with printers that provide their own source of power	R	MX7A058ADPTCBLPER
MX7 Headset coiled adapter cable, includes quick disconnect headset connector. A headset is still required.	R	MX7A060ADPTCBLVOICE
MX7 Base Plate Kit	R	MX7A586RPLCENDPLATE
Tethered Scanners (Cradle connection only)		
Scanner, Powerscan SR, 8' Cbl, WW	R	8300A326SCNRPWRSR8DA9F
Scanner, Powerscan SR, 12' Cbl, US	-	8300A327SCNRPWRSR12DA9F
Scanner, Powerscan LR, 8' Cbl, WW	R	8310A326SCNRPWRLR8DA9F
Scanner, Powerscan LR, 12' Cbl, US	R	8310A327SCNRPWRLR12DA9F
Scanner, Powerscan XLR, 8' Cbl, WW	R	8320A326SCNRPWRXLR8DA9F
Scanner, Powerscan XLR, 12' Cbl, US	-	8320A327SCNRPWRXLR12DA9F
Scanner, LS3408ER, 9' Cbl, US See Note	R	8520A326SCNRERDA9F
Scanner, LS3408FZ, Fuzzy Logic, 9' Cbl, US	R	8510A326SCNRFZYDA9F

Chapter 2 Physical Description and Layout

Hardware Configuration

System Hardware

The MX7 hardware configuration is shown in the following figure.

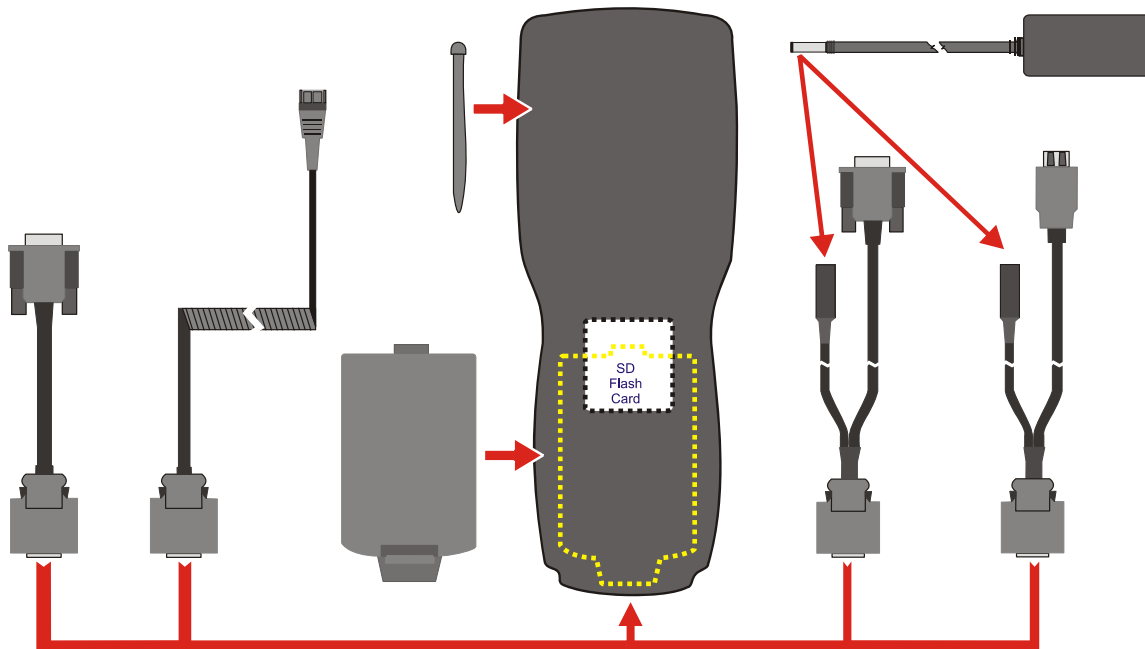


Figure 2-1 System Hardware

Central Processing Unit

The LXE MX7 CPU is a 400MHz Intel Xscale PXA255 CPU. The operating system is Microsoft Windows CE 5.0. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

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

Core Logic

The MX7 supports the following I/O components of the core logic:

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

System Memory

The 400MHz CPU configuration supports 128MB SDRAM, 128MB SD card.

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


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

Internal SD Memory Card

The MX7 has one SD card interface for storage of operating system and program code, as well as persistent storage. The SD slot is accessible from the battery compartment and ships with an LXE-qualified 128MB SD Flash card. Larger capacity flash cards are available from LXE, see Accessories.

The internal SD flash card supports a FAT file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface. Operating system files are hidden on this drive with a terminal unique identifier in the internal flash, to prevent them being accidentally erased by a user. In addition, the registry hive files are stored on this device. At least 32MB of Flash is available for customer use.

Video Subsystem

The touchscreen is a 3.5" (8.9 cm) diagonal viewing area, ¼ VGA 320 by 240 pixel TFT Reflective 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 MX7 uses two batteries for operation.

Main Battery Pack

A replaceable 2200 mAh Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while in the MX7 when the mobile device is connected to the MX7 optional external AC/DC power source. The main battery pack can be removed from the MX7 and inserted in the MX7 Multi-Charger which simultaneously charges up to five battery packs in four 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 6 hours when it is in an MX7 connected to AC power and 3.5 hours when it is in the MX7 multicharger.

Backup Battery

An internal 50mAh Nickel Cadmium (NiCad) backup battery. The backup battery is recharged directly by the MX7 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.

Client Ports

Three ports are available on the MX7.

802.11b/g

The MX7 supports an LXE 802.11b/g network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Adjusting power management on the network card is set to static dynamic control.

WEP, WPA and LEAP are supported. Refer to "Chapter 5 Wireless Network Configuration".

COM Port

The MX7 has one mini D 20-pin serial port (a multifunction I/O port) that can be configured by the user.

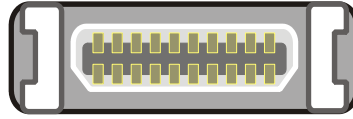


Figure 2-2 COM1 Port

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 “Cable, Multipurpose RS-232 and Power” and “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 multipurpose RS-232/Power cable is connected.

External AC power is not available for the “Adapter, RS-232 terminal port to D9 male” option. Power is drawn from the main battery pack when this adapter is connected..

USB Client Port

The MX7 has one USB Client port for ActiveSync applications. An accessory USB cable, “Cable, Multipurpose USB and Power” is available to connect the MX7 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 Connection

An audio headset interface is available using the “Adapter, Audio” accessory with the I/O port. The connection cable connects the MX7 to a Voxware quick disconnect 4-pin interface. This cable adapts to specific styles of headsets for voice input, stereo or mono output. The MX7 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 MX7 COM port turns off audio output to the MX7 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 not 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 Window's CE operating system. The speaker is located on the front of the MX7, above the MX7 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 MX7 has one integrated barcode scanner/imager port. Only one scan engine is installed at a time. Scan engines are not “hot swappable”. The MX7 may have one of three Symbol laser scan engines:

- Symbol SE824-I000A (see Note)
- Symbol SE955-I000WR
- Symbol SE1524

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 MX7 is depressed or when the trigger on an installed trigger handle is depressed. A control panel applet (Start | Settings | Control Panel | Scanner) is available to set scanner/imager options.

Functionality of the integrated scan engine driver is based on the driver version installed in the MX7. Functions may include audible tones on good scan (at the maximum db supported by the speaker), failed scan, LED indication of a scan in progress, among other functions. If enabled, a vibration device provides a tactile response on a good scan event.



Please refer to the “Integrated Scanner Programming Guide” for instruction on configuring specific scanner/imager parameters by using the MX7 to scan engine-specific setup barcodes in the guide.

See Also: Chapter 4 “Scanner”.

Note: The SE 955 scanner replaced the SE 824 scanner on all MX7’s manufactured after July 2006.

Bluetooth LXEZ Pairing

The MX7 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 MX7. However, the MX7 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX7 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 MX7 does not have a Bluetooth managed LED.
- The LED on the Bluetooth scanner illuminates during a scanning operation; the Scan LED on the MX7 does not illuminate.
- Barcode data captured by the Bluetooth scanner is manipulated by the settings in the MX7 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 MX7 during final barcode data manipulation.

Physical Controls

Power Key

Note: Refer to the section titled “Power Modes” for information relating to the power states of the MX7.

The power key is located next to the < Z > key on the 55-key keypad and next to the <Diamond 2> key on the 32-key keypad. When a main battery pack is inserted in the MX7 for the first time, the Power key must be pressed.

Quickly tapping the Power key places the MX7 immediately in Suspend mode. Quickly tapping the Power key again, pressing any key, pressing the trigger (on the trigger handle), or tapping the touchscreen, immediately returns the MX7 from Suspend.

The System LED blinks green when the video display is Off.

Note: The unit will suspend on AC power and when connected through ActiveSync. Remember to set the suspend timers before using ActiveSync.

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 reboot. Application and control panel applet changes are saved when OK is tapped on an application applet.

The Process


The MX7 reloads the operating system upon every warm boot or cold boot. Anything not saved or preserved to the registry is lost.

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

During cold boot, the system behavior is identical to warm boot with the addition that the registry is reloaded with factory defaults.


Warm Reset

Hold down the Power key for 15 seconds until the display blanks, then release the key. A warm reset does not affect the operating system but data in SDRAM is lost. Data saved to the SD card is not lost. Network connection will need to be re-established.

Or, using the input panel, you can tap  | **Run** and type WARMBOOT ². Tap the OK button.

Cold Reset

Important:-- Because of the extreme nature of the Cold Reset, LXE recommends that the Cold Reset be used only as an emergency procedure and the Warm Reset be used whenever necessary.

Tap  | **Run** and type COLDBOOT ¹. Tap the OK button to coldboot the MX7. The default settings are restored when the device powers on again. Calibrating the touchscreen will need to be performed when the cold boot process is complete.

² This command filename is not case-sensitive.

Flash Cards

Note: When removing or installing SD cards, protect the MX7 internal components from electrostatic discharge.

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

The SD flash card under the main battery pack is intended to store program CAB files, MX7 utilities, the registry and the registry backup information.

The internal SD flash card supports a FAT file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface. Operating system files are hidden on this drive with a terminal unique identifier in the internal flash, to prevent them being accidentally erased by a user. In addition, the registry hive files will be stored on this device.



Figure 2-3 Flash Card Location

Note: As there is no card management software loaded on the MX7, LXE recommends purchasing preformatted Flash cards from LXE as the cards have been tested and qualified for use by the MX7 (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 MX7.

The MX7 has one internal SD Flash card port.

The network drivers are stored on the card in the SD slot (under the main battery pack). During the boot process, the bootloader loads the operating system, the client driver and any saved parameters.

Flash Card Installation / 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 MX7 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 MX7 into Suspend Mode. Disconnect the AC adapter from the MX7.
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 flash 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 reset. *Always perform a warm reset when exchanging one Flash card for another.*

Removal

1. Place the MX7 into Suspend Mode. Disconnect the AC adapter from the MX7.
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

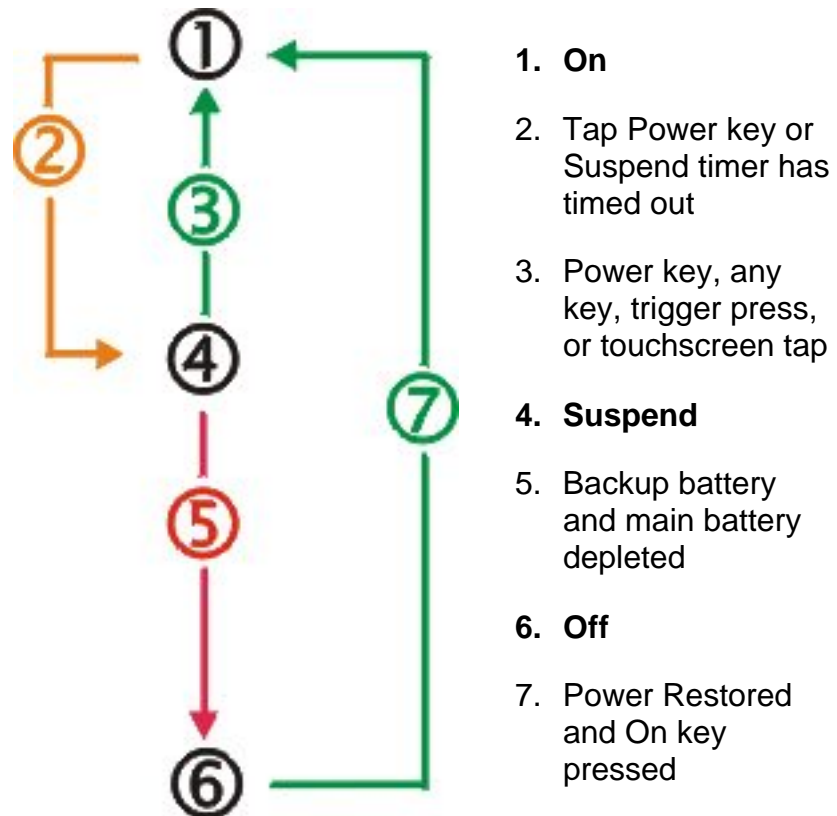


Figure 2-4 Power Modes – On, Suspend and Off

Primary Events Listing

Any key on the keypad	COM1 activity
Stylus touch on the touchscreen	External power connection
Power button tap	USB client connection
Scanner activity	Bluetooth device reconnect / disconnect message

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

The MX7

After a new MX7 has been received, a charged main battery inserted, and the Power key tapped, the MX7 is always On until both batteries are drained completely of power.

When the main battery and backup battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged main battery is inserted or external power is applied and the Power key is pressed.

Suspend Mode

The MX7

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

MX7 Suspend timers are set using  | **Settings** | **Control Panel** | **Power** | **Schemes tab**.

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

- Any key on the keypad
- Stylus touch on the touchscreen
- Handle trigger press
- Connecting to AC power supply
- Power button tap
- Bluetooth device reconnect / disconnect message

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

The MX7 should be placed in Suspend mode before hotswapping 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 MX7 On.

The Keypads

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

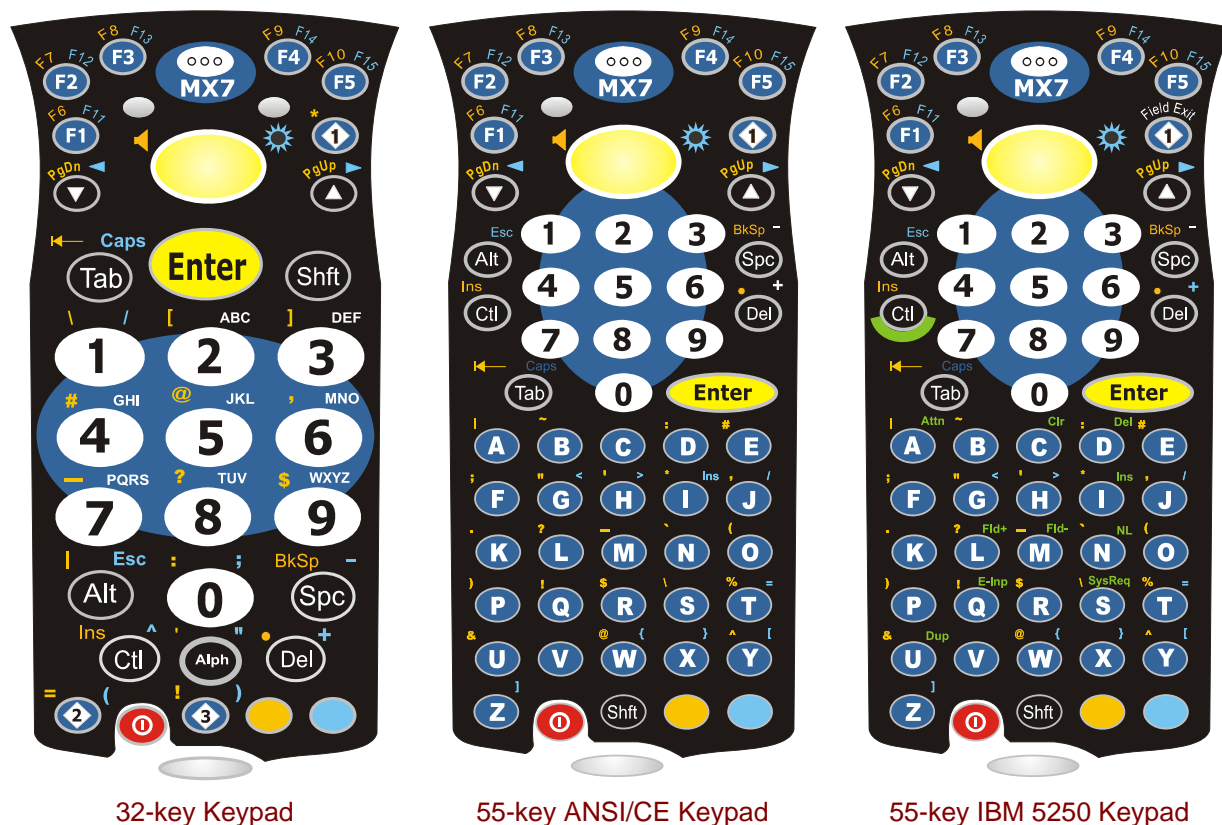


Figure 2-5 The 32-key and 55-key Keypads

See also: Appendix A “Key Maps”.

Using the 55 Key ANSI / CE Keypad

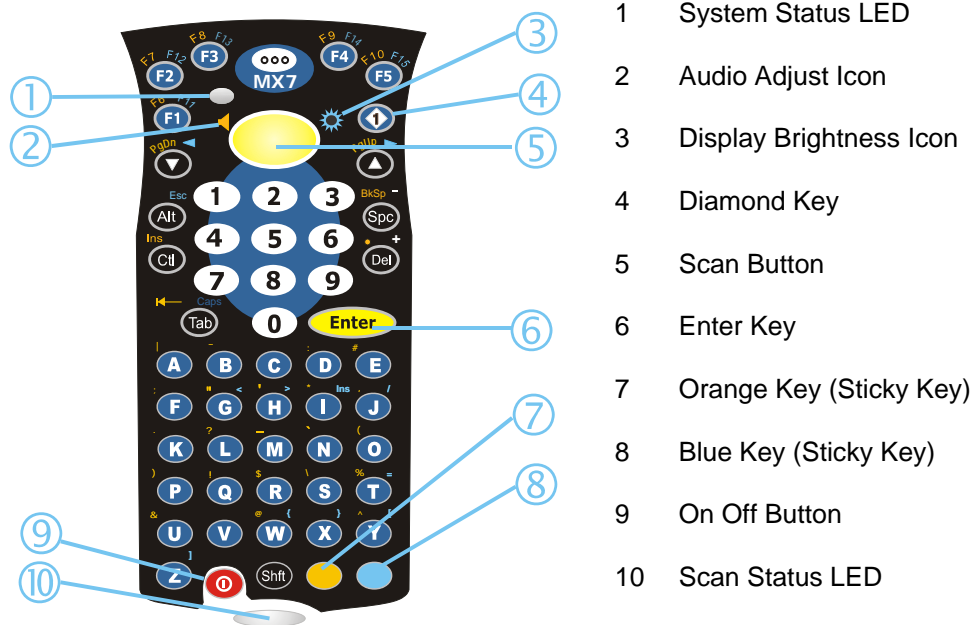


Figure 2-6 The ANSI / Batch Keypad

- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Alphabetic keys default to lower case letters. Press the Shift key, then the alphabetic key for an uppercase letter.
- When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence.

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

Using the 32-Key Numeric-Alpha Keypad

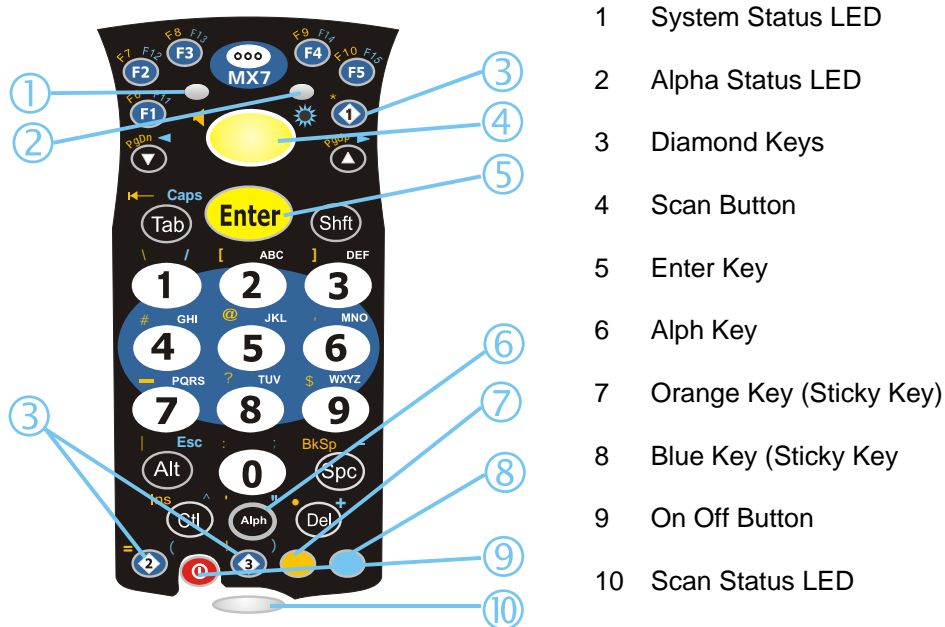


Figure 2-7 The 32-Key Keypad

- 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.

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 wanted 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).

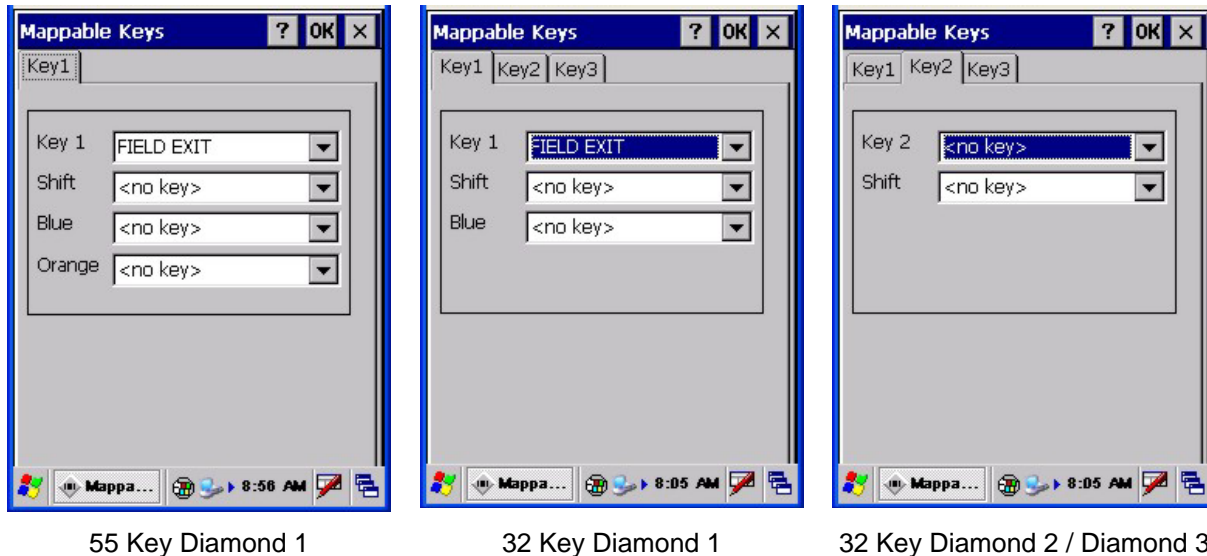



Figure 2-8 Mappable Diamond Keys

The Diamond 1 key always defaults to Field Exit on all keypads. The Diamond 1 key defaults to Field Exit on both keypads. 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.

55 Key Keypad












The user can program the following key combinations using the Diamond 1 key:

	 + 	 + 	 + 
e.g. ESC (Blue+Alt)	e.g. Home (Shft+Down Arrow)	e.g. BackTab (Orange+Tab)	e.g. Insert (Blue+I)

Any combination of “standard” keypresses can be used.

32 Key Keypad

The user can program the following key combinations using the Diamond keys:

 user defined without using a sticky key	 + 	asterisk (*)	 + 
 user defined without using a sticky key	 + 	equal sign (=)	open parenthesis (
 user defined without using a sticky key	 + 	exclamation mark (!)	closed parenthesis)

LED Indicators

See “Appendix A – Key Maps” for instruction on the specific keypresses to access all keypad functions. The MX7 does not have a Bluetooth managed LED.

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 . . .	Comment
Blinking Red	Power Fail	Replace the main battery with a fully charged main battery. Or Connect MX7 to external AC power then replace the main battery with a fully charged main battery.
Steady Red	Main Battery Low	Replace the main battery with a fully charged main battery.
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 MX7 keypad.

When the Scan Status LED is . . .	The Status is . . .
Steady Green	Good Scan
Steady Red	Scan in Progress
No Color	Scanner/Imager ready for use.

Alpha Mode (32-key Alph Key)

The Alpha Mode LED is located below the <F4> key on the 32-key keypad.

LED functions outlined in previous sections titled “System Status LED” and “Scanner LED” are the same for the 32-key mobile device.

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 keypress (as defined by Windows CE) with the exception of the Shift, Alt and Ctrl/Ctl keys.
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-keypress combinations with one finger.

Ctl / Ctrl (Control key)



A Control sticky keypress 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 keypress 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 keypress ends a sticky key function. The Shft key enables the shifted functions of the keypad. This function is similar to a regular keyboard’s Shift key. Note that the Shift key only stays active for one keystroke. Each time you need to use a Shifted function, you need to press the Shft key before pressing the desired key.

When the Shft 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.

Orange and Blue Keys



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.

Orange Key

Tap the Orange key to enter “orange” mode. Tap it again to cancel “orange” mode.

If you were in “blue” mode before you pressed the Orange key, blue mode is cancelled and you enter Orange mode.

Blue Key

Tap the Blue key to enter “blue” mode. Tap it again to cancel “blue” mode.

If you were in “orange” mode before you pressed the Blue key, orange mode is cancelled and you enter Blue mode.

Field Exit

A square icon with a blue border, containing a white circle with a blue number '1' inside. The words 'Field Exit' are written in a curved path above the circle.	<p>IBM 5250 specific keypad only. The Diamond 1 key can be programmed as a Field Exit key. The Field Exit key is used to exit an input field. If the field is an Auto Enter field, the auto transmit function is activated. Refer to the “Mappable Diamond Keys” section for instruction.</p>
A square icon with a black border, containing a white circle with a green 'Ctl' inside. A green highlight is visible around the circle.	<p>IBM 5250 specific keypad only. A Control sticky keypress 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 key before pressing the desired key.</p> <p>Note the green highlight on the Control key and the 5250 commands highlighted in green on the 5250 keypad overlay.</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.

55-Key Keypad

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

Visual Cue: A Capital A is displayed in the taskbar when the device is in CapsLock mode or the Caps Key has been pressed and the next key (to be capitalized) has not been pressed.

32-Key Keypad

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 Display



Figure 2-9 Touchscreen Display

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. 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 turned off.

The default value for the battery power timer is 3 seconds. The default value for the external power timer is “never” and the checkbox is blank.

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”, section titled “Quick Start.”

The keypad backlight can be synchronized with the display backlight activity.

Cleaning the Display and Scan Aperture

If there is a static screen protector installed on the MX7 display, 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 MX7 display are available from LXE (see “Accessories”).


Power Supply

The MX7 computer is designed to work with a Lithium-Ion (Li-ion) battery from LXE. Under normal conditions it 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 MX7 maintains the date and time for a minimum of two days using a main battery that has reached the Low Warning point and a fully charged backup battery. The MX7 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 four hours in an LXE Multi-Charger and six hours when the MX7 is connected to external power.

Checking Battery Status

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

Note: Power drain increases substantially in Turbo mode.

MX7 Status LED and the Batteries

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 MX7 to external AC power then replace the main battery with a fully charged main battery.
Steady Red	Main Battery Low	Low Battery Warning. Replace the main battery with a fully charged main battery.
No Color	Good	No user intervention required.


Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the LXE Multi-Charger or the MX7 unit.

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 it 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 or Very Low ( | **Settings** | **Control Panel** | **Power** | **Battery** tab) connect the AC adapter to the MX7 before replacing the main battery pack.

When the main battery power level is low, the MX7 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 MX7 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 MX7 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 MX7 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 client is reestablishing a network link.

If the backup battery depletes before a fully charged main battery can be inserted, the MX7 will turn Off.

Full operational recovery from Suspend can take several seconds while the wireless client connects to the network, authorization for Voxtel-enabled applications complete, Wavelink Avalanche management of the MX7 startup completes, and Bluetooth relationships establish or re-establish.

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 MX7 has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times comes from the MX7 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 MX7, its features and any operating applications.

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

Discharging

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

Handling Batteries Safely

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



Caution Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.

NiCd and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

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.

MX7 Multi-Charger (Optional)

The multi-charger requires an external power source before battery pack charging / analyzing can commence. The battery pack begins to recharge as soon as it is placed in the battery well. There are five Charging wells. The well closest to the overlay can be used to analyze the main battery pack in the well.

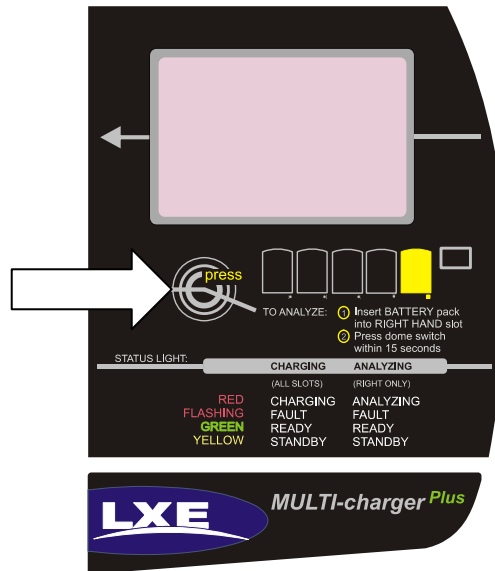


Figure 2-10 LCD Panel and Dome Switch

Pressing the dome switch within three minutes begins the Analyze – Discharge – Charge cycle on the battery pack in the Charge/Analyze well.

The external AC power supply cable connection for the Multi-charger is shipped with the multi-charger.

The main battery pack can be charged in either 1) a powered MX7 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. The retaining clip on the battery pack snaps the battery into place in the battery well. Remove the battery pack by depressing the retaining clip and 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.



Please refer to the “MX7 Multi-Charger User’s Guide” for instruction.

See Also: *Section titled MX7 Cold Storage later in this chapter.*

Multi-Charger Indicators

LED Functions

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

LCD Messages

LCD Indicator	Function	Description
ANALYZE	Analyzing the Battery	Battery pack cycling through Charge, Discharge, Charge.
CHARGE	Charge	Battery pack charging.
DISCHARGE	Discharge	Battery pack discharging.
BAT. FAULT	Battery Fault	Battery pack fault or failure.
READY	Analysis Complete	Battery pack analyzed and ready for use with displayed capacity.
XXXX mAh	Display Capacity	Capacity measured during discharge cycle.
XX VDC	Display volts	Battery volts measured during charge and discharge cycle.

MX7 Cradles (Optional)

MX7 docking cradles restrain the MX7, re-charge batteries, and enable serial, audio or USB communication with a PC, scanner, printer or other peripheral device. MX7 keypad data entries can be mixed with cradle-tethered scanner barcode data entries while the MX7 is in a powered cradle. Bluetooth device connection and use, while the MX7 is docked, are managed by the MX7 Control Panel Bluetooth program, not the cradle.

Using a wall AC adapter the desktop cradle can also recharge a spare MX7 battery in approximately 4 hours. The MX7 battery recharging is managed by the docked MX7 power management configuration. The MX7 can be either On or in Suspend Mode while in the cradles. The MX7 Vehicle Mount cradles do not have spare battery charging capabilities. Special purpose and power cables are available from LXE®.

Wireless host/client communications can occur whether the cradles are receiving external power or not as wireless functions draw power from the main battery in the MX7.

The cradles are designed to secure an MX7 with or without a protective boot (MX7A490PROTBOOTBLK or MX7A491PROTBOOTYEL), a handstrap and/or a trigger handle.

[The MX7 Desktop Cradle](#) requires external power before battery charging and tethered scanning can commence. The cradle can charge both the main battery in the docked MX7 and a spare main battery at the same time.

[The Powered Vehicle Cradle](#) requires an external power source before docked MX7 battery charging and tethered scanning can commence.

[The Passive Vehicle Cradle](#) does not have connectors that can accept an external power source or tethered scanner. It is designed to secure the MX7 in a vehicle.



Please refer to the *MX7 Cradle Reference* Guide for installation, technical specifications and user instruction.

MX7 Cold Storage

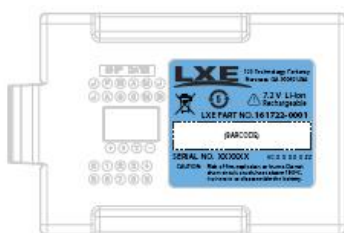
Highlights

- MX7 Cold Storage (MX7CS) battery has a blue label.
- Snowflake decal above the MX7CS keypad.
- Heating element visible on the MX7CS touchscreen and the scanner aperture.
- MX7CS cold storage battery is recharged in the MX7 Multi-charger, MX7 Desk Cradle and when in an MX7 attached to an external power source (e.g. AC adapter).

The MX7 Cold Storage is designed to operate normally when reading barcodes and moving from, and into, cold storage warehouses, freezers and vehicles where the temperatures may vary between -30°C and 5°C (-22°F and 41°F).

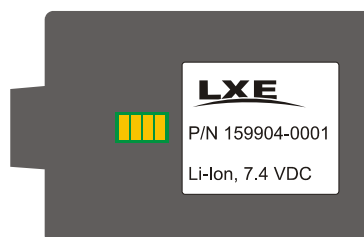
Cold Storage Battery

MX7 Cold Storage Battery Label



1250mAh

Standard MX7 Battery Label



2200mAh

There is no change in the way the Cold Storage battery is inserted into and removed from the MX7CS battery well. See section in *Quick Start* titled *Inserting Fully Charged Battery* for instruction.

MX7CS Battery Life – minimum 2.5 hours while the unit is roaming, powered on with ambient temperature -10°C (14°F) or above, Display backlight turned on, Keypad LED backlight on, radio connected to Access Point, and scanner decoding barcodes.

The LXE Li-Ion main battery (MX7A381BATT) has been designed specifically for the MX7 Cold Storage device. This battery has a blue label while the standard MX7 battery has a white (MX7A380BATT) label.

Snowflake Decal

An MX7 Cold Storage device has a snowflake decal between the touchscreen and the keypad. It is located to the left when the mobile device screen is facing forward.



Due to the heating elements overlaying the scan aperture, scanning may require the user to move the MX7CS scan aperture closer to the barcode for good scan results.

Heating Elements

Heating elements activate when ambient temperature drops below 0°C (32°F). LXE recommends using the stylus when performing screen touch functions.

There may be some condensation as the MX7CS moves in and out of cold storage areas. The condensation on the touchscreen and the scan aperture quickly dissipates.

The touchscreen heating elements and scanner aperture heating elements may be visible when the MX7 is tilted slightly. No user interaction is required to turn the heating elements on/off. Stylus taps on the touchscreen function normally.

Recharging Batteries

The Cold Storage battery pack can be recharged to full capacity while in an MX7CS connected to an external power source and also while the Cold Storage battery pack is inserted in the charging bay in a powered MX7 desk cradle. The battery pack temperature must be above 10°C (50°F) before re-charging can begin.

Battery packs in the MX7 Multi-charger begin charging when the battery pack temperature is between 10°C (50°F) and +40°C (100°F).

To charge the Cold Storage battery pack to full capacity, the MX7 Multi-charger firmware must be at V1.07 or greater. The firmware version is noted on the multi-charger label on the bottom of the device.

If your multi-charger firmware needs to be upgraded, please contact your LXE representative.

The multi-charger and AC adapter are not designed to operate in a freezer or cold storage environment. Please refer to the *MX7 Multi-charger User's Guide* for instruction and technical information.

Hot-swapping the Cold Storage Battery

The MX7CS, and a charged 2.5V SuperCap backup battery, retains data during a main battery hot-swap at -30°C (-22°F) for at least 90 seconds. The temperature of the fully charged replacement Cold Storage main battery must be +10°C (14°F), or above.

Normal Operation Temperature Ranges

- In the freezer where the temperature ranges between -30°C to -18°C (-22°F to 0°F).
- In the loading dock where temperature ranges between 0°C to 5°C (32°F to 41°F) with the relative humidity at 65%
- Moving between the freezer and a loading/unloading area where the temperature transitions from -30°C to 5°C (-22°F to 41°F)

Chapter 3 System Configuration

Introduction

There are several different aspects to the setup and configuration of the MX7. 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 MX7 may vary. The following sections provide a general reference for the configuration of the MX7 and some of its optional features.

Note: LXE recommends frequently charging the MX7 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 MX7.

This chapter's contents assumes the system administrator is familiar with Microsoft Windows CE 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 MX7 and its Windows CE environment.

Note:

The MX7 reloads the operating system upon every warm boot or cold boot. Anything not saved or preserved to the registry is lost.

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

During *cold boot*, the system behavior is identical to warm boot with the addition that the registry is erased, forcing the MX7 to reboot with factory defaults. The registry is recreated when 20 minutes of uptime elapses or upon the first save or suspend function.

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 MX7 you receive the software files required by the separate programs needed for operation and 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 MX7 are specific to the intended function of the MX7.

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

Software Load

The software loaded on the MX7 computer consists of Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer for Windows CE browser and MX7-specific utilities. The software supported by the MX7 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)

- Java executables and browser components are handled by the Java option (when installed).

Terminal Emulation

- RFTerm (VT220, TN5250, TN3270). Runs automatically at the conclusion of each reboot.

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

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

Software Applications

The following applications are included:

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

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

Software Backup

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

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 MX7 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 MX7 SDK Kit part number.

Boot Loader

The MX7 supports a proprietary boot loader. It is the responsibility of the boot loader to:

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

The MX7 reloads the OS every time during warm boot or cold boot. In Warm Boot (i.e., the user executes a Warm Boot) the OS and the CAB files are reloaded from the internal SD card and the preserved registry is also reloaded. Anything else (user data), which was not preserved in the registry, is lost. During Cold Boot (i.e., user executes a Cold Boot utility) the system behavior is identical to Warm Boot with the addition that the registry is reloaded with factory defaults.

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

Folders Copied at Startup

The following folders are copied on startup:

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

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

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

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

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

Optional Applications

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 MX7. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX7. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly Name for each MX7. The Bluetooth control panel can be accessed by tapping **Start | Settings | Control Panel | Bluetooth**, or by doubletapping the Bluetooth icon in the taskbar.

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 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

Related Manual: “Using Wavelink Avalanche on LXE Windows Computers”.

The MX7 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, the Enabler begins normal performance. The Enabler is by default 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_MX7.

LXE CE devices manufactured before October 2006 must have their drivers and system files upgraded before they can use the Avalanche Enabler functions. Please contact an LXE representative for details on upgrading the mobile device baseline.

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

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


Desktop



For general use instruction, please refer to commercially available CE user's guides or the CE on-line Help application installed with the MX7.


Note: Whenever possible, use the MX7 AC power adapter with the MX7 to conserve the main battery and to ensure the backup battery is charged.

The MX7 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 MX7 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 MX7 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 network card and Internet Service Provider – ISP enrollment is not available from LXE).
Radio Config Utility	Used when setting power management, antenna diversity and roaming profiles. LXE recommends using the defaults set by the manufacturer.
Odyssey Client	Used for configuring Funk Odyssey client for network security settings. Note that only one client can be used at a time. If the Odyssey Client is present, the Summit Client is not present.
Summit Client	Used for configuring Summit client for network security settings. Note that only one client can be used at a time. If the Summit Client is present, the Odyssey Client is not present.
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

Folder	Description	Preserved upon Reboot
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	Internal SD Flash 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**

Communication	Stores Network communication options
ActiveSync	Begin ActiveSync connection
Connect	Run this command after setting up a connection
LXConnect	Manage MX7 files using ActiveSync
Remote Display	Displays MX7 file structure on a remote desktop monitor.
Start FTP Server	Begin connection to FTP server
Stop FTP Server	Stop connection with FTP server
Microsoft File Viewers	View downloaded files (see Note)
Excel Viewer	View Excel documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word and RTF files
Command Prompt	The command line interface in a separate window
Inbox	Microsoft Outlook mail inbox
Internet Explorer	Access web pages on the world wide internet
Java	Option.
LXE RFTerm	Option. Terminal emulation application. RFTerm automatically opens as soon as a reboot is completed.
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Odyssey Client	RF client management program
Radio Config Utility	Radio management program. WZC icon in toolbar
Summit Client	RF client management program
Transcriber	Handwriting recognition program using an integrated dictionary
Wavelink Avalanche	Option. Remote management for networked devices.
Windows Explorer	File management program

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

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to 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.
- If installed, with an Odyssey Client, LXE Login Utility runs automatically at the conclusion of each reboot.

Communication

Access:  | **Programs | Communication**


Note: Some communication menu options require an external modem connection to the MX7. Modems are not available from LXE nor supported by LXE.

ActiveSync

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

After a relationship (partnership) has been established with the MX7 and a desktop computer, ActiveSync can synchronize using the network link, serial port, or USB port on the MX7.

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

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

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

Connect

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

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

The default connect setup is USB direct connect.

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

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

Remote Control

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

Equipment Required: *MX7 Multipurpose USB / Power Cable* or *Multipurpose RS-232 / Power Cable. Desktop/laptop computer.*

Remote Display is used with ActiveSync to display the contents of the MX7 file structure on a desktop/laptop computer screen. Once connected, the desktop keyboard and mouse can be used to manipulate files, data or settings on the MX7.

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

- “Initial Install | USB Connection”
- “Initial Install | Connect – Initial Install Process”
- “Explore”
- “Disconnect”

Note: Initial ActiveSync connection requires a USB connection, subsequent connections can be either USB or RS-232 serial. When the MX7 enters Suspend, an established ActiveSync connection is maintained. Refer to “ActiveSync / Get Connected Process” for full details.

1. Run ActiveSync on the desktop/laptop.
2. Connect the MX7 to the desktop computer using the USB cable. Follow the instructions on the desktop to set up a partnership (LXE recommends choosing the *No* option to set up the MX7 as a guest).
3. Select the ActiveSync menu option Explore and the file structure of the MX7 is displayed in the Mobile Device window on the desktop monitor.
4. Files on the desktop computer can be dragged to a folder on the MX7 and dropped to add them to the MX7.
5. ActiveSync converts the file to run on a CE device automatically during the transfer.
6. To close or disconnect the ActiveSync connection with the MX7, disconnect the USB connector first. ActiveSync on the desktop closes. Remote (Display) Control on the MX7 closes.

Refer to “ActiveSync / Get Connected Process” for full details.

LXEConnect

Access:  | **Programs | Communication | LXE Connect**

Equipment Required: *MX7 USB ActiveSync Cable. PC or laptop computer.*

LXE Connect is used with an ActiveSync USB connection to display the contents of the MX7 file structure on a PC/laptop screen. Once connected, the PC keyboard and mouse can be used to manipulate files, data or settings on the MX7. ActiveSync is pre-installed on the MX7.

LXEConnect is installed and run on the PC/laptop. The installation file is copied from the MX7.

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

- “Initial Install | USB Connection”
- “Initial Install | Connect – Initial Install Process”
- “Explore”
- “Disconnect”

Note: Initial ActiveSync connection requires a USB connection, subsequent connections can be either USB, wireless or RS-232 serial. Refer to “ActiveSync / Get Connected Process” for full details.

**** Cable for initial ActiveSync Configuration:**

USB Client to PC/Laptop	USB-Client cable	MX7A052MULTICBLUSB
-------------------------	------------------	--------------------

Install LXEConnect

1. If needed, install ActiveSync (version 3.8 or greater) on a PC/laptop with a USB-A port.
2. If needed, power up the MX7. Connect the Power/USB Y-cable to the base of the MX7.
3. Connect the MX7 to the PC using the USB cable. The USB-A end of the cable connects to a USB port on a desktop or laptop PC. The other end connects to the MX7 power/USB Y-cable secured to the base of the device.
4. After connection is established, the Activesync dialog box appears on the PC screen.
5. Select “No” for partnership when prompted.
6. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in *ActiveSync / Get Connected Process*.
7. Select the ActiveSync menu option Explore.
8. A Windows Explorer window is displayed for the MX7 on the PC. Browse to the MX7 \System\LXEConnect folder.
9. Select and copy the LXEConnect.msi and Setup.exe files from the MX7 to the user PC. Make a note of the location chosen for the files.
10. Close the ActiveSync explorer dialog box. Do not disconnect the ActiveSync cable.
11. Run the LXEConnect Setup.exe program that had been copied to a folder on the PC. The LXE Connect Setup Wizard program begins.
12. Follow the on-screen installation prompts. The PC default installation directory is C:\Program Files\LXE\LXEConnect.
13. When the installation is complete, create a desktop shortcut for the LXEConnect utility, if desired.
14. LXEConnect is ready to use.

Using LXEConnect

1. If an ActiveSync connection has not been established, connect the MX7 to the PC using the specified cable. See *Install LXEConnect* for instruction.
2. Doubletap the LXEConnect icon that was created on the PC desktop or doubletap the LXEConnect.exe file in the default PC installation folder: C:\Program Files\LXE\LXEConnect. If the user chose a different file location for installation, use the chosen path to locate the LXEConnect.exe file.
3. LXEConnect launches.
4. The About CERDisp box is displayed. Tap the OK button to dismiss the About CERDisp dialog box. The dialog box automatically times out after approximately 30 seconds.
5. A Windows Explorer window is displayed on the PC of the MX7 desktop.
6. Input from the PC's mouse and keyboard are recognized as if they were attached to the MX7.
7. When the remote session is complete, terminate the LXEConnect program on the PC by selecting File | Exit or tapping the X button in the upper right hand corner to close the application.
8. Disconnect the ActiveSync cable from the MX7 and the PC.

Refer to *ActiveSync / Get Connected Process* for full details when using ActiveSync on a desktop PC and the MX7.

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.

Command Prompt

Access:  | Programs | Command Prompt

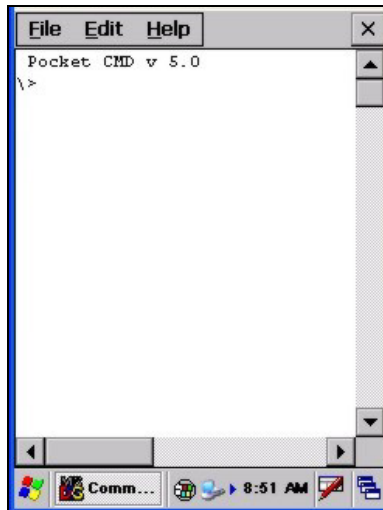


Figure 3-1 Pocket CMD Prompt Screen

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 MX7 inbox and a PC’s desktop inbox. Refer to “ActiveSync Processes” in this guide.

Internet Explorer

Access:  | Programs | Internet Explorer

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

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

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

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

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

Media Player

Access:  | **Programs | Media Player**

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

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

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

Microsoft WordPad

Access:  | **Programs | Microsoft WordPad**

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft 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.

Odyssey Client

Access:  | **Programs | Odyssey Client**

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

Disable Odyssey **Start | Programs | Odyssey Client | Settings | Disable Odyssey**

When Odyssey is disabled, the Wireless Zero Config screen is displayed. When Odyssey is disabled before Suspend mode, it is *not* re-enabled upon a return from suspend.

Enable Odyssey **Start | Programs | Odyssey Client | Settings | Enable Odyssey**

When Odyssey is disabled, selecting Enable Odyssey from the Settings menu *may* not re-enable Odyssey. Odyssey is enabled by default after every cold and warm reset.

See Chapter 5 “Wireless Network Configuration” for Odyssey client setup information and instruction.

Radio Config Utility

Access:  | **Programs | Radio Config Utility**

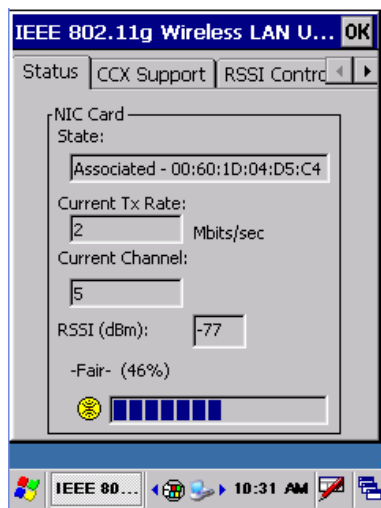


Figure 3-2 Radio Config Utility Main Menu



WiFi icon in Toolbar. Tapping the WiFi icon in the toolbar presents the Radio Config Utility Main Menu to the user. See Chapter 5 “Wireless Network Configuration”, section titled “IEEE 802.11g Wireless LAN Configuration Utility” for WiFi information and instruction.

Wireless Zero Config Utility and the Odyssey Client

This utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the application is inactive at this time.

Note: LXE recommends using the Funk Odyssey client to configure the Odyssey Client. Wireless Zero Config is not recommended for configuring the network card.

Summit Client

Access:  | **Programs | Summit**

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

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

See Chapter 5 “Wireless Network Configuration” for Summit Client Utility setup information and instruction.

Certs

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

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

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

See Chapter 5 “Wireless Network Configuration” for directions for acquiring CA and user certificate files.

Wireless Zero Config Utility and the Summit Client

This utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the application is enabled and the MX7 is not connected to a network.

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

1. Tap the Summit Client Utility icon on the desktop, or tap **Start | Programs | Summit | SCU**.
2. Select **ThirdPartyConfig** in the Active Config drop down box.
3. A message appears that a Power Cycle is required to make settings activate properly. Tap **OK** to close the message window.
4. Tap the **Power** button to place the MX7 in **Suspend**, then tap the Power button to **wake the MX7** from Suspend mode.

The Wireless Zero Config utility begins.

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

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

When the taskbar is auto hidden, press the **Ctrl** key then the **Esc** key sequence (Blue+Alt) to make the Start button appear.



Figure 3-3 Taskbar General Tab

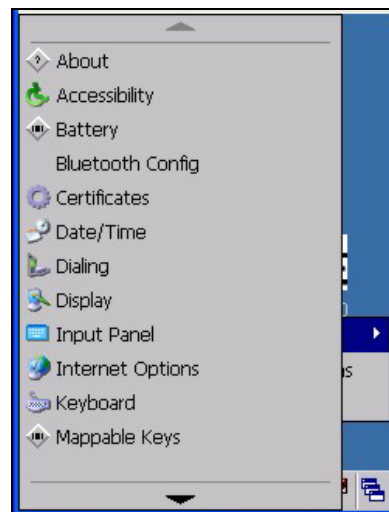
Advanced Tab

Expand Control Panel

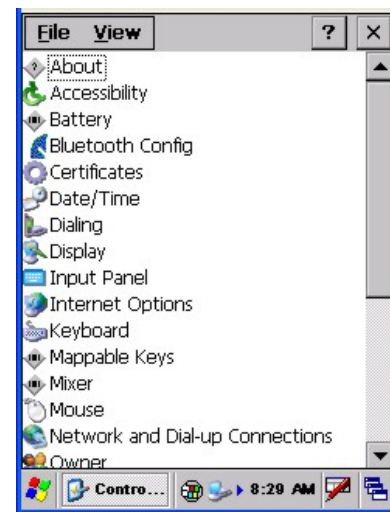
Tap the checkbox to have the Control Panel folders appear in drop down menu format from the **Settings | Control Panel** menu option. When it is unchecked, the Control Panel Properties screen is displayed.



Figure 3-4 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, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility. See Chapter 6 for details.
Battery	View voltage and status of the main and backup batteries. Battery charge and discharge is performed using this option.
Bluetooth	Discover and manage Bluetooth devices.
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Dialing	Set dialup properties for internal modems (not supplied/supported by LXE).
Display	Set background graphic and scheme. Set backlight properties and timers.
Input Panel	Select the current key / data input method. Select custom key maps.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate. Turn keypad backlight on, off or to follow display.
Mappable Keys	Assign key presses to Diamond keys.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.

Option	Function
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 MX7 access password properties for signon and/or screen saver.
PC Connection	Control the connection between the MX7 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	Select to remove specific 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, and good scan vibration options. Assign baud rate, parity, stop bits and data bits for COM1 port. See section titled “Determine Your Scanner Software Version”.
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 at this release)</i>
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound wav files to CE events.
WiFi	Set the parameters for a Summit client. (See “Chapter 5, Wireless Network Configuration” for instruction.)

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, FPGA Version and Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	LXE Utilities, LXE Drivers, LXE Image, LXE API, Internet Explorer, and .NET Compact Framework Version.
Network IP	Current network connection IP and MAC address.

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.

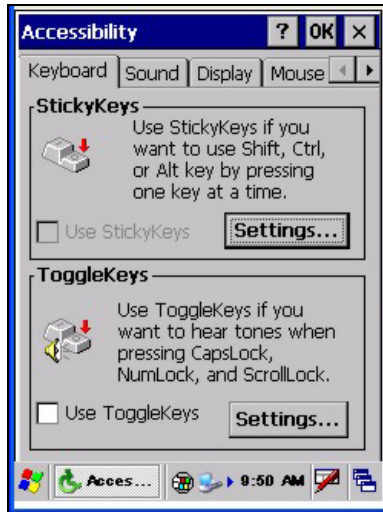


Figure 3-5 System – Accessibility

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 applications or features specified in the AppLock configuration by the Administrator are available to the end-user.

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

AppLock contains a component which sets configuration parameters and application launch settings as specified by the Administrator.

See Chapter 6 “AppLock” for further information and instruction.

Battery

Access:  | Settings | Control Panel | Battery

View the status of the Main and Backup batteries.

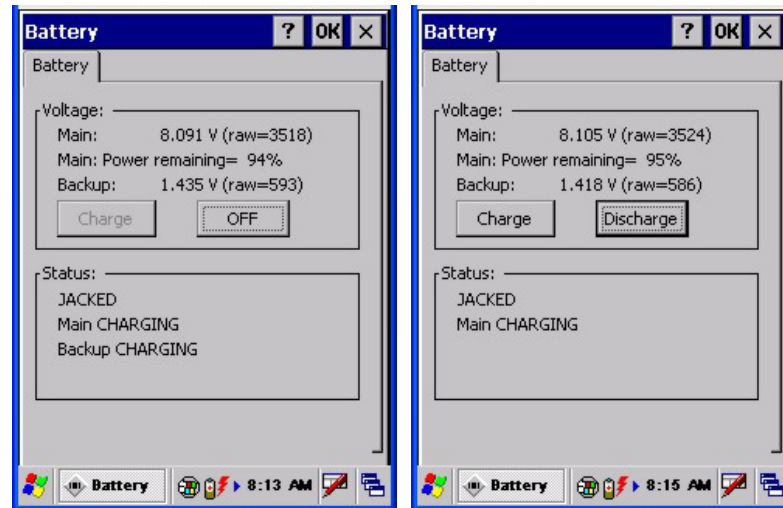


Figure 3-6 System – Battery

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. Use the Charge or Discharge buttons to charge and discharge the backup battery:

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

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

The Main Battery is charged only when an AC adapter is connected via the serial port or when the Main Battery is removed from the MX7 and placed in the MX7 Multi-charger.

Bluetooth

Access:  | **Settings | Control Panel | Bluetooth**

Discover and manage pairing with nearby Bluetooth devices. Non-LXE Bluetooth devices may be discovered but are inaccessible to the MX7 user as they are filtered out on the Bluetooth Devices panel and are not displayed. Your Bluetooth panel setups may be different than those shown on the following pages. The MX7 does not have a Bluetooth managed LED.

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.

- The default Bluetooth setting is On.
- The MX7 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 must be deleted before a different scanner or printer can be paired with the MX7.
- The remote Bluetooth device should be as close as possible, and in direct line of sight, to the MX7 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the MX7. The MX7 operating system has been upgraded to the revision level required for Bluetooth client operation.

Discover Button

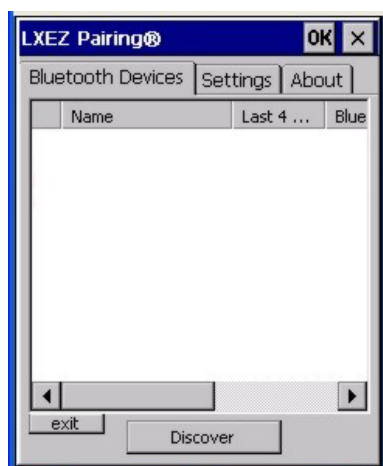


Figure 3-7 Control Panel - Bluetooth

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

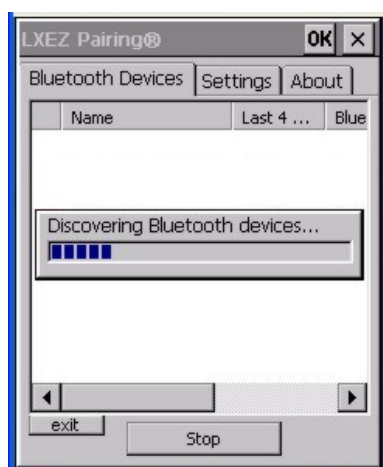


Figure 3-8 Discover Bluetooth Devices

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 MX7 is shown in the Bluetooth Devices panel. Previously paired device data is persistent through warmboot and Suspend/Resume functions.

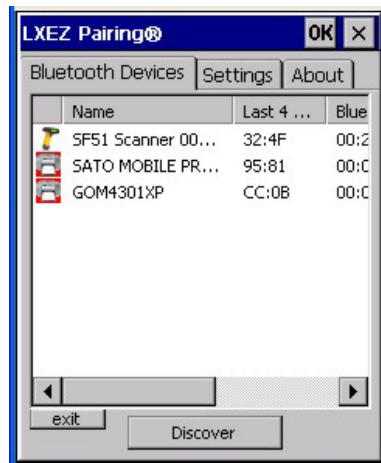


Figure 3-9 Bluetooth Devices Panel

Note: When an active paired device, not the MX7, enters Suspend Mode, is turned Off or leaves the MX7 Bluetooth scanning range, the Bluetooth connection between the paired device and the MX7 is lost. There may be audible or visual signals as paired devices disconnect from the MX7. Non-LXE Bluetooth devices may be discovered but are inaccessible to the MX7 user as they are filtered out on the Bluetooth Devices panel and are not displayed.

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 MX7 and the device Bluetooth connection is active.

Inactive devices can be deleted from the list. Active devices can be disconnected from the MX7 and remain on the list.

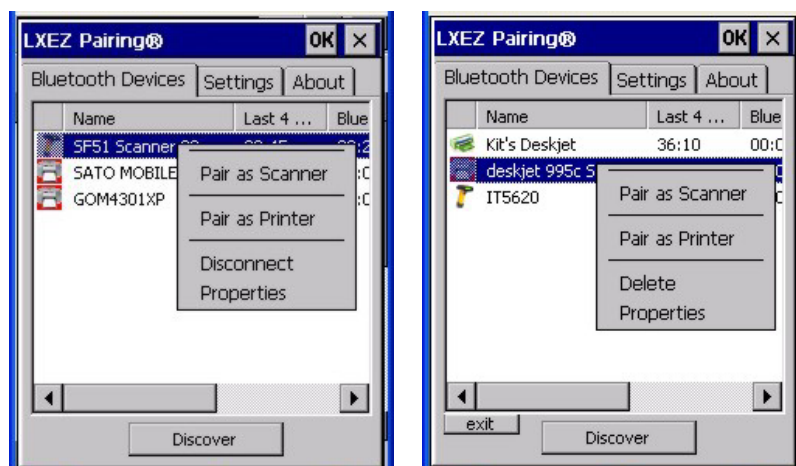


Figure 3-10 Bluetooth Device Disconnect / Delete

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

Tap **Pair as Scanner** to set up the MX7 to receive data from the scanner.

Tap **Pair as Printer** to set up the MX7 to send data to the printer.

Tap **Disconnect** to disconnect an active device (icon with white background) from the MX7 paired device database. The icon background turns red and the device remains in the list.

Tap **Delete** to delete an inactive device (icon with red background) from the MX7 paired device database. Close the LXEZ Pairing control panel to erase the device from the list after deleting.

Tap **Properties** to view the status of a device.

Bluetooth Device Properties

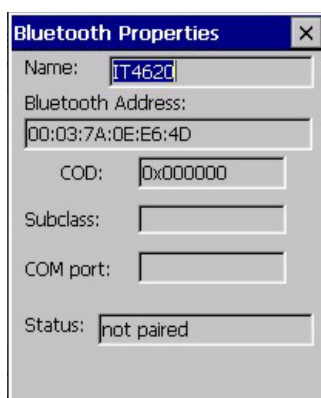


Figure 3-11 Bluetooth Device Properties Menu

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 3-12 Bluetooth Device Settings Panel

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	<p>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.</p> <p>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.</p>
Computer is connectable	Enabled	Disable this option to inhibit MX7 connection with all Bluetooth devices.

Option	Default	Information
Computer is discoverable	Disabled	Enable this option to ensure other devices can discover the MX7.
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 MX7 stops searching after 30 minutes. This option draws power from the Main Battery.
Computer Friendly Name	OS Version	The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

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

About





Figure 3-13 Bluetooth About Panel

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

Pairing and Auto-Reconnect

The 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 MX7 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).
	MX7 is not connected to any Bluetooth device. MX7 is ready to connect with any Bluetooth device. MX7 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 MX7 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 3-14 System – Stored Certificates

Lists the Stored certificates trusted by the MX7 user. These values may change based on the type of network 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.

Date/Time

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

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

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

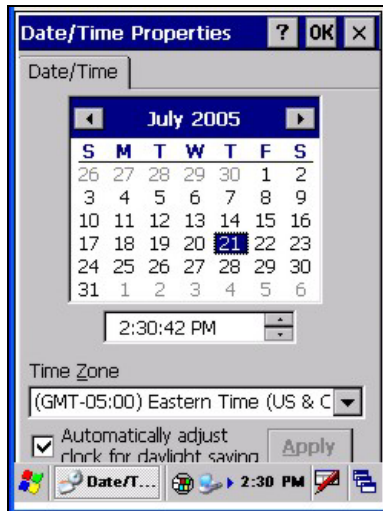


Figure 3-15 Date/Time Properties

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.

The MX7 includes a GrabTime utility which can be configured to synchronize the time at each bootup. Please see “Enabling GrabTime” in the “Utilities” section for details.

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 3-16 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	
Background	Windows CE
Tile	Disabled
Appearance	
Default	Windows Standard
Backlight	
Battery Auto Turn Off	Enabled
Idle Timer	3 seconds
External Auto Turn Off	Enabled
Idle Timer	2 minutes

Background

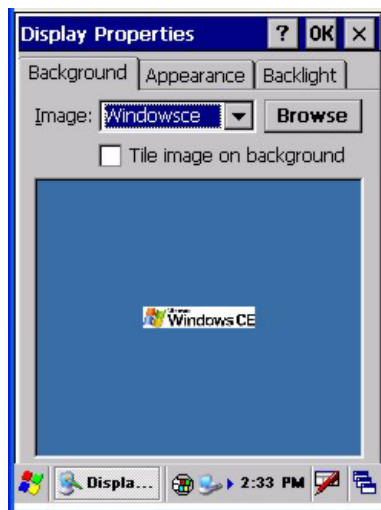


Figure 3-17 Display – Background

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

Appearance

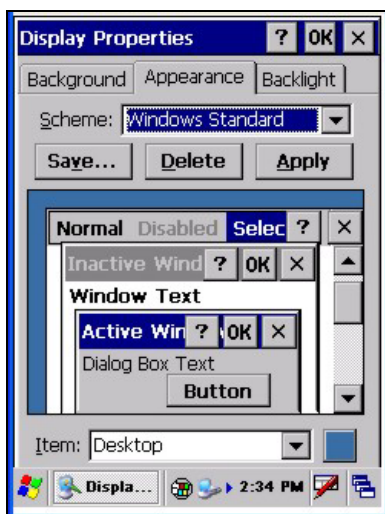


Figure 3-18 Display – Appearance

There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the MX7. Tap the OK box to exit, or “X” to escape without making any changes. Saved changes take effect immediately.

Backlight

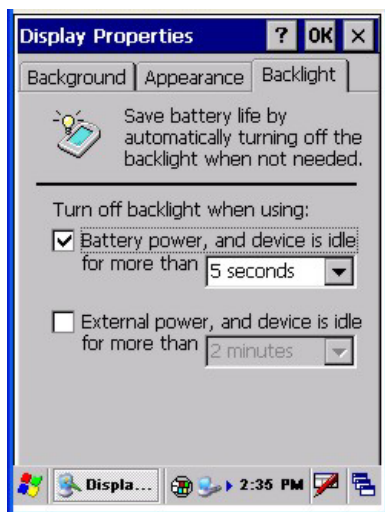


Figure 3-19 Display – Backlight

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.

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

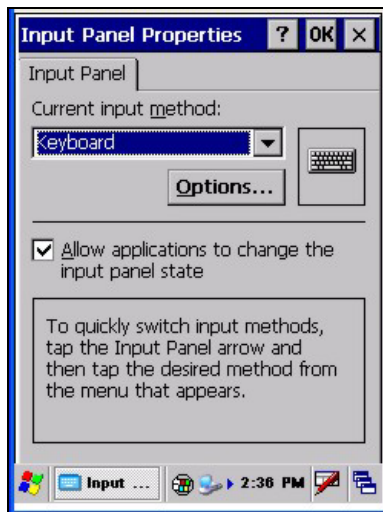


Figure 3-20 Input Panel

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

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

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

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

Internet Options

Access:  | Settings | Control Panel | Internet Options

Set options for internet connectivity.

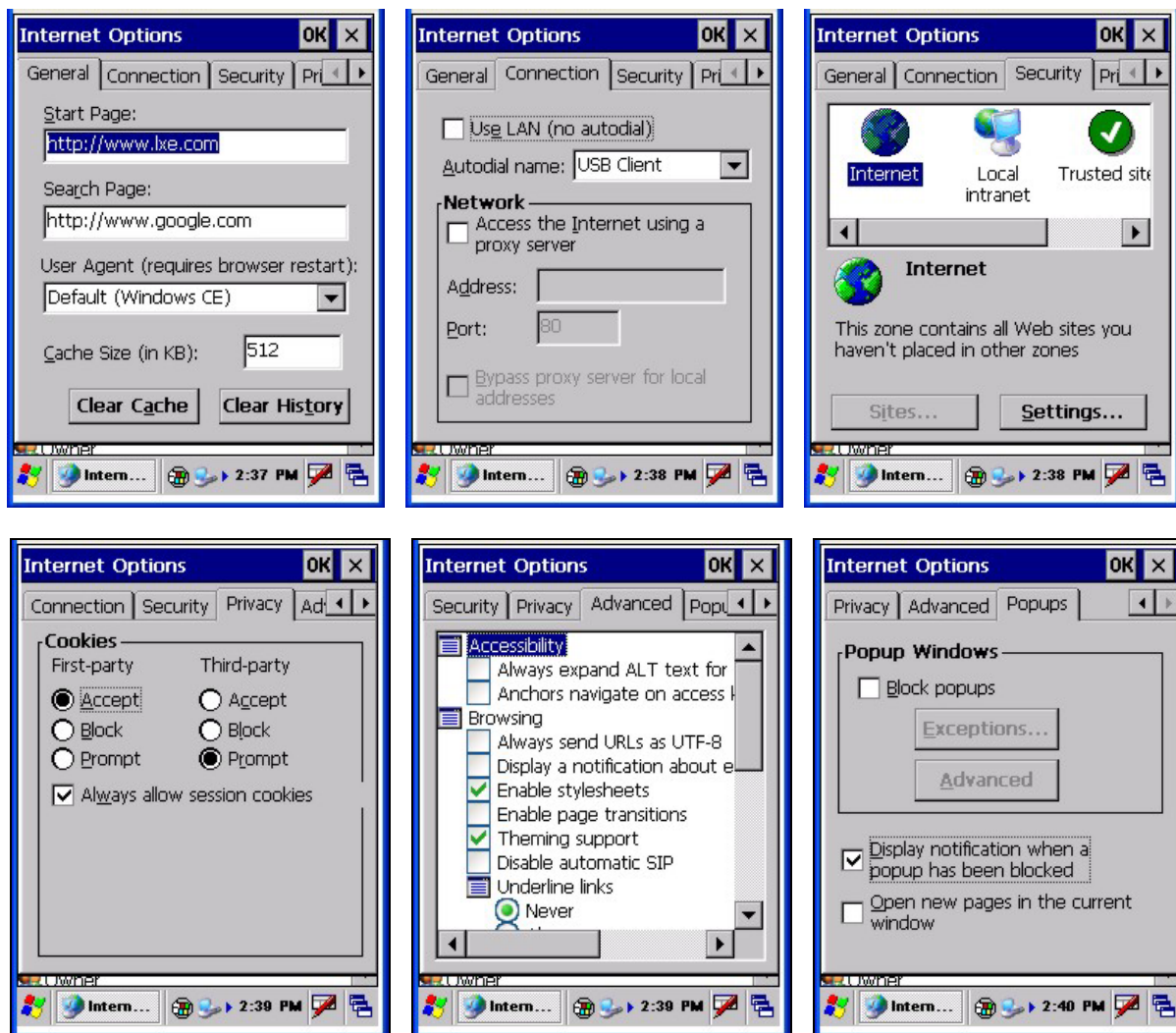


Figure 3-21 Internet Options

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	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank

Factory Default Settings	
Proxy Server	Disabled
Bypass Proxy	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enable
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Keyboard

Access:  | Settings | Control Panel | Keyboard Icon

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

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key map	Default MX7
Backlight	Always Off

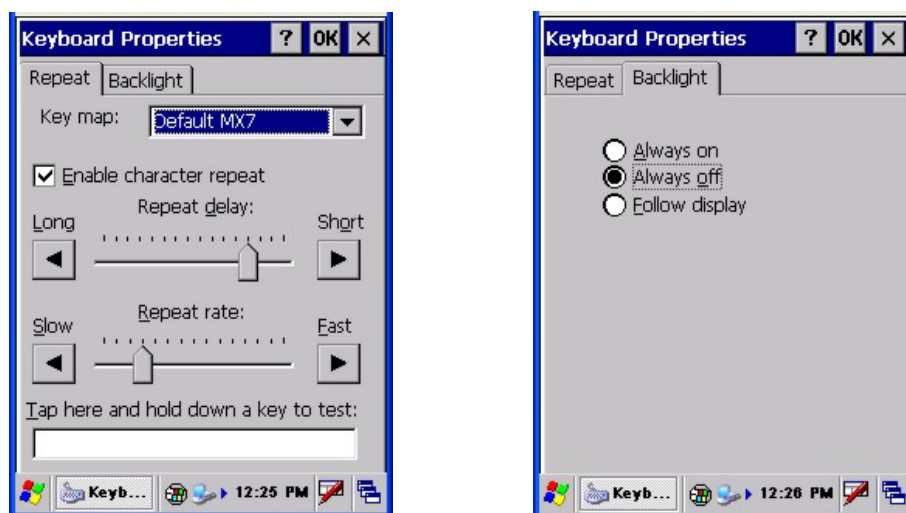


Figure 3-22 Keyboard Properties

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) key taps.

Keymaps and Fonts

Please contact your LXE representative about the availability of these fonts for your MX7:

Descriptive name	Font filename	Notes
Simplified Chinese	simsum.ttc	These Asian fonts are ordered separately and built-in to the MX7 OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the default (extended) fonts. See About Software Language for the name of any installed fonts.
Traditional Chinese	mingliu.ttc	
Japanese	msgothic.ttc	
Korean	gulim.ttc	

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

Backlight

The default value is Always off. The backlight will not activate during Suspend/Resume or hardware reset.

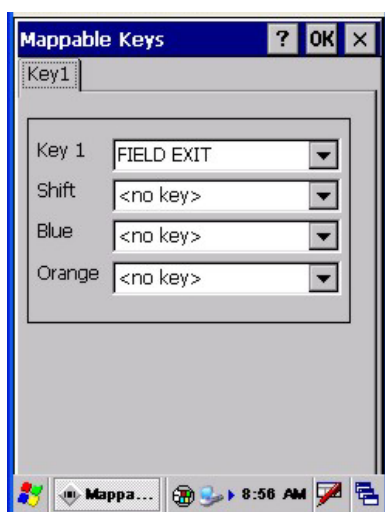
Select Follow Display to synchronize the keypad backlight with the Display backlight timer settings. See **Start | Settings | Control Panel | Display icon | Backlight tab**.

Mappable Keys

Access:  | Settings | Control Panel | Mappable Keys Icon

Use this option to assign key sequences to Diamond keys.

Factory Default Settings		
55 Key Keypad		
Diamond 1		
No sticky key	Field Exit	
Shift+Diamond 1	No key	
Orange+Diamond 1	No key	
Blue+Diamond 1	No key	
32 Key Keypad		
Diamond 1		
No sticky key	Field Exit	
Shift+Diamond 1	No key	
Orange+Diamond 1	*	Fixed setting (not mappable)
Blue+Diamond 1	No key	
Diamond 2		
No sticky key	No key	
Shift+Diamond 2	No key	
Orange+Diamond 2	=	Fixed setting (not mappable)
Blue+Diamond 2	(Fixed setting (not mappable)
Diamond 3		
No sticky key	No key	
Shift+Diamond 3	No key	
Orange+Diamond 3	!	Fixed setting (not mappable)
Blue+Diamond 3)	Fixed setting (not mappable)



55 Key Diamond 1



32 Key Diamond 1



32 Key Diamond 2 / Diamond 3

Figure 3-23 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	
Output	
Master Volume	-6dB
Sidetone	12dB
Input	
Input	None
Input Boost	Disabled
Record Gain	22.5dB

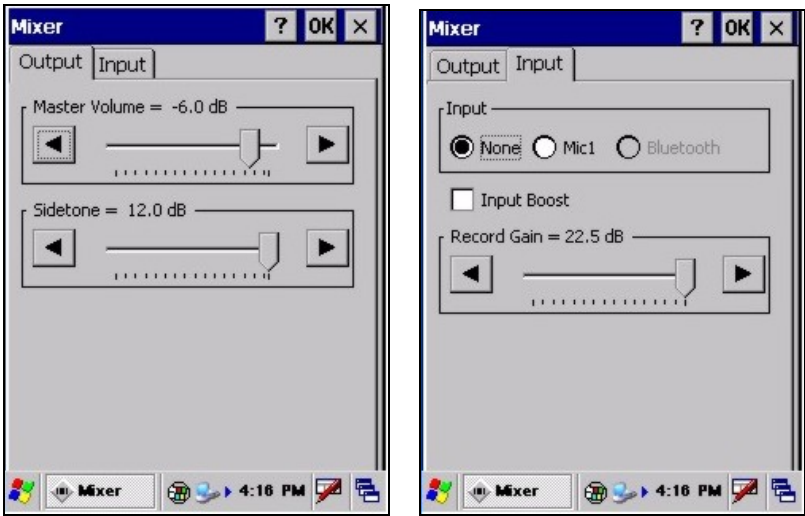


Figure 3-24 Mixer

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 **Mic1** 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

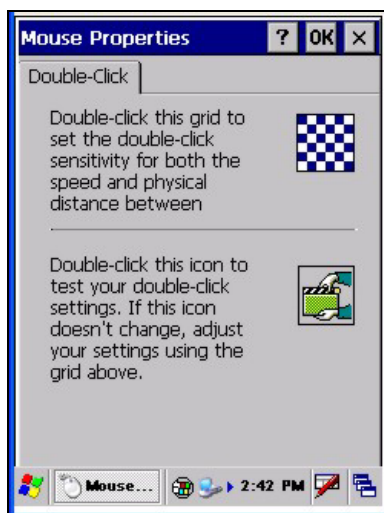


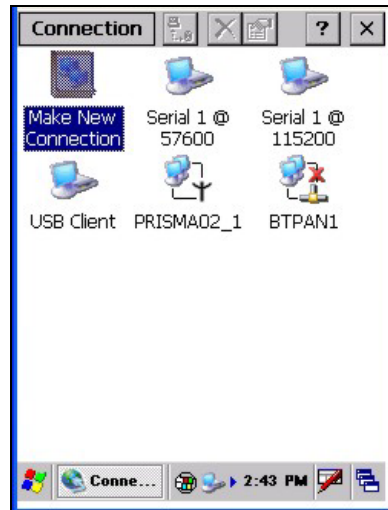
Figure 3-25 Mouse

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

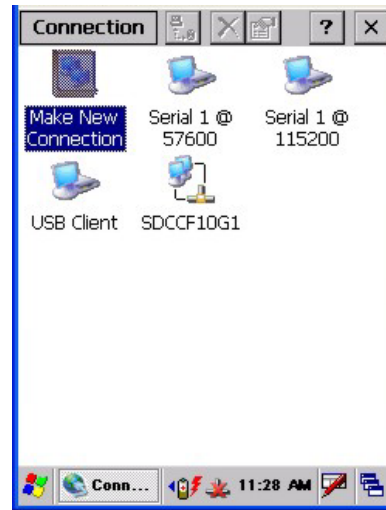
Network and Dialup Connections

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 MX7.



Odyssey Client Connection Panel





Summit Client Connection Panel

Figure 3-26 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	
Identification	
Name, Company, Address, Telephones	Blank
Display at power-on	Disabled
Notes	
Notes	Blank
Display at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank

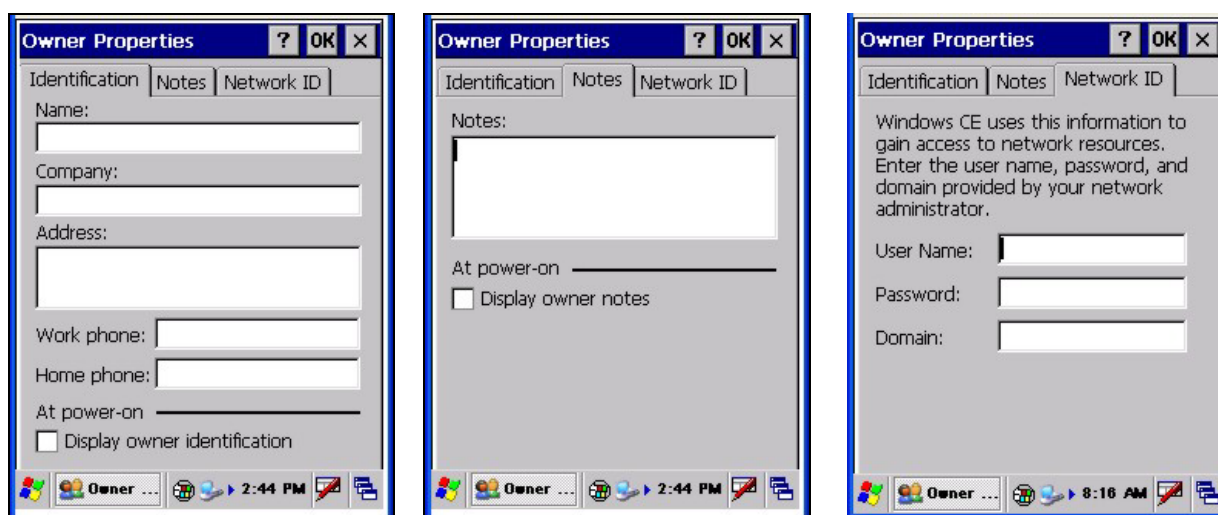


Figure 3-27 Owner Properties

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 MX7 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 3-28 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 coldboot or cold reset. If entering a power-on or screensaver password will not allow you to disable password protection or run COLDBOOT, contact LXE Technical Support.

PC Connection

Access:  | Settings | Control Panel | PC Connection

Control the connection between the MX7 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.

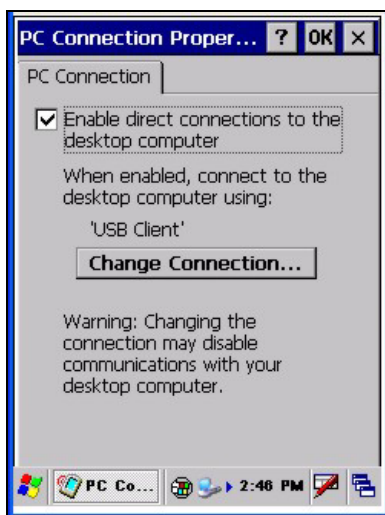


Figure 3-29 PC Connection

Please refer to the “Backup MX7 Files” section later in this chapter for parameter setting recommendations.

Power

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

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

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

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

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

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

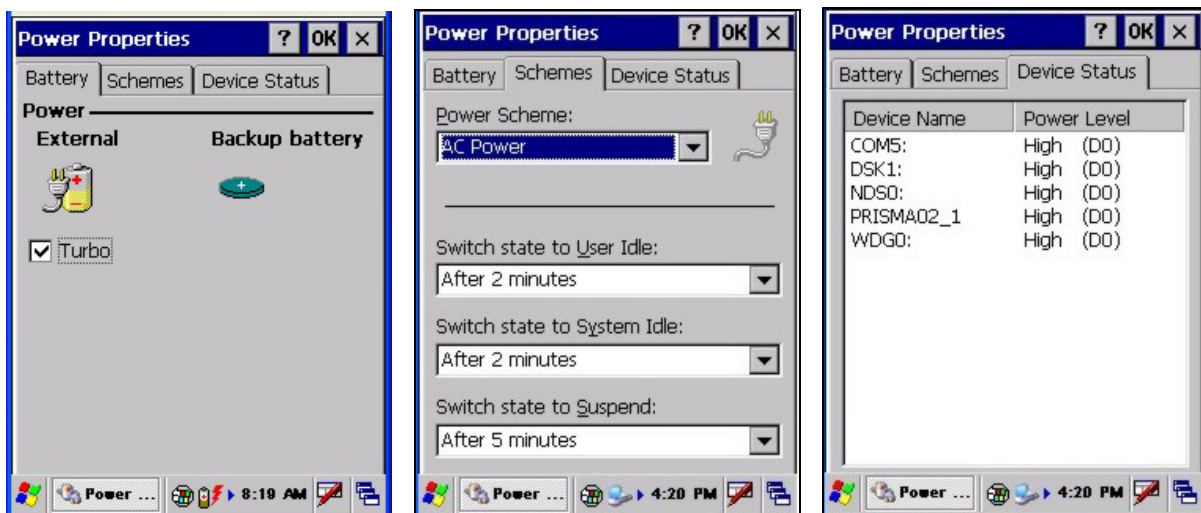


Figure 3-30 Power

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

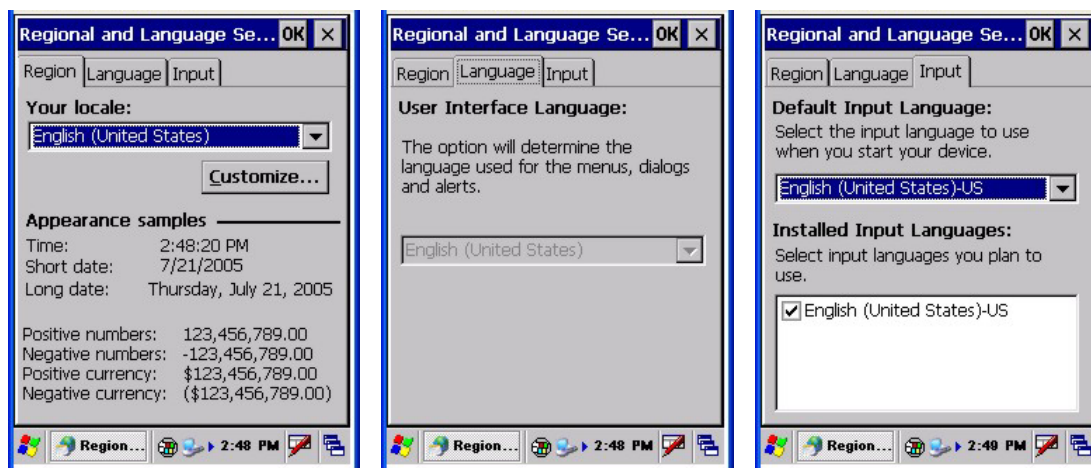


Figure 3-31 Regional Settings

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 MX7 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 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.

Determine Your Scanner Software Version

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX7 devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device. To identify the software version, tap the “About” icon in the Control Panel.

If your Barcode Tab looks like this	Go to
	This chapter, this section titled “Scanner”
It looks different	Chapter 4 “Scanner”.

Factory Default Settings

Factory Default Settings	
Main	
Port 1	Internal
Port 2	Disabled
Port 3	Disabled
Send key messages (WEDGE)	Enabled
Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Disabled / Long
Bad Scan Vibration	Disabled / Long
COM1 Port (external serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Barcode	
Use Advanced Barcode Processing	Disabled

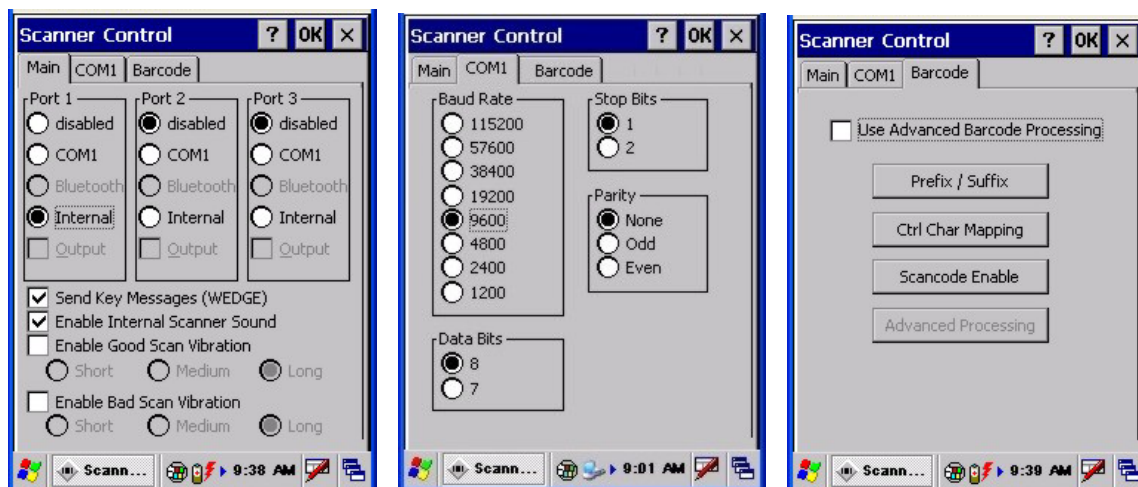


Figure 3-32 Scanner Control Panels

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”. Even if Send Key Messages is enabled (key mode), the data is still available using the scanner APIs (block mode).

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. This change takes effect immediately.

Main Tab

Access:  | Settings | Control Panel | Scanner | Main tab

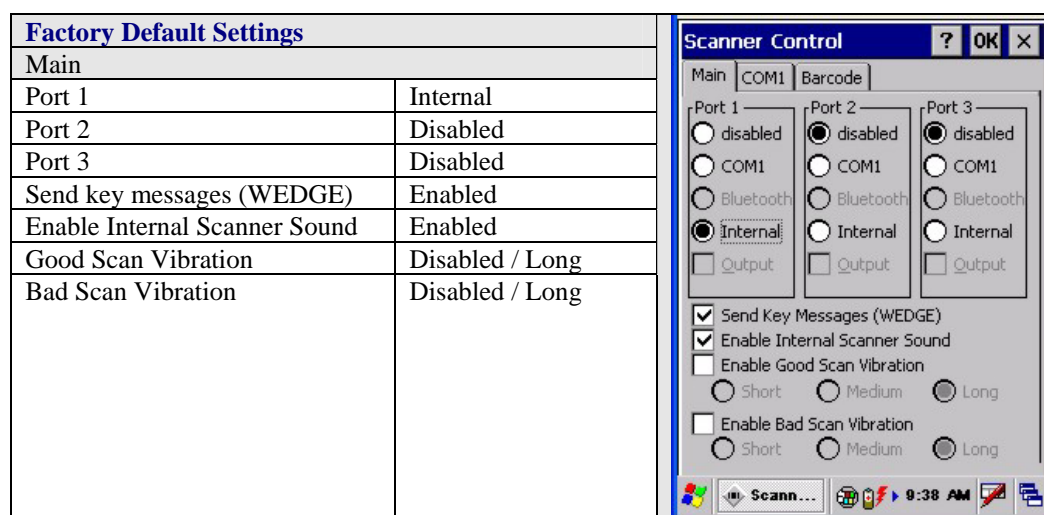


Figure 3-33 Scanner Panel - Main

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)	The default setting is Enabled. This feature coexists with the Prefix/Suffix feature and the Advanced Control Character Mapping feature. Enable for Key Message mode, disable for Block Mode. Enable to use Advanced Control Character Mapping.
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>
Good Scan / Bad Scan Vibration	<p>The default setting is Disabled. Enable this parameter when a tactile response 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.</p> <p>Enable short, medium or long duration for each selection (good scan/bad scan).</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

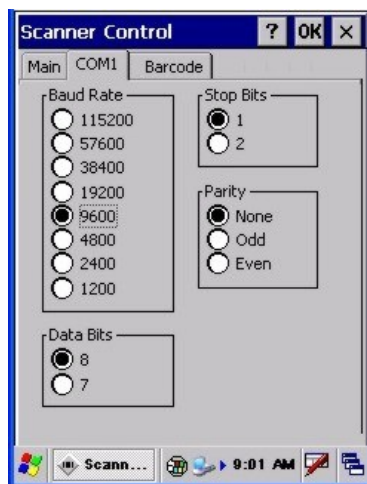


Figure 3-34 Scanner Panel – COM1

Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

EV-15 scanner default values are 19200 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 – Advanced - Prefix / Suffix

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

Prefix / Suffix is only available when *Use Advanced Barcode Processing* is disabled (default).

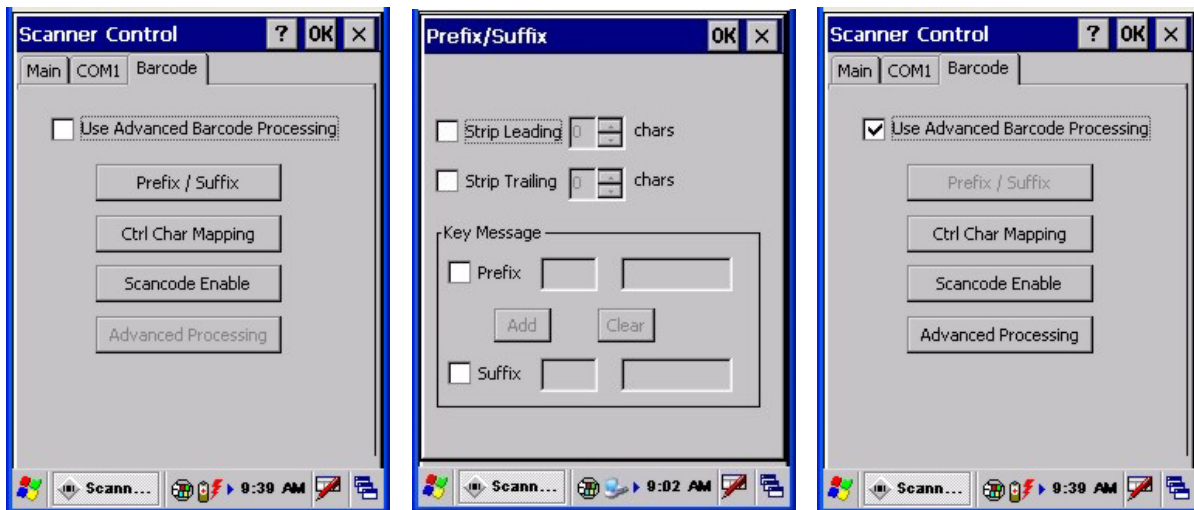


Figure 3-35 Barcode – Advanced – Prefix / Suffix

Prefix/Suffix (and pre-existing data) is ignored when *Use Advanced Barcode Processing* is enabled.

Strip Leading / Strip Trailing Characters

This feature, when enabled, strips the specified number of characters from a barcode, either from the beginning (leading) or at the end (trailing), or both.

When this feature and the Add Prefix and / or Add Suffix features are both enabled, the leading and trailing characters are stripped before the prefix or suffix is appended.

The configuration for stripping leading and trailing characters is specified independently. To enable, either or both of the checkboxes labeled Strip Leading and Strip Trailing must be checked. Then the number of characters to be stripped can be typed into the edit control or set using the spin control on the right of the edit control.

The maximum number of characters that can be stripped is 99 characters for each leading and trailing number of characters. When the Strip Leading and Strip Trailing checkboxes are blank (or disabled), the edit controls are disabled; however the last specified number of characters to strip is retained and dimmed.

When the number of characters to be stripped is greater than the number of characters in the barcode a good read beep is sounded but all barcode data is discarded.

Prefix / Suffix

If Add Prefix and / or Add Suffix are combined with Strip Leading and / or Strip Trailing, the leading and / or trailing characters are stripped before the prefix or suffix is added.

The mode for Prefix/Suffix feature is determined by the “Send Key Messages (WEDGE)” setting in the Main tab. When checked (enabled), the prefix/suffix feature is in *Key Message mode*. Key

message mode sends the prefix, barcode, and suffix to the application with the focus as keystrokes. In Key message mode all keys on the keypad can be entered.

When the “Send Key Messages” is not checked, *Block mode* is enabled. Block mode allows ASCII characters (0x0 – 0x7F), plus backspace, tab, delete, return and escape. In Block mode the prefix/suffix data is added to the beginning and end of the buffered barcode data that can then be read by an application from the WDG: device.

Up to 19 characters can be specified for the prefix and up to 19 characters can be specified for the suffix. The characters can be text or control characters, e.g. tab, carriage return. The characters can be entered into the prefix and suffix text boxes by typing from the keypad, entering the key’s hex equivalent, or entering in hat (^) encoded delimited (8-bit code table) notation.

- To enable the Prefix or Suffix processing, check the associated checkbox. When the box is checked, the edit controls to the right are enabled. Keys/characters are typed into the edit control following the checkbox.
- Selecting the Add button then adds the key to the associated list of keys in the read-only edit control to the right of the Add / Clear buttons. The keys are shown as comma-delimited strings.
- To erase the Prefix or Suffix, select the read-only edit control that contains the currently configured Prefix or Suffix and select the Clear button.
- The Add and Clear buttons function on the control that is selected when the button is pressed.
- Hex values can be entered by preceding the two digit hex value with ‘0x’. Control characters can also be entered using the ‘hat’ delimited notation, i.e. ^M for Carriage Return.
- All keypad keys can be entered by typing the key. Some keypad keys are only valid if in “Key Message” mode. For example, the Function Keys (F1, PF1) are only valid in “Key Message” mode.

Interaction between Strip Leading/Trailing and Prefix/Suffix Settings

1. Replacements are not done on the Prefix and Suffix, only the barcode data, for both Block and Key Message mode. Control characters in the Prefix and Suffix are translated when Translate All is enabled.
2. Replacements are done on the barcode data and then characters are stripped for both Strip Leading and Strip Trailing features. As an example, suppose we have the following data and configuration:

The barcode scanned begins with Group Separator (GS) followed by the character ‘A’

Group Separator is translated to ‘GS’

Strip Leading is set to 2

In this case, the Group Separator is translated to ‘GS’ and then the ‘GS’ is stripped by the Strip Leading setting; rather than the Group Separator and ‘A’ being stripped.

3. If Translate All is enabled and replacements are assigned, the assigned replacements take precedence over the default one-to-one translation enabled by Translate all. For example if Translate All is enabled and Carriage Return is replaced by ^J, the value, 0x0d, in the barcode (prefix and suffix) are replaced with CTRL+Shift+J instead of CTRL+Shift+M keystrokes in Key Message mode.

4. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to 'Ignore (drop)' by the assigned replacements, it is discarded before the Translate All processing is performed and is therefore not translated.
5. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to text by the assigned replacements, the text is substituted for the control character. In this case, the control character would not be in the data processed by the Translate All feature.
6. If the application that is accessing the Barcode Wedge in Block mode, supports Hat encoded characters, like ^M, hat encoded characters can be assigned in the defined action and then interpreted by the receiving application by using the 'escape' format described above. The same is true for hex-encoded characters.

Barcode - Advanced – Ctrl Char Mapping

Access:  | Settings | Control Panel | Scanner | Barcode tab

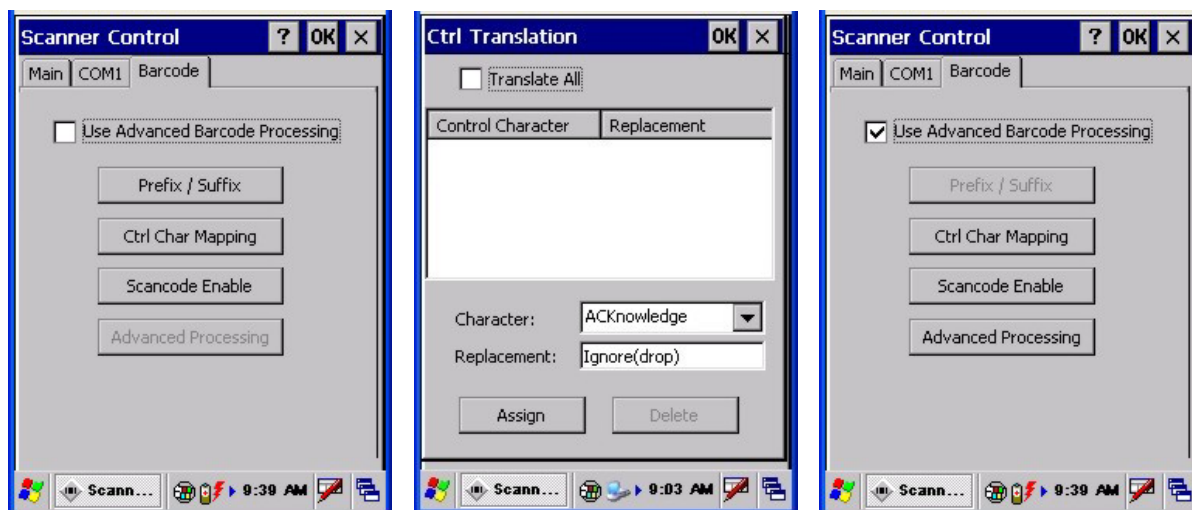


Figure 3-36 Barcode – Advanced – Ctrl Translation

Note that Control Character Mapping is available regardless of the status of the *Use Advanced Barcode Processing* checkbox.

See “Hat Encoding” and “Decimal-Hexadecimal Chart” in Appendix B.

Translate All

If “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.

When “Translate All” is not checked and “Send Key Messages” is checked, CTRL codes are passed through in Block mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes in Key Message mode. If a control character is replaced

by another control character, the replacement is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

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.

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). It does not replace control characters in the prefix and suffix. The assignments provided by this enhancement allow the user to override the one-to-one translation provided by Translate All.
Character	This is a drop down combo box that contains the control character name. Refer to the table in "Assigned Replacements" for the list of control characters and their names. When a character name is selected from the combo box, the 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 into the Replacement edit control, reselecting the character from Character combo box redisplayes the 'Ignore (drop)' default 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 combo 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.
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 - Advanced – Scancode Enable

Access:  | **Settings | Control Panel | Scanner | Barcode tab**

See the “Integrated Scanner Programming Guide”, section titled “Data Options” for full details on AIM Codes and Symbol Codes.

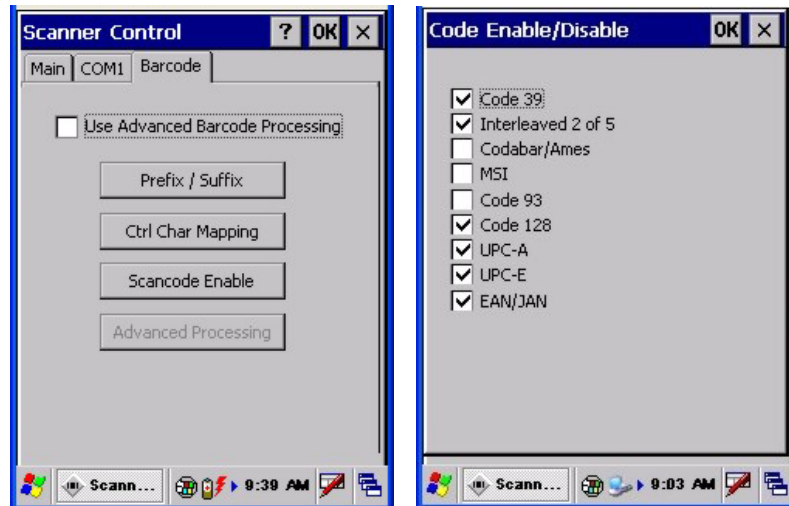


Figure 3-37 Barcode – Advanced – Scancode Enable/Disable

Note that Scancode Enable is available regardless of the status of the *Use Advanced Barcode Processing* checkbox.

This panel displays a list of all barcode symbologies supported by the integrated barcode scanner. Barcodes are sent to the application just as they are received from the scanner and before the ‘Strip Leading / Trailing’ or ‘Append Prefix / Suffix’ features.

Barcode - Advanced – Code ID

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

Note that the *Use Advanced Barcode Processing* checkbox must be enabled before Advanced Processing can occur.

See Also: The “Integrated Scanner Programming Guide”, section titled “Data Options” for full details on AIM Codes and Symbol Codes.

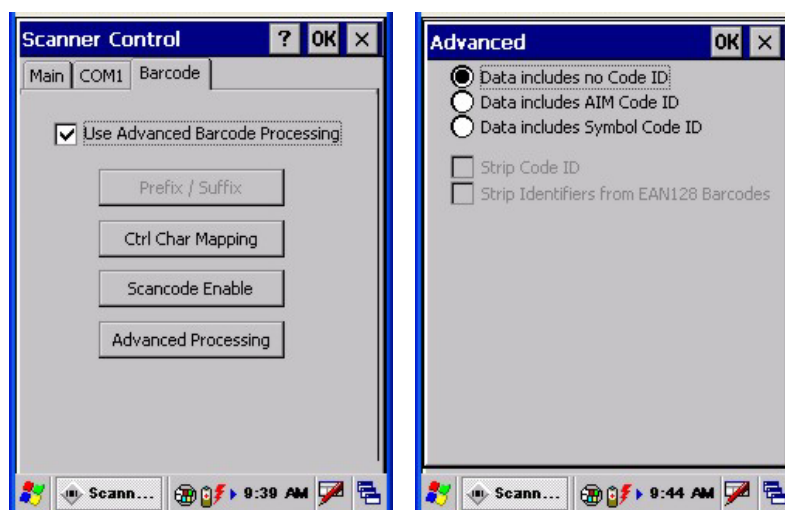


Figure 3-38 Barcode – Advanced Processing – No Code ID

Options on this Barcode and Advanced panels are not available if there is no integrated scanner, or a non-Symbol scan engine, installed in the MX7.

No Code ID

Default. All symbology IDs are transmitted. This means that by default, all good scan barcodes are sent to the application just as they are received from the scanner, regardless of any possible symbology ID attached. The *Strip Code ID* radio button is unavailable when No Code ID is enabled.

AIM Code ID

Enabling the Strip Code ID checkbox ensures the 3-character AIM Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data includes Symbol Code ID* if the AIM Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.

Symbol Code ID

Enabling Strip Code ID ensures the 1-character Symbol Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data includes AIM Code ID* if the Symbol Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.

Strip Code ID

Enabling this parameter removes the number of characters (specified by AIM Code ID or Symbol Code ID radio button setting) before the barcode is sent to the application.

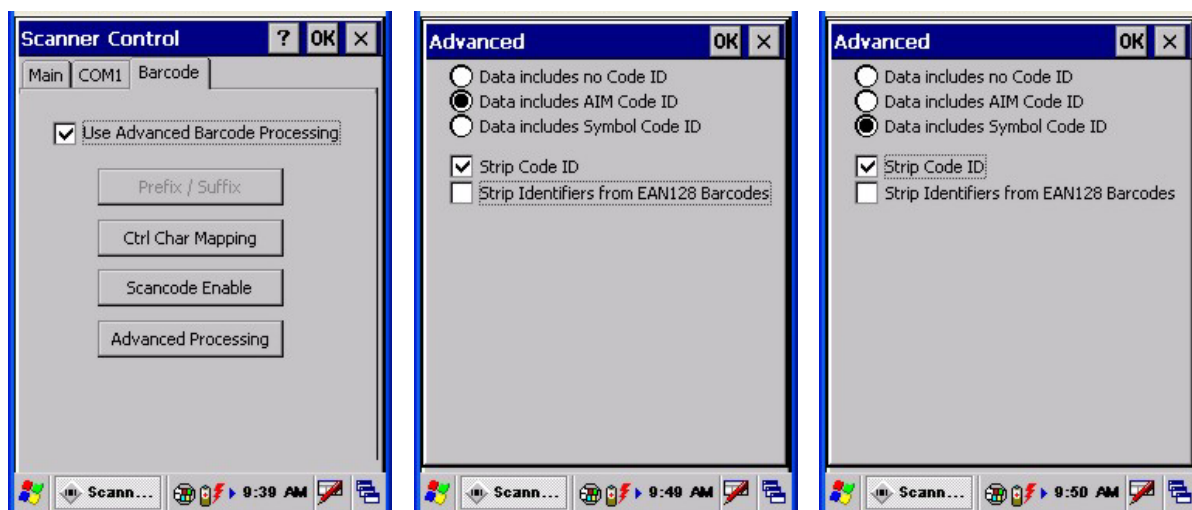


Figure 3-39 Barcode – Advanced Processing – Strip Code ID

This checkbox is unavailable when *Data includes no Code ID* radio button is enabled.

Strip Identifiers from EAN128 Barcodes

When *Strip Code ID* is disabled (unchecked), the AIM Code or Symbol Code ID is included in the barcode data being matched.

Scanned barcodes *are not matched* against the following parameters unless they are EAN128 barcodes. If the scan engine does not support EAN128 barcodes, or EAN128 barcodes have been disabled, the *Strip Identifiers from EAN128 Barcodes* function is not available.

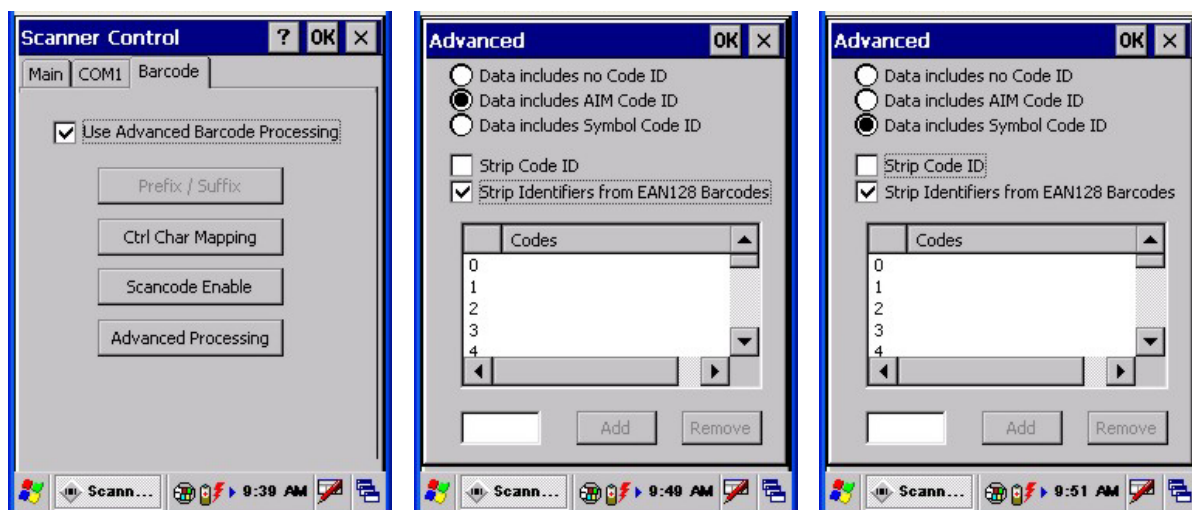


Figure 3-40 Barcode – Advanced Processing – EAN128 Barcodes

The user specifies whether the barcodes have an AIM Code ID (3 characters) or a Symbol Code ID (1 character). They also specify whether the AIM or Symbol Code ID will be stripped or passed through to the Codes match, **as long as the barcode is an EAN128 barcode**.

Adding Codes to the Match List for EAN128 Barcodes

The first elements of an EAN128 barcode are matched against the entries in the Match Code list, in the order entered in the list. For example, if the match code list contains *Item 0 ABC*, *Item 1 C* and *Item 2 AB* in that order, the *AB* has no effect. When a match is found (e.g. Code ID *A* was matched by *Item 0 ABC* and the process terminated) or when the end of the list is reached, processing terminates.

Up to 20 Codes (up to 16 characters each) can be added to the Match list. The characters can be text or control characters, e.g. tab, carriage return. The characters can be entered into the Match Code List text box by typing from the keypad, entering the key's hex equivalent, or entering in hat (^) encoded delimited (8-bit code table) notation.

- Keys/characters are typed into the lower left text box.
- To add a match code, move the cursor to the lower left text box. Add the characters to the box and select the Add button to place the new Match Code in the List Box.
- To edit a match code, highlight the match code in the List Box and double-click. The match code text is moved to the lower left text box. Make changes to the copied match code and select the Add button.
- To delete a match code, highlight the code in the List Box and select the Remove button. The match code is deleted from the list.
- After adding, editing or removing match codes, perform the Suspend/Resume function to store your changes in the registry.
- Hex values can be entered by preceding the two digit hex value with '0x'. Control characters can also be entered using the 'hat' delimited notation, i.e. ^M for Carriage Return. See "Hat Encoding" and "Decimal-Hexadecimal Chart" in Appendix B.
- All keypad keys can be entered by typing the key.

Note: No matching is done for barcodes using this option if they are not EAN128 barcodes.

Stylus

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

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

Double Tap

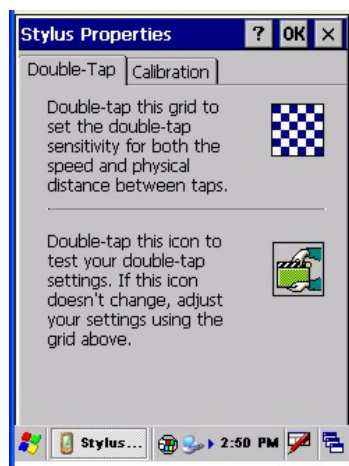


Figure 3-41 Stylus - Double-Tap

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

Calibration

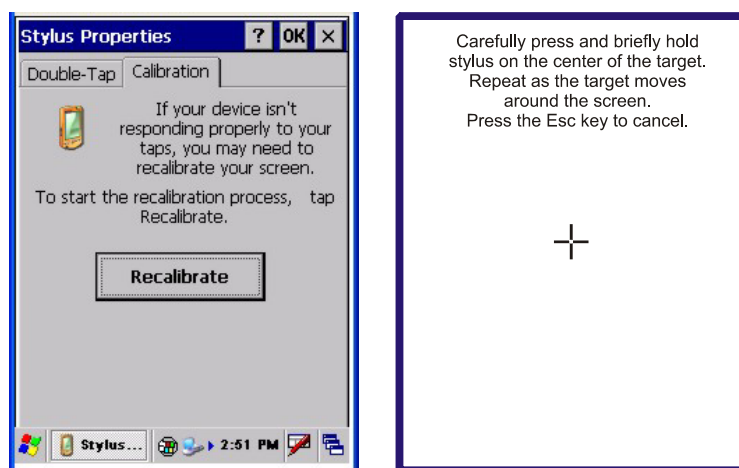


Figure 3-42 Stylus - Calibrate

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	MX7001
Device Description	LXE_MX7

General

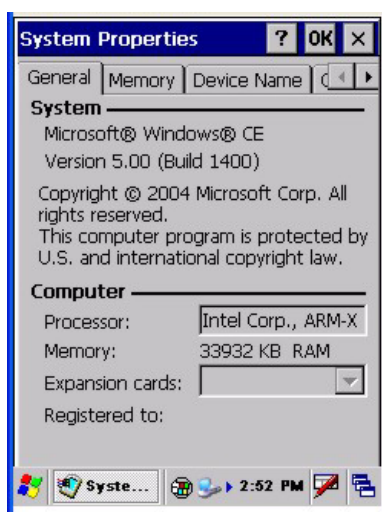


Figure 3-43 System - General

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

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

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

Memory

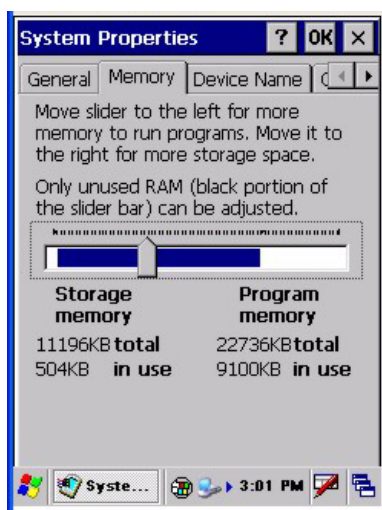


Figure 3-44 System - Memory

Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the MX7 is running slowly, try increasing the amount of program memory. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Device Name

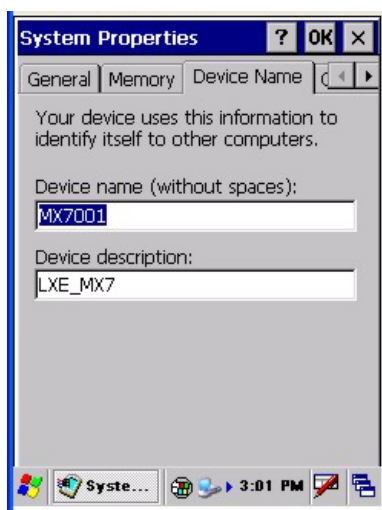


Figure 3-45 System - Device Name

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

Copyrights

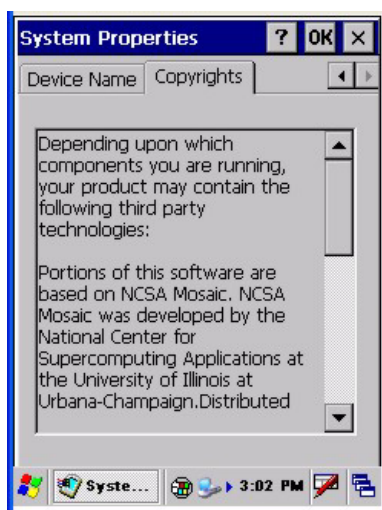


Figure 3-46 System - Copyrights

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!

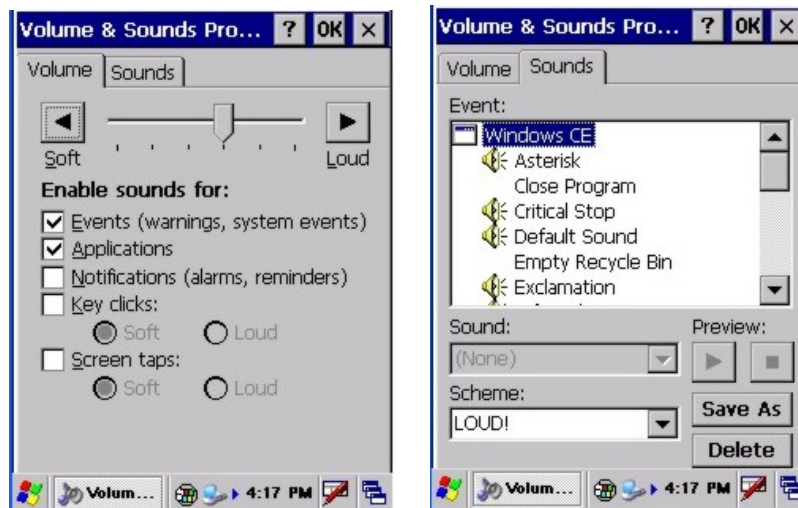


Figure 3-47 Volume & Sounds

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

Good Scan and Bad Scan Sounds

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

SD Flash Cards, CAB Files and Programs

The Flash card, located under the main battery pack, is intended to protect the user from losing the LXE drivers and configuration information in the event of a cold boot. Also, on any boot, the contents of any registered CAB files are automatically unpacked.

Access Files on the Flash Card

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

Files

A flash card is used for permanent storage of the LXE drivers and utilities. It is also used for registry content back up. The flash card is located in the socket under the main battery pack.

CAB files, when executed, are not deleted.

LXECR1.CAB	Driver for LXE 802.11 network card
LXECR1A.CAB	Additional file for 802.11 network card operation
ODYSSEY.CAB	Odyssey Client files needed for network card operation
SUMMIT.CAB	Summit Client files needed for network card operation.
The following CAB files are optional and may or may not be present:	
BLUETOOTH.CAB	Bluetooth Client files needed for LXEZ Pairing operation.
LXE_MX7_ENABLER.CAB	Wavelink Avalanche Enabler.
RFTERM.CAB	RFTerm terminal emulation application.
JAVA.CAB	Java application.
APPLOCK.CAB	AppLock program. See Chapter 6 “AppLock”.
LXELOGIN.LXE	Persistent user login utility installed by customer with Odyssey Client and becomes LXELOGIN.CAB

Note: Always perform a warm reset (Start / Run / Warmboot) when exchanging one flash card for another.

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 MX7 must be established using serial RS-232 or USB connection. When more than one PC will be synchronizing with the MX7, each PC will need its own partnership with the MX7 established. See section titled “Initial Install” for the procedure.

After the partnership has been established with the MX7 and the host computer, ActiveSync can be performed over serial, USB, or wirelessly.

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your PC with the MX7 and vice versa. Synchronization compares the data on the MX7 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 MX7 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 MX7, the data appears to transfer, but it is ignored by the MX7 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 MX7 and the desktop/laptop (PC). Once a relationship has been established, tap  | **Help** | **ActiveSync** for help.

Install ActiveSync on Desktop/Laptop


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

www.microsoft.com/downloads

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

Install ActiveSync 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 MX7. 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 MX7 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 MX7. Tap the Change Connection button. From the popup list, choose

USB Default

This will set up the MX7 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 MX7 (the client). Tap the  | **Programs** | **Communication** | **Connect** icon on the MX7.

The MX7 connection is made using  | **Programs** | **Communication** | **ActiveSync**.

** [Cables for initial ActiveSync Configuration:](#)

USB Client to PC/Laptop	MX7A052MULTICBLUSB
Serial Client to PC/Laptop	MX7A055MULTICBLDA9F

When the desktop/laptop computer and the MX7 successfully connect, the initial ActiveSync process is complete.

Change Connection Parameters

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

Option	Description
USB (Default)	This will set up the MX7 to use the USB port direct.
COM1 @ 57600	This will set up the MX7 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).

Connect

Connect the correct cable to the PC (the host) and the MX7 (the client).

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

Cable, Multipurpose USB and Power	MX7A052MULTICBLUSB
Cable, Multipurpose RS-232 and Power	MX7A055MULTICBLDA9F

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 MX7 from the PC side, with some limitations.

You can copy files to or from the MX7 using drag-and-drop.

You will not be allowed to delete files or copy files out of the \Windows directory on the MX7. (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 – MX7 User’s Guide” from your desktop computer to the My Documents folder on the MX7.

Disconnect

Serial Connection

- Disconnect the cable from the MX7.
- Put the MX7 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 MX7.
- 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 MX7 into suspend while connected via USB. The MX7 will be unable to connect to the host PC when it resumes operation.

Network Connection

- Put the MX7 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.

Backup MX7 Files

Use the following to backup data files from the MX7 to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

Initial ActiveSync partnership between the MX7 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 the network.



Figure 3-48 ActiveSync Connection Settings on a Windows PC

MX7 and PC Partnership

An ActiveSync partnership between the PC and MX7 has been established. See section “Initial Setup”.

Serial Port Transfer

- A PC with an available serial port and an MX7 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.
- Null modem cable with all control lines connected. LXE recommends using the RS-232 cable listed in the following section “Connect”..

USB Transfer


- A PC with an available USB port and an MX7 with a USB cable. The desktop or laptop PC must be running Windows 98 SR2, Windows 2000 or Windows XP.
- LXE-specific USB cable as listed in the following section “Connect”.
- “Allow USB connection with this desktop computer” is checked.

Wireless Network Transfer

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

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 MX7 is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. ( | **Settings** | **Control Panel** | **System** | **Device Name**)

If the cold booted MX7 tries to reestablish the partnership with the same host PC, a new random number is generated for the MX7 and ActiveSync will insist the unique name of the MX7 be changed. If the MX7 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 MX7 is connected to a PC by a cable, disconnect the cable from the MX7 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 MX7

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 wireless link is broken. Make sure that the network card has a valid IP address.

Utilities

These utilities are pre-loaded by LXE. In previous versions the following files were placed in the MX7 file structure as shown – they are now available using the *MX7 Options tab* in the Control Panel.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels or programs.

LAUNCH.EXE

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

Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup. The CAB file can update the registry as desired and cause the unpacked file(s) to be placed in the appropriate location.

The registry information needed is under the key *HKEY_LOCAL_MACHINE \ SOFTWARE \ LXE \ Persist*, as follows. The main subkey is any text, and is a description of the file. Then 3 values are added:

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

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

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

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

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

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

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

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

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

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

The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a wireless client 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 client 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 ³:

```
;; ----- 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

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

;; ----- Symbol client support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Symbol Radio]
    "FileName"="\System\SYMBOL.CAB"
    "Installed"=dword:0
    "FileCheck"="\WINDOWS\NICTT.EXE"
    "Order"=dword:2
    "PCMCIA"=dword:1

;; ----- LXE USB network card support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE USB Radio]
```

³ 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.

```

"FileName"="\System\LEXECR1.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\PRISMA02.DLL"
"Order"=dword:2
"PCMCIA"=dword:2

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Old LXE USB Radio]
"FileName"="\System\LXEUSB.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\PRISMA02.DLL"
"Order"=dword:2
"PCMCIA"=dword:1

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

;; ----- Summit client 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

;; ----- Odyssey client support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Odyssey]
"FileName"="\System\ODYSSEY.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\odysseyIMCE.DLL"
"Order"=dword:0E
"Delay"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Odyssey license]
"FileName"="\System\LEXECR1A.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\odyssey.txt"
"Order"=dword:0D
"Delay"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Odyssey install]
"FileName"="\System\LXElogin.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\lxelogin.exe"
"Order"=dword:05
"Delay"=dword:0

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Odyssey login]
"FileName"="\Windows\LXElogin.exe"
"Installed"=dword:0
"FileCheck"="ALWAYSEXEC"
"Order"=dword:0F
"Delay"=dword:0

;; ----- 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 client device is ready
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
    "FileName"="\WINDOWS\LXE\RFTERM.EXE"
    "Installed"=dword:0
    "FileCheck"="ALWAYSEXEC"
    "Order"=dword:40
    "Delay"=dword:1

;; ----- RFID support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFID]
    "FileName"="\System\RFID.CAB"
    "Installed"=dword:0
    "FileCheck"="\WINDOWS\RFID_WDG.DLL"
    "Order"=dword:0C

;; ----- 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

```

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

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

```

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
    "FileName"="COPYFOLDERS"
    "FileCheck"=""
    "Order"=dword:0F

```

To have files (CAB, EXE, REG, or WAV files) loaded on startup, when sequence of execution is not important, you can put these files in the \System\Startup folder (on the internal Flash card). This is parsed by the Launch utility, and these programs are started or executed.

REGEDIT.EXE



Before using REGEDIT.EXE, please refer to commercially available Microsoft Power Tools for Windows manuals . For example Microsoft Windows Registry Guide, Second edition.

The Registry Editor allows viewing, searching for items and changing settings in the registry. The registry contains information about how the mobile device runs. LXE recommends **caution** when inspecting and editing the Registry as making incorrect changes can damage the mobile device operating system. LXE recommends making a backup copy of the registry before viewing or **c a r e f u l l y** making changes to the registry.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

WARMBOOT.EXE

Double tap this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double-tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

Configuring GrabTime

Note: This utility affects the behavior of GrabTime at warmboot. After a coldboot, GrabTime is disabled.

The MX7 has a GrabTime utility which can automatically synchronize the MX7 with a worldwide time server (via an Internet connection) at boot up. By default, GrabTime for time synchronization at boot up is Off.

To enable GrabTime to run automatically at boot up, run **\Windows\grabtime.reg** and perform a warmboot. For more detail, see *LAUNCH.EXE*, earlier in this chapter.

Synchronize with a local time server

1. Use ActiveSync to copy **GrabTime.ini** from the **My Device | Windows** folder on the MX7 to the host PC.
2. Edit GrabTime.ini (on the host PC) to add the local time server's domain name to the beginning of the list of servers. You can then optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini to the **My Device | System** folder on the MX7.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. Each time the mobile device is cold booted, the Windows/GrabTime.ini file is replaced with the default version and the System/GrabTime.ini file is not.

Configuring CapsLock Behavior

To set CapsLock status to On after a warmboot, run \Windows\CapsLockOn.reg and perform a warmboot.

To set CapsLock status to Off after a warmboot, run \Windows\CapsLockOff.reg and perform a warmboot.

Note: Setting CapsLock to On using this method does not display the CapsLock icon in the Windows CE taskbar. The current status of CapsLock can be changed with the CAPS key, however this method does not change CapsLock behavior upon reboot.

Note: These utilities affect the behavior of the CapsLock on warmboot. After a coldboot, CapsLock is disabled.

Configuring IPv6

By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up.

To disable IPv6, run \Windows\ipv6Disable.reg and perform a warmboot.

To enable IPv6, run \Windows\ipv6Enable.reg and perform a warmboot.

Note: These utilities affect the behavior of IPv6 on warmboot. After a coldboot, IPv6 is enabled.

Launch App / Launch Command

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels or programs.

The Launch App / Launch Command are defined for use by CE administrators. The VK_LAUNCH_APP1-4 and VK_LAUNCH_CMD1-4 keys are parsed and executed directly by the keyboard driver. They are configurable in registry keys to execute any desired function.

The CMD keys differ from the APP keys in that they call the ShellExecuteEx API, which lets them open documents directly; the APP keys only start EXE applications.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the mobile device emits a single beep, if the launch is successful, the mobile device is silent.

The registry keys are:

[HKEY_LOCAL_MACHINE\Software\LXE\Launch\App1] . . . App2, App3, App4]

“Exe”=“” [name of executable file]
 “Opt”=“” [options or parameters for executable file]

[HKEY_LOCAL_MACHINE\Software\LXE\Launch\Cmd1] . . . Cmd2, Cmd3, Cmd4]

“File”=“” [name of file]
 “Parm”=“” [parameters for file/exe execution]

See Also: Appendix A - Key Maps, “Creating Custom Key Maps” for more information.

Command-line Utility

Command line utilities can be executed by Start | Run | [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all data in RAM is erased). The command is not case-sensitive.

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

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap Start | Run | then type prtscrn and tap OK, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and the captured screen file (scrnnnnn.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

LXE Login Utility

Odyssey Client only. The LXE Login Utility is installed on the mobile device by LXE; however, the MX7 is not configured to load the LXE Login Utility automatically. The LXE Login Utility is designed to let you specify an Odyssey Client login name for the currently selected profile.

The login prompt is displayed at system boot and when resuming from suspend. MX7 focus remains on the login prompt until it is dismissed. Nothing else can be done on the MX7 until the user responds to the login prompt.

Follow the instructions in the following section titled “Installation” to configure your MX7 to load the LXE Login Utility. After the installation instructions have been executed, the LXE Login Utility automatically loads after any warm or cold reset of the MX7. It is activated again on a resume from suspend mode.

Note: If it is necessary to remove the LXE Login Utility, LXE strongly recommends using the instructions in the section “Uninstall the LXE Login Utility” to stop the utility from running on the MX7.

Installation

The LXE Login Utility CAB file must be renamed. Follow the instructions below to rename the CAB.

*Note: File extensions must be enabled for viewing for the following procedure to work. To insure extensions are enabled for viewing, double tap **My Device** on the Desktop. Select the **View** menu and the select **Options**. Uncheck **Hide file extensions**.*

1. Double tap **My Device** on the Desktop.
2. Double tap **System**.
3. Use the scroll bar to locate **LXELogin.LXE**.
4. Tap and hold on LXELogin.LXE until the “right mouse-click” menu appears.
5. Select the **Rename** menu item. The stylus cursor changes to the input cursor (I) and **LXELogin.LXE** is highlighted.
6. Press the right arrow key to position the input cursor at the end of the input field.
7. Use the **BkSp** key to erase **LXE** from the filename.
8. Type **CAB** and press the **Enter** key.
9. Warm reset the mobile device by selecting **Run** from the **Start** menu, type **WARMBOOT** in the Open edit control panel and press the **Enter** key.

Using the Utility

If multiple Profiles are configured on the mobile device, LXE Login Utility changes the username for the active profile.

Important: The profile must be changed before suspending the unit if the active profile username is to be changed when returning from Suspend.

Select the desired active profile by double tapping on the **Odyssey Client** icon on the Desktop. Select the active profile by changing the selection in the drop-down combo box below the **Connect to:** checkbox.

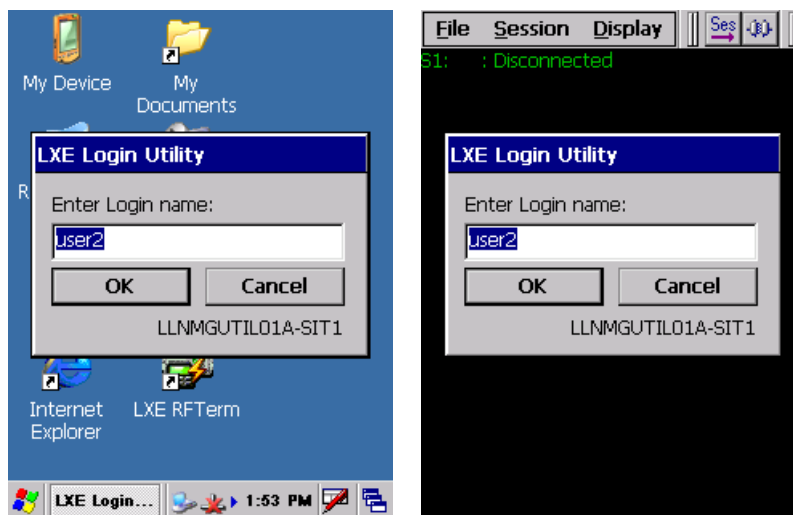


Figure 3-49 LXE Login Utility User Prompt

The Login prompt is displayed at system boot and when resuming from suspend. In the second example of the screen shown above, RFTerm has been locked using AppLock and the prompt is displayed on top of the administrator-locked RFTerm.

Note: Focus remains on the login prompt until it is dismissed. Nothing else can be done on the MX7 until the user responds to the prompt.

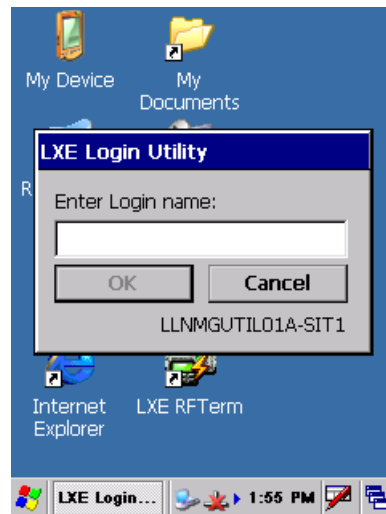
The currently configured username is displayed and highlighted in the edit control. If the displayed username is desired, press Enter or tap the OK button on the screen.

If the username needs to be changed, start typing the new user name and press Enter or tap the OK button on the screen.

If the LXE Login Utility prompt is closed by pressing Esc or tapping the Cancel button on the screen, the username change is ignored and the previously configured username is used.



User Name Typed



User Name Cleared

Figure 3-50 Enter / Select Login Name

If the username is cleared, the OK button is disabled. This prevents the user from accidentally clearing the username before continuing.

After leaving this prompt, by pressing either Enter or Esc (or tapping the OK or Cancel buttons), the Odyssey Client is displayed.

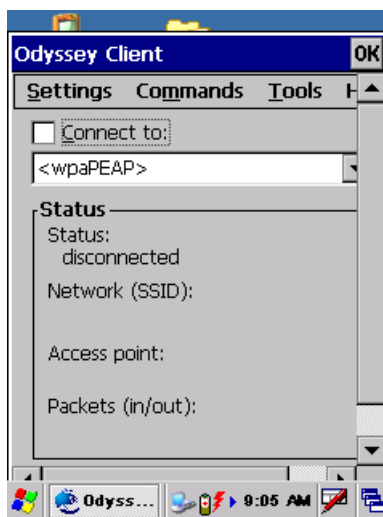


Figure 3-51 Odyssey Client Screen

Press the Spc key or check the **Connect to:** box. The Status changes from **disconnected** to **searching for access point**. After the access point is found, the password prompt is displayed. The <user> shown in the password prompt should match the username typed in the LXE Login Utility.

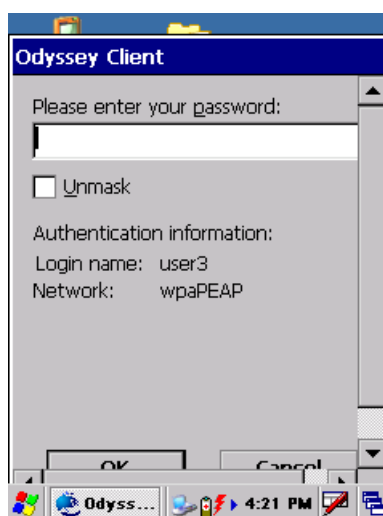


Figure 3-52 Enter the Odyssey Client Username Password

If the Login name displayed in the Odyssey Client password screen is not correct, cancel the authentication by pressing the **Esc** key or tapping the **Cancel** button on the screen.

When the Odyssey Client password screen is cancelled, the following message is displayed.

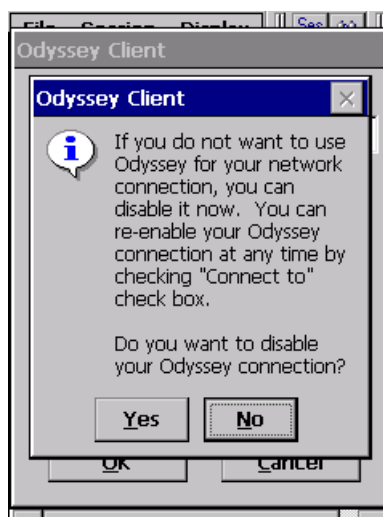


Figure 3-53 Odyssey Client Password Screen Cancelled

Select **Yes** by pressing Enter using the keypad or tapping the **Yes** button on the screen.

Note: Sometimes the password prompt is displayed a second time. If the password prompt is displayed again, repeat the last two steps to cancel the password prompt.

Suspend and resume the MX7 by pressing the power key twice. The LXE Login Utility screen is displayed to the user to enter a new username. Repeat the process described previously in this section to connect.

After correcting the username and starting the connection, enter the password that matches the selected username and press Enter or tap the OK button. The connections are opened.

Sometimes the Odyssey Client is redisplayed with the Status updated. If this happens, press **Enter** to close the Odyssey Client to return to the desktop or last active application.

Uninstall the LXE Login Utility

After the LXE Login Utility has been installed using the instructions in the “Installation” section, it automatically loads anytime a cold or warm reset is performed on the mobile device. To stop the LXE Login Utility from loading, follow the instructions below to uninstall the CAB.

*Note: File extensions must be enabled for viewing for the following procedure to work. To insure extensions are enabled for viewing, double tap **My Device** on the Desktop. Select the **View** menu and the select **Options**. Uncheck **Hide file extensions**.*

1. Double tap **My Device** on the Desktop.
2. Double tap **System**.
3. Use the scroll bar to locate **LXELogin.CAB**.
4. Tap and hold on LXELogin.CAB until the “right mouse-click” menu appears.
5. Select the **Rename** menu item. The stylus cursor changes to the input cursor (I) and **LXELogin.CAB** is highlighted.
6. Press the right arrow key to position the input cursor at the end of the input field.
7. Use the **BkSp** key to erase **CAB** from the filename.
8. Type **LXE** and press the **Enter** key.
9. Warm reset the mobile device by selecting **Run** from the **Start** menu, type **WARMBOOT** in the Open edit control panel and press the **Enter** key.

Wavelink Avalanche Enabler Configuration

An MX7 device manufactured before October 2006 must have drivers and system files upgraded before it can use the Avalanche Enabler functions. Please contact an LXE representative for details on upgrading the mobile device baseline. Related manual: *Using Wavelink Avalanche on LXE Windows Computers*.

Terminology may appear different, based on your installed version:

- Avalanche Manager may be shown as the Avalanche Mobility Center Console
- Avalanche Agent may be shown as the Avalanche Mobile Device Server
- Avalanche Management Console may be shown as the Avalanche Mobility Center or the Avalanche Mobility Center Console

Note that actual operation of the Enabler on the mobile device does not change.

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, the Enabler begins normal performance. The Enabler is by default 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_MX7_ENABLER.CAB.

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 MC Console (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

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_MX7`.

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 network 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. The Enabler will also automatically download and process all available packages.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the Enabler will attempt to apply all network and wireless settings contained in the active profile. The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler. These local parameters cannot be overridden from the Avalanche Mobility Center Console.

The default Enabler adapter control setting are:

- [Manage network settings – enabled](#)
- [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. Click 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 3-54 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;">system</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;">leave</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="781 1211 1174 1444" data-label="Image"> </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 on the Wavelink Avalanche Management Console can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details).

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 mobile device.
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 Management 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

Avalanche Server Address:

☒ Check serial connection.

☐ Disable ActiveSync

☐ Restrict Adapter Link Speed

Min. Link Speed: 1000 kbs

Figure 3-55 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.
Restrict Adapter Link Speed	When enabled and the link speed is less than the minimum specified, the Enabler cannot connect.

Execution Tab

Note the dimmed options on this panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.

LXE recommends using AppLock. See *Chapter 6 – AppLock*.

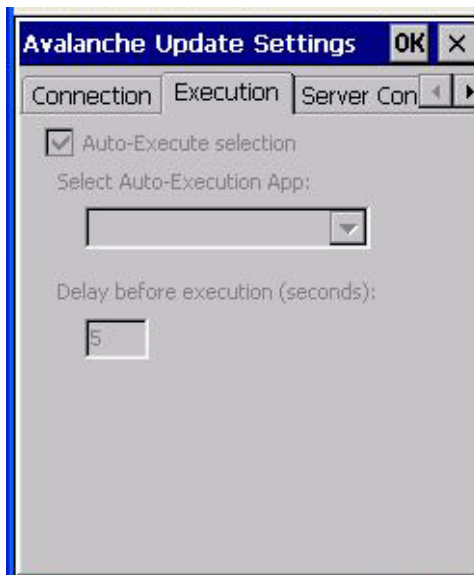


Figure 3-56 Avalanche Enabler Execution Options (Dimmed)

Auto-Execute Selection	An application that has been installed with the Avalanche Management system 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

The screenshot shows a configuration window for the 'Server Contact Tab'. It includes the following options:

- ☒ Sync clock
- Contact:
 - ☒ On startup
 - ☐ On ext. power
 - ☐ On resume
 - ☐ Periodic Update:
 - every: 1 day(s)
 - at: 00:00 (Midnight)
- ☒ Wakeup device if suspended
- ☐ Reboot before attempt
- ☐ Require external power
- ☐ Use relative offset

Figure 3-57 Avalanche Enabler Server Contact Options

Sync Clock	Reset the time on the mobile computer based on the time on the Mobile Device Server.
Contact	<p>On Startup – Connect to the Mobile Device Server when the Enabler is accessed.</p> <p>On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.</p> <p>On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as being docked in a powered cradle.</p> <p>Periodic Update - 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.</p>
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 the Mobile Device Server.
Require external power	Only connect when the device has external power (connected to an AC adapter).

Startup/Shutdown Tab

LXE recommends using LXE AppLock for this function. AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in Chapter 6 *AppLock*.

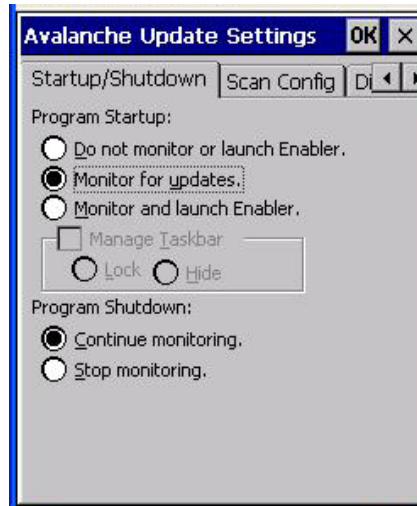
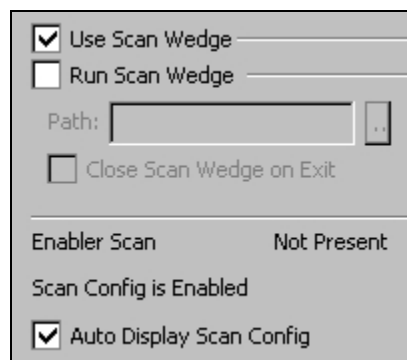


Figure 3-58 Avalanche Enabler Startup / Shutdown Options

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 3-59 Avalanche Enabler Scan Config Option

Display Tab



Figure 3-60 Avalanche Enabler Window Display Options

Update Window Display

The user interface 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 LXE AppLock for this function. AppLock is resident on each mobile device with a Windows OS.

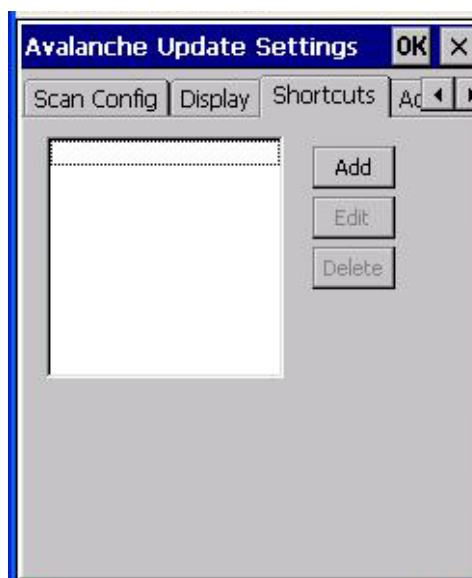


Figure 3-61 Avalanche Enabler Application Shortcuts

Configure shortcuts to other applications on the mobile device. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

LXE recommends using LXE AppLock for this function. See *Chapter 6 - AppLock* for instruction.

Adapters Tab

Note: LXE recommends the user review the network settings configuration utilities and the default values in Chapter 5 before setting All Adapters to Enable in the Adapters applet.

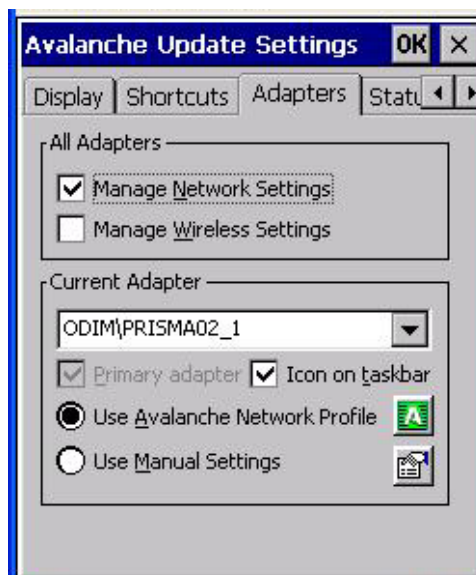


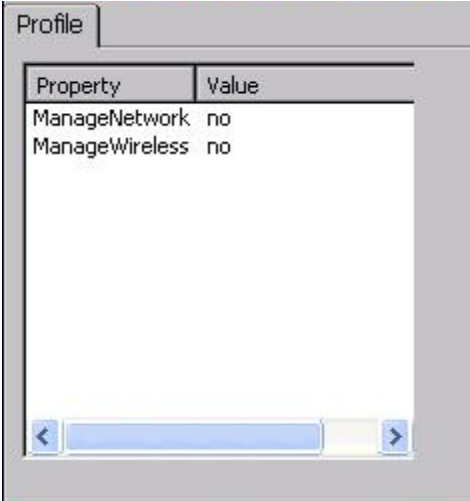




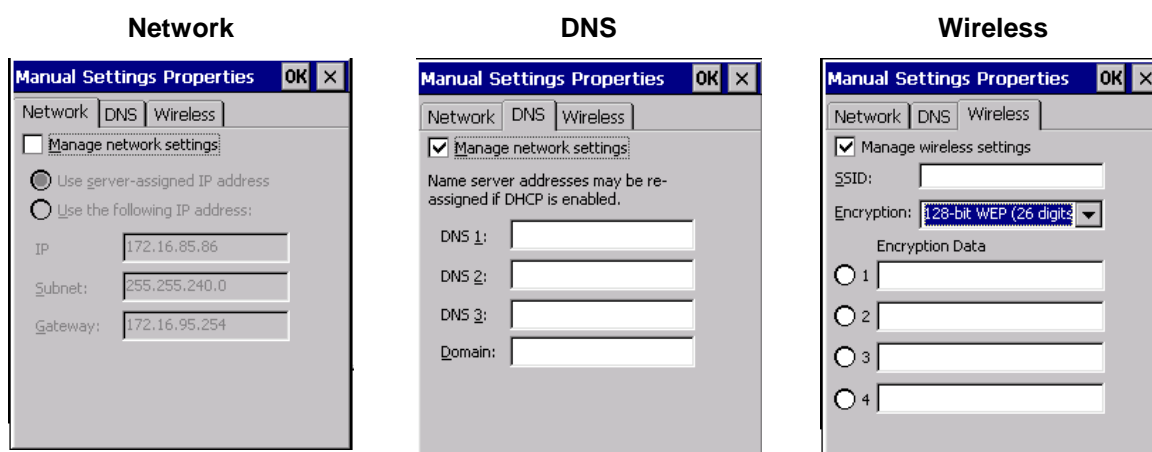
Figure 3-62 Avalanche Enabler Adapters Options - Network

Manage Network Setting	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Management Console and is disabled by default. This parameter setting does not apply to Summit Clients only .
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.

<div>Use Avalanche Network Profile</div>	<div>The Enabler will apply all network settings sent to it by the Management Console.</div> <div><div><input checked="" type="radio"/> Use Avalanche Network Profile </div></div>
<div>Avalanche Icon</div> <div></div>	<div>Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.</div> <div></div> <div>Figure 3-63 Avalanche Network Profile Displayed</div>

Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche Management Console and use only the network settings on the mobile device. 
Properties Icon 	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.



For device-specific descriptions of these Enabler parameters, refer to Chapter 5 “Wireless Network Configuration”.

LXE does not recommend enabling “Manage Wireless Settings” for Client devices.

Figure 3-64 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.

MX7 and Controlling Wireless Settings

Odyssey Client on the MX7

If the Odyssey Client on the LXE MX7 mobile device is the default client control application, follow these instructions. The Odyssey Client application cannot be automatically disabled by the Enabler. After the Enabler has made contact with the Mobile Device Server and if the Enabler is to control the wireless settings on the MX7 the administrator must:

1. Disable the Odyssey Client. Start the Funk Odyssey Client Configuration user interface by tapping the Odyssey Client icon on the MX7 desktop.
2. Tap Settings | Disable Odyssey. Select Exit. Perform a warm reset.
3. Download the wireless settings that are to be applied to the MX7.

4. Perform a warm reset on the MX7. Upon a successful reset, the Odyssey Client remains disabled and the Enabler is in control of the wireless settings.

To return control of the wireless settings to the Odyssey Client, perform a cold reset.

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.

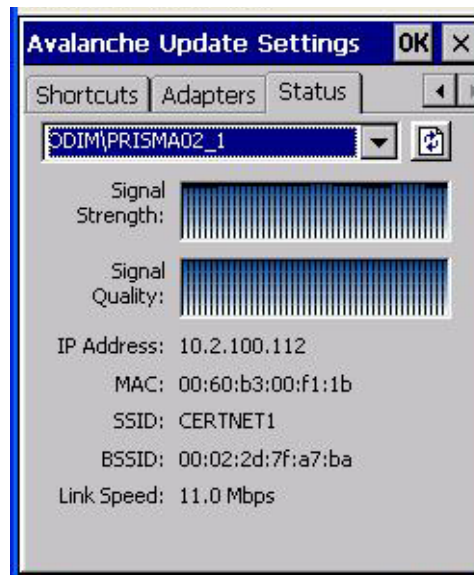


Figure 3-65 Status Display

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.

eXpress Scan

eXpress Scan may be used for the initial network configuration of the mobile device. Available configuration parameters can include wireless network settings and the Avalanche Mobile Device Server Address.

Barcodes are created with the eXpress Config utility. Please refer to *Using Wavelink Avalanche on LXE Windows Computers*, available on the LXE manuals CD, for information on eXpress Config. Depending on the barcode length and the number of parameters selected, eXpress Config generates one or more barcodes for device configuration.

To use eXpress Scan to configure an LXE device:

1. Start eXpress Scan on the LXE device by double tapping the eXpress Scan icon on the desktop.



Figure 3-66 eXpress Scan Desktop Icon

2. Enter the barcode password used when the barcode was created, if any.

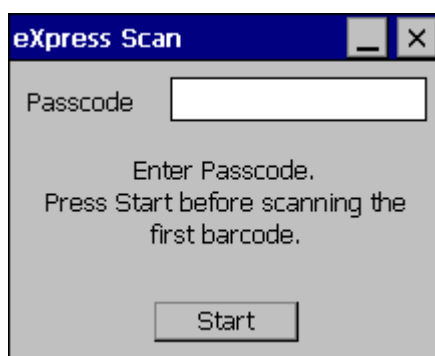
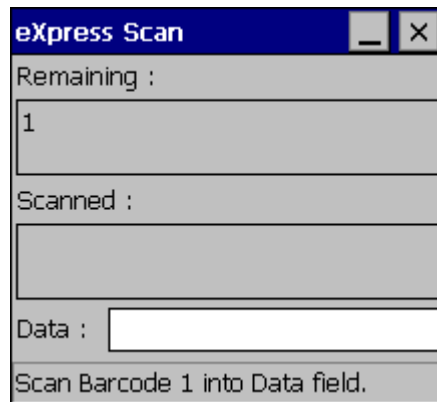


Figure 3-67 eXpress Scan Password Input

Tap **Start**.

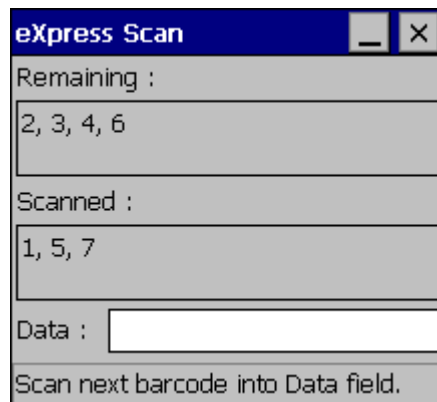
3. Barcode 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the barcodes were created.



The screenshot shows a window titled "eXpress Scan" with a blue title bar. Inside, there are three main sections: "Remaining :", "Scanned :", and "Data :". The "Remaining :" section contains a text box with the number "1". The "Scanned :" section contains an empty text box. The "Data :" section contains an empty text box. At the bottom of the window, there is a status bar that reads "Scan Barcode 1 into Data field."

Figure 3-68 Scan Barcode 1

4. If the passwords match, the barcode data is processed and the screen is updated to reflect the number of barcodes included in the set.



The screenshot shows the same "eXpress Scan" window. The "Remaining :" section now contains the text "2, 3, 4, 6". The "Scanned :" section now contains the text "1, 5, 7". The "Data :" section remains empty. The status bar at the bottom now reads "Scan next barcode into Data field."

Figure 3-69 Scan Remaining Barcodes

The remaining barcodes may be scanned in any order. After a barcode is scanned, that barcode is removed from the "Remaining:" list and placed in the "Scanned:" list.

5. If the passwords do not match, an error message is displayed. The current screen can be closed using the X in the upper right corner. The password can be re-entered and Barcode 1 scanned again.
6. Once the first barcode is scanned, the remaining barcodes may be scanned in any order.

7. After the last barcode is scanned, the settings are automatically applied.

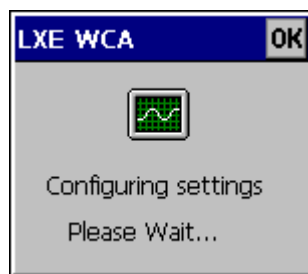


Figure 3-70 Configuring Settings

8. Once configured, the device is warmbooted and the new settings are active.
9. If Wavelink Avalanche is deployed and the appropriate network settings are configured, the device connects to the Mobile Device Server and any software updates and additional configuration data are downloaded.

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

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

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: MX7NK.BIN, MX7EBOOT.NB0, MX7.BIT

The MX7 reloads the operating system upon every warm boot or cold boot. Anything not saved or preserved to the registry is lost.

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

During cold boot, the system behavior is identical to warm boot with the addition that the registry is reloaded with factory defaults.

Preparation

- LXE recommends that installation of the Flash card be performed on a clean, well-lit surface.
- Place the mobile device in Suspend Mode and remove the main battery pack.
- Lift the rubber barrier and pull the SD card out of the slot.
- Locate the <A> key on the 55-key keypad.
- Locate the <Alph> key on the 32-key keypad.

How To

1. Place the SD flash card with new image files on it into the SD slot.
2. Select Start | Run and type Coldboot.
3. Before the splash screen appears, press and hold down the <A> key on the 55-key keypad. Press and hold down the <Alph> key on the 32-key keypad. Continue to hold the <A> or <Alph> key down until the displays shows “Writing bootloader to flash”.

Note: If you do not press and hold the key quickly enough, the display shows “Loading system from ATA”. Remove the main battery for 2 seconds, re-insert the battery and press the Power button. Press and hold the <A> or <Alph> key again.

4. The mobile device will automatically reboot after flashing the bootloader. “Loading system from ATA” is displayed on the screen and when the new OS finishes loading, all software upgrades are complete.
5. The touchscreen will need to be re-calibrated.

Once the bootloader is loaded and the files are copied onto the internal Flash drive, you can reflash the bootloader at any time by rebooting the MX7, and holding down the <A> or <Alph> key on the keypad before the splash screen appears.

Wait until the splash screen displays “Writing new bootloader”, and you can release the <A> or <Alph> key.

When reflashing is complete (3-5 seconds), the MX7 will reboot and startup with the new bootloader again.

Chapter 4 Scanner

Introduction

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

All options described in this chapter may not be available on your version of the Scanner control panel. When the Continuous Scan Mode option is available on your mobile device, the Scanner Control panels may appear different than those in this chapter. Contact your LXE representative for version updates and availability.

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 MX7 integrated scanner/imager *only*. Barcode manipulation parameters apply to barcodes scanned by the MX7 integrated scanner/imager engine *only*.

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.

Note: Barcode manipulation parameter settings in this chapter are also applied to the incoming data resulting from successful barcode scans sent to the MX7 for processing by LXE mobile Bluetooth scanners.

The MX7 may have one of three Symbol laser scan engines:

- Symbol SE824-I000A (see Note)
- Symbol SE955-I000WR
- Symbol SE1524

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 MX7 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 MX7 to scan engine-specific setup barcodes in the guide.

Note: The SE 955 scanner replaced the SE 824 scanner on all MX7’s manufactured after July 2006.

Determine Your Scanner Software Version



Integrated Scanner Programming Guide and the *Reset All barcode*. After scanning the Reset All (to factory defaults) barcode for the specific scan engine, the next step is **Start | Control Panel | Scanner**. Tap the OK button and close the scanner applet. This action will synchronize all scanner formats.

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX7 devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device. To identify the software version, tap the “About” icon in the Control Panel.


If the Barcode Tab looks like this	Go to
	<p>Chapter 3 “System Configuration” section titled “Scanner”</p>
It looks different	This chapter.

Figure 4-1 Scanner Control Panels

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.

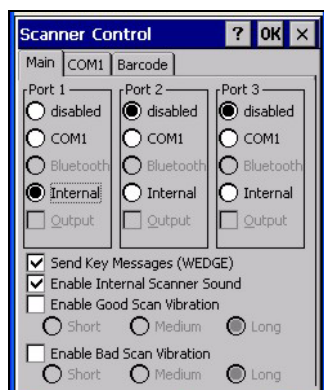
See “Barcode Processing Examples” at the end of the “Barcode Tab” section.

See “Appendix C – Reference Material”, section titled “Valid VK Codes for CE”.

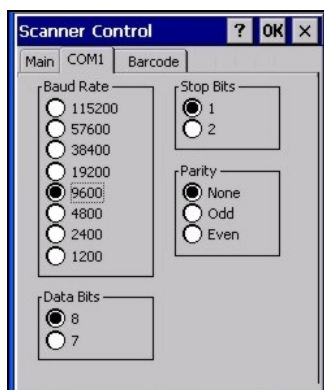
Factory Default Settings

Factory Default Settings	
Main	
Port 1	Internal
Port 2	Disabled
Port 3	Disabled
Send key messages (WEDGE)	Enabled
Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Disabled / Long
Bad Scan Vibration	Disabled / Long
COM1 Port (external serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Barcode	
Enable Code ID	None
Continuous Scan Mode	Disabled
Timeout between same symbol	1 second

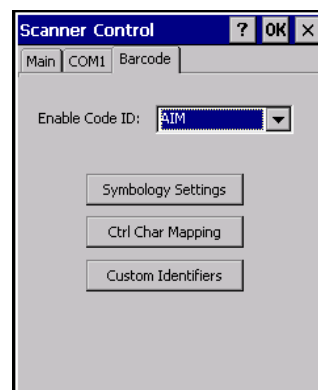
Factory Default Settings	
Vibration	
Good Scan Vibration	Off
Bad Scan Vibration	Off



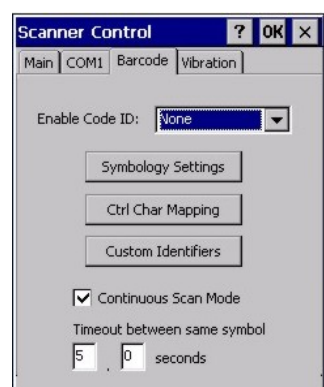
Main Tab



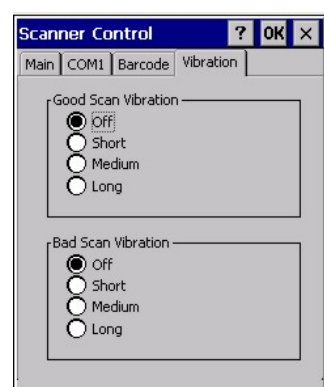
COM Tab



Barcode Tab



New Barcode Tab



Vibration Tab

Figure 4-2 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.

Main Tab

Access:  | Settings | Control Panel | Scanner | Main tab

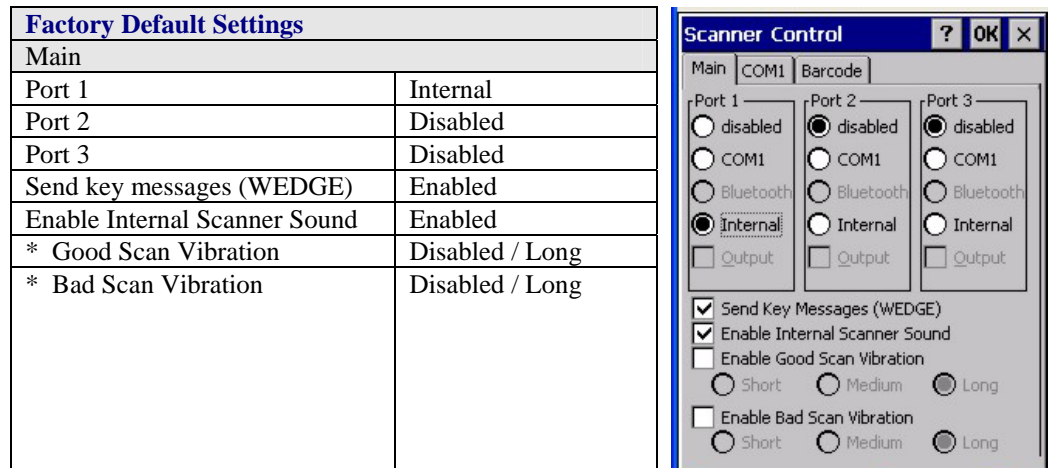


Figure 4-3 Scanner Control / Main

* Vibration checkboxes previously on the Main tab panel are located on the Vibration tab panel. 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)	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”.
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 MX7 on the same data.</p>

Parameter	Function
* Good Scan / Bad Scan Vibration	<p>The default setting is Disabled. Enable this parameter when a tactile response 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.</p> <p>Enable short, medium or long duration for each selection (good scan and bad scan).</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

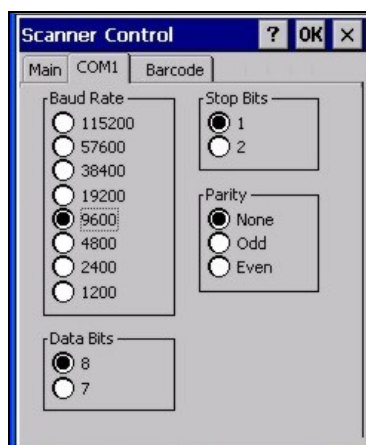


Figure 4-4 Scanner Control / COM1

Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity.

EV-15 scanner default values are 19200 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**

Barcode	
Enable Code ID	None
Continuous Scan Mode	Disabled
Timeout between same symbol	1 second

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.

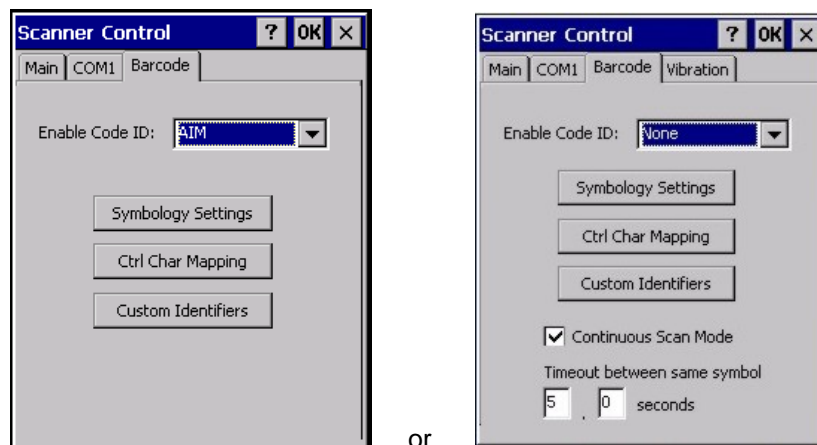


Figure 4-5 Scanner Control / Barcode tab

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.

Continuous Scan Mode

Access:  | **Settings | Control Panel | Scanner | Barcode tab**

Enabling Continuous Scan Mode will ensure the laser is always on and decoding.



Caution: *Laser beam is emitted continuously. Do not look or stare into the laser beam.*

Factory Default Settings	
Continuous Scan	
Continuous Scan Mode	Disabled
Timeout between same symbol	1 second

Set the Timeout between same symbol to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.

If trigger mode, power mode, or timeout between same symbol parameters are changed using external configuration barcodes in the *Integrated Scanner Programming Guide*, the operating system automatically restores the parameters to their programmed settings upon a warm or cold boot and/or any change made in the control panel.

When the scanner is in continuous mode the trigger and scan buttons function as a scanner On/Off switch.

The scanner red LED will always be off in continuous mode. The audio beeps and green LED work the same as they do for normal trigger mode.

Switching to and from continuous and normal trigger modes is in effect immediately upon pressing the OK button in this control panel, a warm boot is not required or necessary.

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 MX7 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 MX7 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 MX7**. 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.

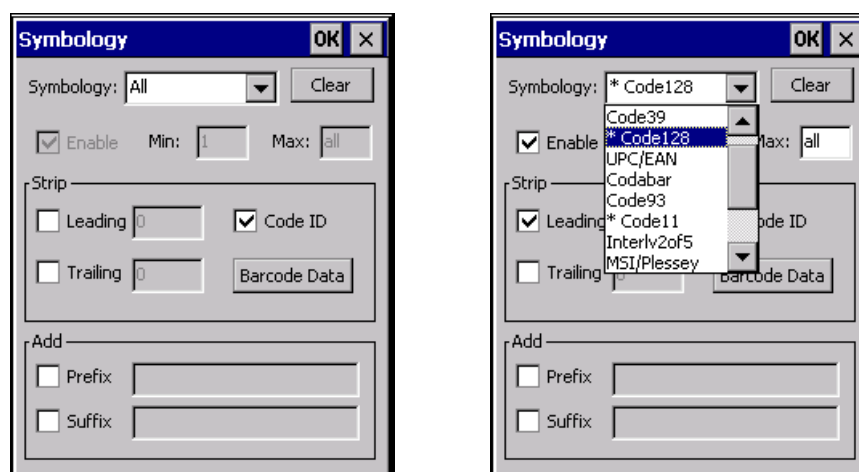


Figure 4-6 Barcode Tab / Symbology Settings

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 symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two. If a symbology has not been configured (does not have an * next to it) the settings for "All" are used which is not necessarily the 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 symbologies 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

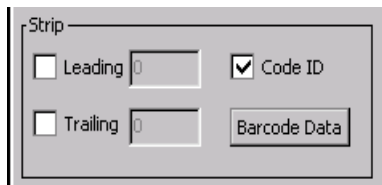


Figure 4-7 Symbology / Strip Leading / Trailing

This group of controls determines what data is removed from the barcode before the data is buffered for the application. If all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.

If the total number being stripped is greater than the number of characters in the barcode data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

- | | |
|-----------------|--|
| Leading | This strips the number of characters specified from the beginning of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default. |
| Trailing | This strips the number of characters specified from the end of the barcode data (not including Code ID). The data is stripped unconditionally. This is disabled by default. |
| Code ID | Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise). |

Barcode Data Match List

Barcode Data

This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.

To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap the OK button to store any additions, deletions or changes.

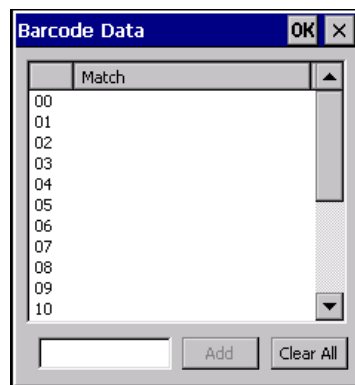


Figure 4-8 Symbology / Barcode Data Match List

Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The Add button changes to Insert . Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace . When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a 'good' beep will still 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.

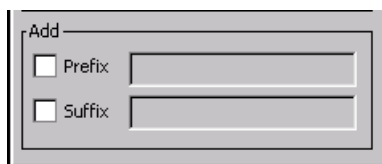


Figure 4-9 Symbology / Prefix and Suffix Control

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.

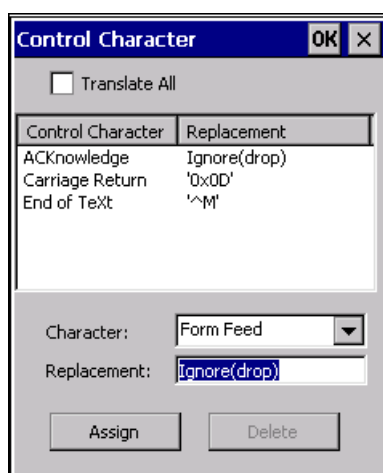


Figure 4-10 Barcode Tab / Ctrl Char Mapping

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	<p>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 <i>Ignore (drop)</i> is shown and highlighted in the Replacement edit control. <i>Ignore (drop)</i> 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 redisplayes the default <i>Ignore (drop)</i> in the Replacement edit control.</p>
Replacement	<p>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.</p> <p>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.</p> <p>The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.</p>
List Box	<p>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.</p>
Delete	<p>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.</p>

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).*

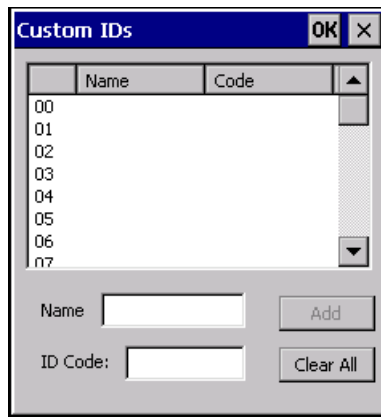


Figure 4-11 Barcode Tab / Custom Identifiers

After adding, changing and removing items from the Custom IDs list, tap the OK button to save changes and return to the Barcode panel.

Parameters

- Name** text box Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the **Name** and **ID Code** may have the same value. **Name** is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.
- ID Code** text box ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add	Entering data into both the Name and ID Code fields enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The Add button changes to Insert . Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a barcode is converted to the text 'STX'.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	'^M'	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	'\^I'	Value 0x09 in a barcode is converted to the text '^I'.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	'0x0A'	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '0\x0A'	Value 0x0C is a barcode is converted to text '0x0A'

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	EAN-128 (JC1)	EAN-13 (JE0)	Intrlv 2 of 5 (JIO)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-128	JC11234567890123	bbb1234567890xxx
EAN-128	JC111234567890123	bbb11234567890xxx
EAN-128	JC1123	< <i>rejected</i> > (too short)
EAN-13	JE01234567890987	cccJE04567890yyy
EAN-13	JE01231234567890987	cccJE0234567890yyy
EAN-13	JE01234	cccJE0yyy
I2/5	JIO4444567890987654321	< <i>rejected</i> > (too long)
I2/5	JIO4444567890123	ddd7890zzz
I2/5	JIO444	dddzzz
I2/5	JIO22245622	ddd45zzz
Code-93	JG0123456	< <i>rejected</i> > (disabled)
Code-93	JG0444444	< <i>rejected</i> > (disabled)
Code-39	JA01234567890	aaa4567890www
Code-39 full ASCII	JA41231234567890	aaa1234567890www
Code-39	JA4	< <i>rejected</i> > (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 rule 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:

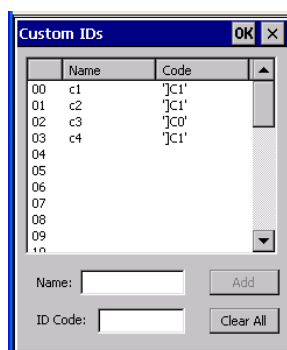
For the purposes of this example, the following sample barcode parameters will be used – EAN128 and Code128 barcodes. Some of the barcodes start with ‘00’ and some start with ‘01’. The barcodes are different lengths.

- 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’

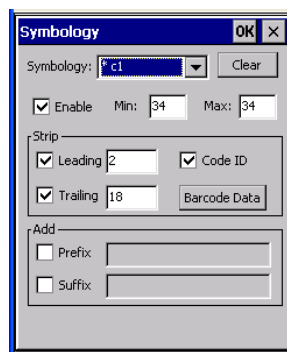


AIM Custom IDs

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"

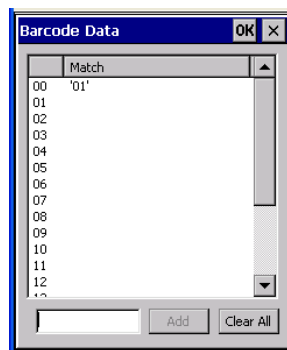
Add the AIM custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.



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

Vibration checkboxes previously on the Main tab panel are located on the Vibration tab panel.

Factory Default Settings	
Vibration	
Good Scan vibration	Off
Bad Scan vibration	Off

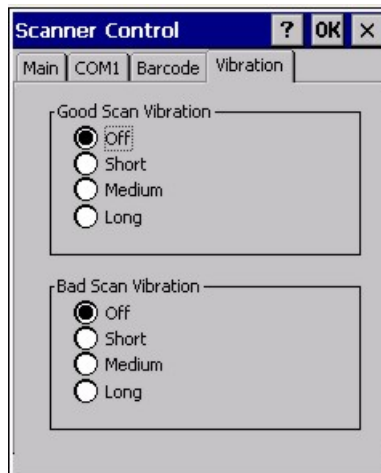


Figure 4-12 Vibration Tab

Enable this parameter when a tactile response on a good scan or bad scan is desired. Scan sounds are accompanied by a tactile response when the internal scanner Sound parameter is enabled.

Enable short, medium or long duration for each selection (good scan and bad scan).



Chapter 5 Wireless Network Configuration

Introduction

The MX7 mobile device uses the LXE 802.11 network card and either the Funk® Odyssey Client software on the mobile device or the Summit Client software. Both client software utilities support WEP encryption, WPA security, no authentication and all authentications listed below.

The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates **or** an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates.

The Odyssey Client device is an 802.11b/g network card, capable of both 802.11b and 802.11g data rates.

This chapter is separated into two sections: Funk Odyssey Client Configuration and Summit Client Configuration. Please refer to the table below for the security options supported by each client.

Security Options Supported	Summit Client (CE .NET 4.2 - 802.11b/g) (CE 5 - 802.11a / 802.11g)	Odyssey Client (CE .NET 4.2 - 802.11b/g)
No Security	Yes	Yes
WEP	Yes	Yes
LEAP	Yes	Yes
EAP-FAST	Yes	No
PEAP-MSCHAP	Yes	Yes
WPA/LEAP	Yes	Yes
WPA-PSK	Yes	Yes
PEAP-GTC	Yes	Yes
EAP-TLS	Yes	Yes

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.



Please refer to the *LXE Security Primer* to prepare the Authentication Server and Access Point for MX7 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.

Certificates are necessary for many of the WPA authentications. Please refer to the *Root Certificates* and *User Certificates* sections at the end of this chapter for more information on generating and installing certificates.

Summit Client Configuration



It may be necessary to upgrade client drivers in order to use certain Summit Client Utility (SCU) features and/or security options described in this chapter. Please contact your LXE representative for Summit driver update availability.

Note: Terminology used on your screen displays may be different than those shown in the figures in this chapter.

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: Perform a Warm Reset after adding a new profile or changing parameters of an existing profile to save the changed parameters in the registry. Perform a Warm Reset by using the Power key to first Suspend then Resume the mobile device.

Summit Client Utility

Access: **Start | Programs | Summit | SCU**
 or SCU Icon on Desktop
 or Summit Tray Icon in Taskbar (if present)
 or WiFi Icon in the Windows CE Control Panel (if present)



Figure 5-1 Summit Client Utility (SCU) Tabs

The **Main** tab provides information, the Admin Login and active config (profile) selection.

Profile specific parameters are found on the **Config or Profile** tab. The parameters on this tab can be set to unique values for each profile.

The **Status** tab contains information on the current connection.

The **Diags** tab provides utilities to troubleshoot the network card. Update Driver and Site Survey functions are not available in this release.


Global parameters are found on the **Global Settings or Global** tab. The values for these parameters apply to all profiles.

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.

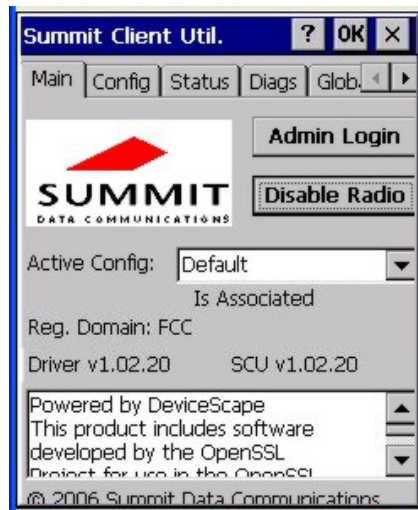


The signal strength for the currently associated/authenticated Access Point is stronger than -40 dBm.

Main Tab

Note: Terminology used on your screen displays may be different than those shown in the figures in this chapter.

Factory Default Settings	
Main	
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI



or



Figure 5-2 Summit Client Utility – Main tab

The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version.
- Driver version.
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11a/b/g radio).
- Regulatory Domain.
- Copyright Information by be accessed by tapping the About SCU button.
- Active Config / Active Profile profile name.
- Status of the network device (Down, Associated, Authenticated, etc).

The Active Config or Active Profile can be switched without logging in to Admin mode. A password is required before making changes to Summit client profile parameters. A password is not required to switch from one profile to another. LXE recommends performing a Suspend/Resume function after changing profiles.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module. See *Wireless Zero Config Utility* later in this chapter for Wireless Zero Config instruction.

The Disable Radio button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

The Admin Login button provides access to editing wireless parameters. Config / Profile and Global / Global Settings may only be edited after entering the Admin Login password. The

password is case-sensitive. Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Admin Login

To login to Admin 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 Admin 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 it is case sensitive) and tap OK. If the password is incorrect an error message is displayed.

The Admin default password can be changed on the Global or Global Settings tab.

The end user can:

- Turn the radio on or off on the Main tab.
- Select an Active Config / Active Profile on the Main tab screen.
- View the current parameter settings for the profiles on the Config / Profile tab.
- View the global parameter settings on the Global / Global Settings tab.
- The current connection details on the Status tab.
- Radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags tab.

After Admin login, the end user can also:

- Create, edit, rename and delete profiles on the Config / Profile tab.
- Edit global parameters on the Global / Global Setting tabs.

Config Tab

*Note: Tap the **Commit** button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!*

Factory Default Settings	
Config / Profile Panel	
Config / Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See section titled <i>Config/Profile Parameters</i> for Default
Auth Type	Open
EAP type	None
Encryption	None



or

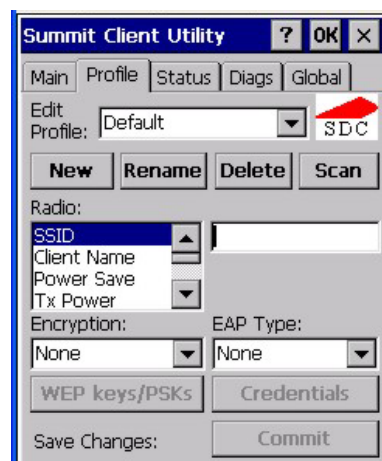
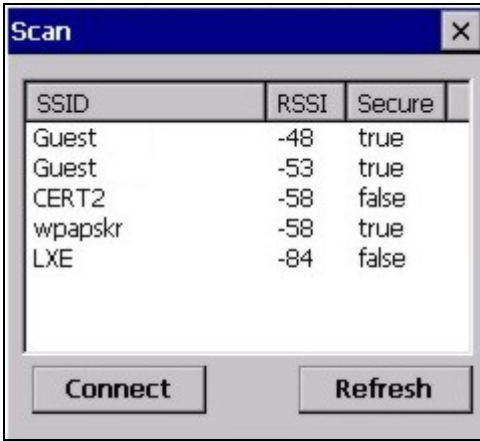


Figure 5-4 Summit Client Utility – Config / Profile tab

When logged in as Admin (see “Admin Login”), use the Config / Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in.

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.

Button	Function
New	Creates a new profile with the default settings (see <i>Config/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.
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></div> <p>Figure 5-5 SCU - Scan</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 create 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* -- Newer versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the Config or Profile tab.

Important – The settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security type chosen. Please refer to *Wireless Security* later in this Summit Client Utility section to determine the proper settings for the security type implemented on the wireless LAN.

Config / Profile Parameters

Parameter	Default	Explanation
Config or Profile	Default	<p>A string of 1 to 32 alphanumeric characters, establishes the name of the Config or Profile.</p> <p>Options are Default or ThirdPartyConfig.</p>
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the network card 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 devices, e.g. Access Points.
Power Save	Fast	<p>Power Save Mode is On.</p> <p>Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).</p>
Tx Power	Maximum	<p>Maximum setting regulates Tx power to the Max power setting for the current regulatory domain.</p> <p>Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW or 1mW.</p> <p><i>Note: Depending on the version of the SCU, the options for Tx Power are between Maximum and 1mW.</i></p>
Bit Rate	Auto	<p>Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device.</p> <p>Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.</p>

Parameter	Default	Explanation
Radio Mode	BG radio: BG Rates Full Or A radio: BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio (802.11b/g or 802.11a/b/g) installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) ABG Rates Full (All A rates and all B and G rates with A rates preferred) BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) Default: BG Rates Full (for 802.11b/g radios) BGA Rates Full (for 802.11a/b/g radio) <i>Note: BG radio only – Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.</i>

It is important this parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the LXE device may only connect to APs set for G rates and not those set for B and G rates.

The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	Radio Mode
A Main and BG Main	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Please contact your LXE representative if you have questions about the antenna(s) installed on your MX7.

Parameter	Default	Explanation
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.

Parameter	Default	Explanation
EAP Type	None	<p>Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point.</p> <p>Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, EAP-TLS or PEAP-GTC.</p> <p><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></p>
Encryption	None	<p>Type of encryption to be used to protect transmitted data.</p> <p>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.</p> <p><i>Note: The Encryption type chosen determines if the WEP/PSK Keys button is active and also determines the available entries in the WEP or PSK Pop-up window.</i></p>

Status Tab

This screen displays information on the current profile and client connection. Information cannot be edited or changed on the Status panel.

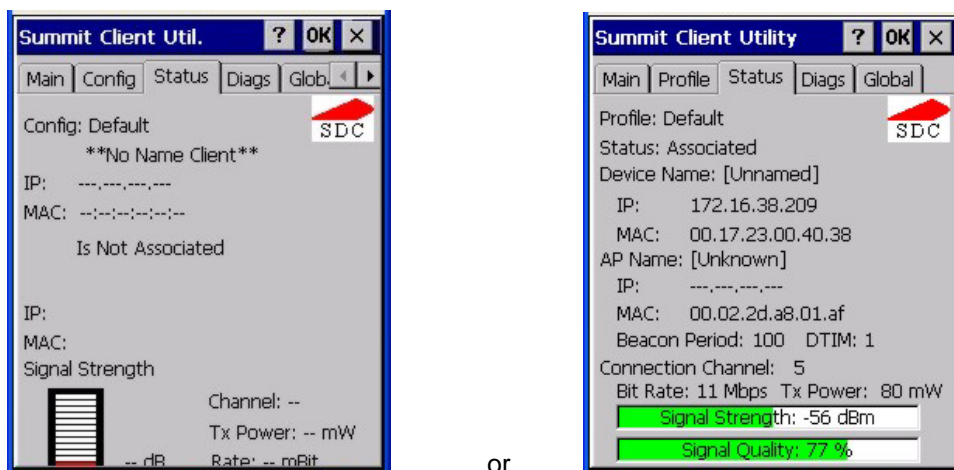


Figure 5-6 Summit Client Utility – Status tab

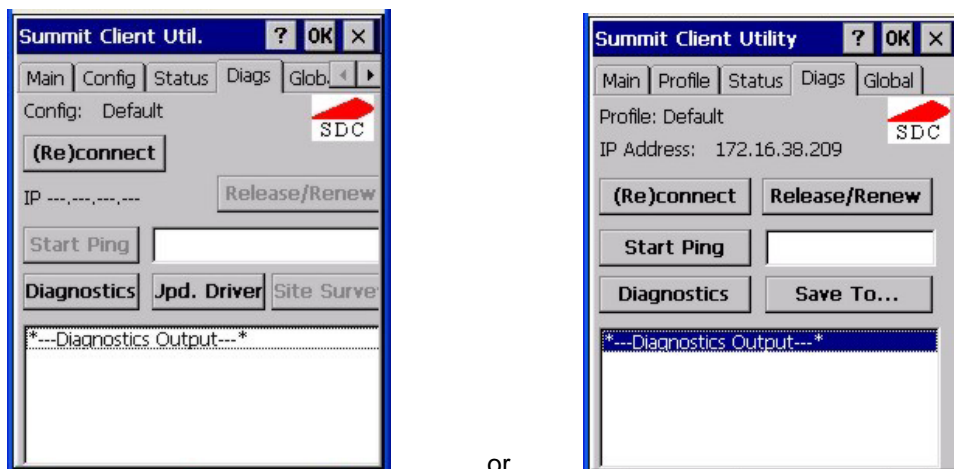
The panel displays:

- Config / Profile being used.
- The client name, IP address and MAC address.
- The status of the network connection (down, associated, authenticated, etc.).
- The name, IP address and MAC address of the Access Point maintaining the connection to the network.
- Channel currently being used for wireless traffic.
- Beacon period – the time between AP beacons in kilomicroseconds (1 kilomicrosecond – 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Current transmit power in mW.
- Rate in Mbps.
- Signal strength (RSSI) and signal quality (changes with network activity). Signal quality is a measure of the clarity of the signal and 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 network connectivity issues for the IP address shown. Admin login is required for the (Re)connect button function. It can also be used to update the client driver on the MX7 (this option is not available in all versions of the Summit driver). *Site Survey functions are not available in this release.*



or

Figure 5-7 Summit Client Utility – Diags tab

Buttons

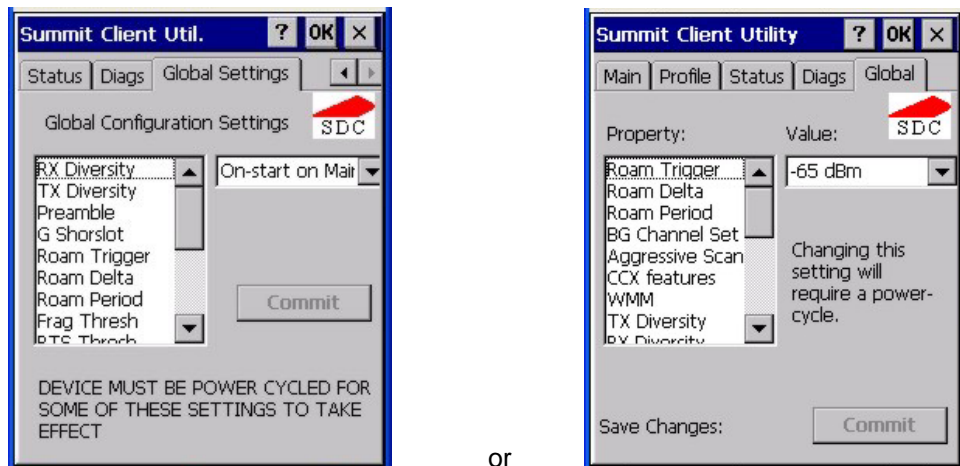
Button	Function
(Re)connect	Tap this button to apply, or reapply, the current config profile and attempt to associate or authenticate to the wireless LAN. Activity is logged in the Diagnostic Output text box on the lower part of the panel.
Release/Renew	Release the current IP address to obtain a new 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 client 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 client'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. <i>Not available in earlier releases.</i></p> <p>Tap the Save To button to save the Diagnostics log to a TXT file in the (default) My Device folder.</p>
Site Survey	<i>Not available in this release.</i>

Global or Global Settings Tab

The parameters on this panel can only be changed when an Administrator 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	BG: On-Start on Main A: Main Only
TX Diversity	BG: On A: Main Only
Preamble	Auto (not available in all versions)
G Short Slot	Auto (not available in all versions)
Roam Trigger	-65 dBm
Roam Delta	BG: 10 dBm A: 5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full (not available in all versions)
DFS Channels	Off (Not supported in this version)
Aggressive Scan	On (not available in all versions)
Frag Threshold	2346
RTS Threshold	2347
Ping Payload	32 bytes
Ping Timeout	5000
Ping Delay ms	1000
LED	Off
Hide Passwords	Off
Admin Password	SUMMIT (or Blank)
Auth Timeout	8 sec. (not available in all versions)
Certs Path	System
CCX	BG: Off A: Optimized
WMM	Off
Tray Icon	On (not available in all versions)



or

Figure 5-8 Summit Client Utility – Global Settings tab

Global Parameters

Custom Parameter Option

LXE does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Parameter	Default	Function
RX Diversity	BG radio: On-start on Main A radio: Main Only	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).

The options for the RX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	RX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On Start On Main
BG Main and BG Aux	On Start On Main

Please contact your LXE representative if you have questions about the antenna(s) installed on your MX7.

Parameter	Default	Function
TX Diversity	BG radio: On A radio: Main Only	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).

The options for the TX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	TX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On
BG Main and BG Aux	On

Please contact your LXE representative if you have questions about the antenna(s) installed on your MX7.

Parameter	Default	Function
Preamble	Auto	The type of network header, or preamble, for packets (not available in all versions). Options are: Auto, Short, or Long.
G Short Slot	Auto	802.1x short slot timing mode (not available in all versions). Options are: Auto, On, or Off. Note: The G Short Slot parameter has no effect on the Summit client device. This option is always set to On regardless of the parameter setting.
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	BG radio: 10 dBm A radio: 5 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	BG radio: 10 sec A radio: 5 sec	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.

Parameter	Default	Function
BG Channel Set	Full	<p>Defines the channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search roaming time may be reduced over scanning all channels.</p> <p>Options are: Full (all channels) / 1,6,11 (the most commonly used channels) / 1,7,13 (for ETSI and TELEC radios only) / Custom</p>
DFS Channels	Off	<p>Support for 5GHZ 802.11a channels where support for DFS is required.</p> <p>Options are: On, Off.</p> <p><i>Note: Not supported in this release.</i></p>
Frag Thresh	2346	<p>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 network interference.</p> <p>Options are: Any number between 256 bytes and 2346 bytes.</p>
RTS Thresh	2347	<p>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.</p> <p>Options are: Any number between 0 and 2347.</p>
Ping Payload	32 bytes	<p>Maximum amount of data to be transmitted on a ping.</p> <p>Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.</p>
Ping Timeout ms	5000	<p>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.</p> <p>Options are: Any number between 0 and 30000 ms.</p>
Ping Delay ms	1000	<p>The amount of time, in milliseconds, between each ping after a Start Ping button tap.</p> <p>Options are: Any number between 0 and 30000 ms.</p>
LED	Off	<p>The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device.</p> <p>Options are: On, Off.</p>

Parameter	Default	Function
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 text box. The password is Case Sensitive. Options are: none.
Certs Path	System	A valid Windows folder path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the folder path currently exists before assigning the path in this parameter. See sections titled “Root Certificates” and “User Certificates” later in this chapter for instructions on obtaining CA and User Certificates. 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	BG radio: Off A radio: Optimized <i>Note: In earlier versions, the default for BG radios was Off.</i>	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
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

Parameter	Default	Function
Aggressive Scan	On	<p>When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs (not available in all versions).</p> <p>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.</p> <p>Options are: On, Off.</p>
Auth Timeout	8 sec	<p>Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail (not available in all versions).</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 the Global panel is closed before tapping the Commit button, changes are not saved!

Summit Wireless Security

Use the instructions in this section to complete the entries on the Config or Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your System Administrator for complete information about your network and its wireless security requirements.

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.

Default profile	LXE recommends editing the Default profile instead of creating new profiles. Important: Perform a Warm Reset (using the Suspend/Resume key sequence) after changing parameters to save the changed parameters in the registry.
Switching profiles	Successfully connecting after switching from one profile to another may take up to 30 seconds from the moment the “Is not authenticated” or “Is not Associated” messages are displayed.
Adding, changing or renaming profiles	LXE recommends performing a Warm Reset function (Suspend/Resume key sequence) after tapping the Commit button.

Note: Unsaved changes – Newer versions of the SCU display a reminder if the Commit button is not tapped before an attempt to close or browse away from a panel when parameters had been changed.

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.

How to: Use Stored Credentials

1. After completing the other entries in the profile, tap 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.

Notes: 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.

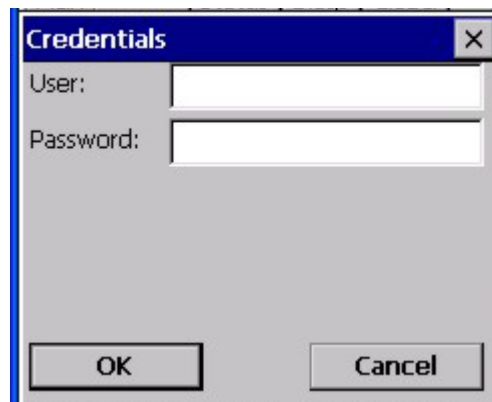


Figure 5-9 Sign-On Screen

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

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

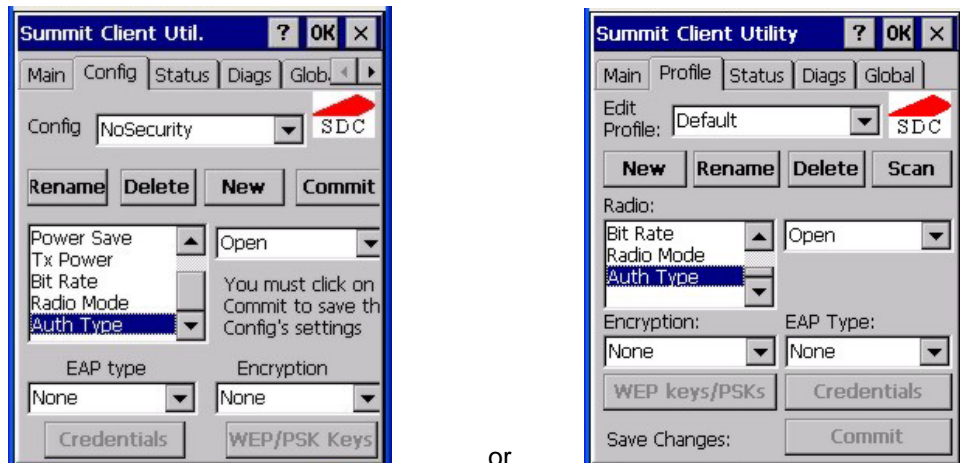
9. Follow the instructions later in this chapter for *Downloading a Root CA Certificate to a PC*.
10. Copy the certificate to the specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the **Certs Path** global variable. Please note the location chosen for certificate storage should persist after warmboot.
11. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
12. Enter the certificate name in the **CA Cert** textbox.
13. 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 Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.



or

Figure 5-11 Configure a Summit Profile with No Security

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to None.

Tap the **Commit**⁴ button to save the new profile configuration.

Perform a **Warm Reset** function to connect using the new profile configuration.

⁴ 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/PSK** Keys button. The WEP Key Entry text entry box appears.

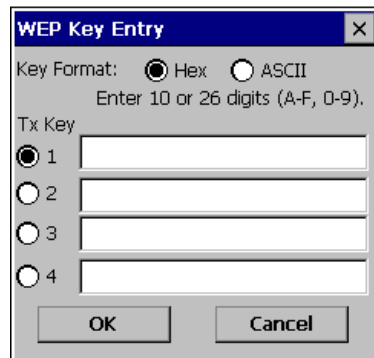


Figure 5-12 WEP Keys

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 AP is configured for open authentication, set the Auth Type client parameter to “Open”.

If the AP is configured for network EAP only, set the Auth Type client parameter to “LEAP”.

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.

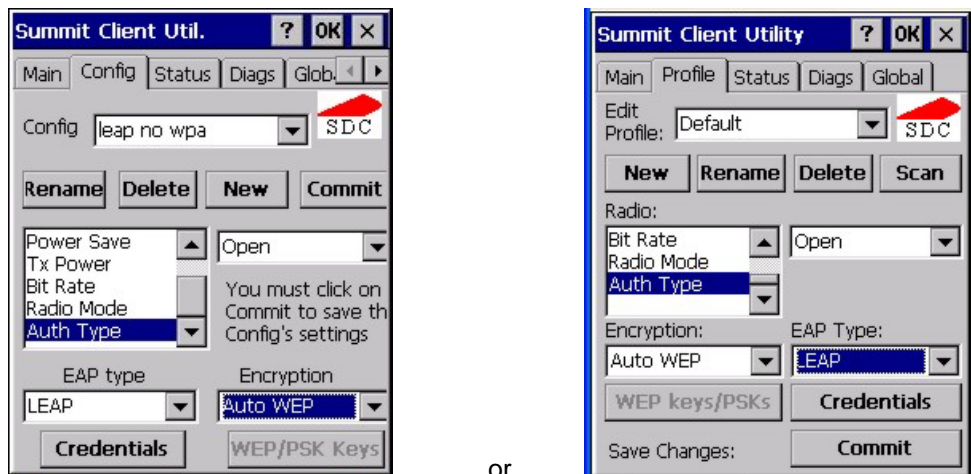


Figure 5-13 Configure a Summit Profile with LEAP w/o WPA

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.

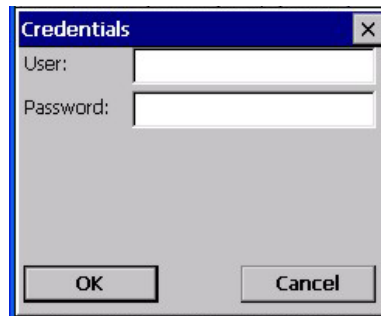


Figure 5-14 LEAP Credentials Dialog

Enter the **Username** or Domain \Username in the Credentials popup text entry box.

Enter the **Password**. Tap **OK**.

Tap the **Commit** button to save the new profile configuration.

Perform a **Warm Reset** function 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 Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.

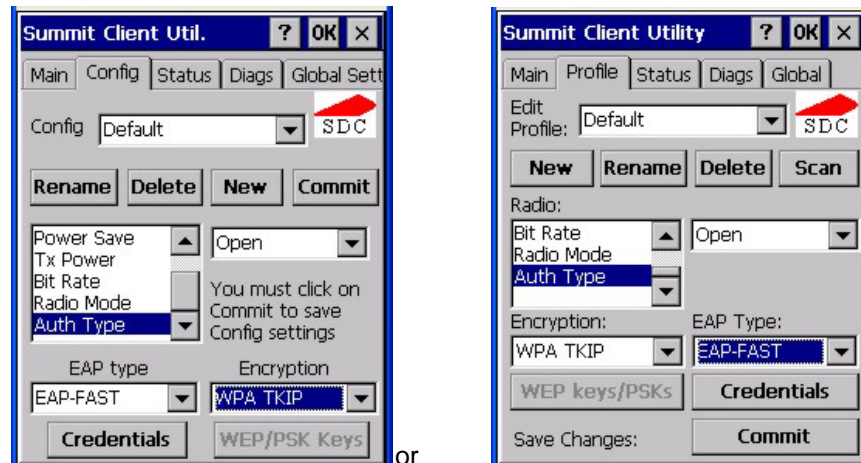


Figure 5-15 Configure a Summit Profile for EAP-FAST

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to EAP-FAST.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the client device. Please refer to the *LXE Security Primer* for more information on the RADIUS server configuration.

To use Stored Credentials, tap the **Credentials** button.

Note: 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.

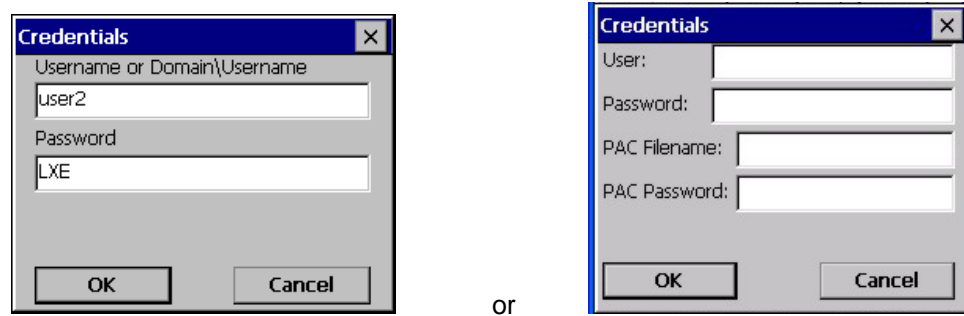


Figure 5-16 Summit EAP-FAST Credentials

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired.

Enter the **Password**, if desired. Tap **OK**.

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the mobile device. The same username/password must be used to authenticate each time. When using automatic PAC provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

For manual PAC provisioning, the PAC filename and password must be entered. The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be Read Only.

Tap OK then tap Commit to save the new profile configuration. Ensure the correct Active Profile is selected on the Main tab and perform a warmboot (or Suspend/Resume) function.

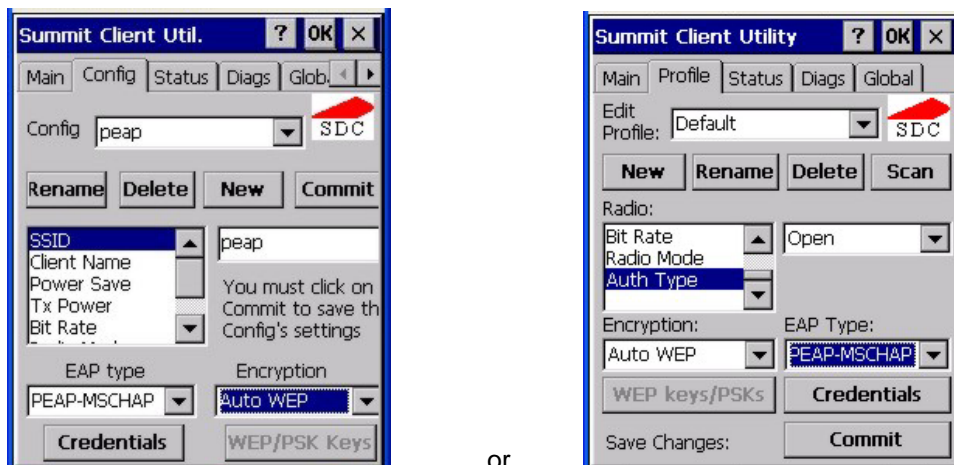
See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

PEAP/MSCHAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.



or

Figure 5-17 Configure a Summit Profile with PEAP/MSCHAP

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to PEAP-MSCHAP.

Set **Encryption** to Auto WEP (without WPA). To configure PEAP-MSCHAP for WPA set Encryption to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

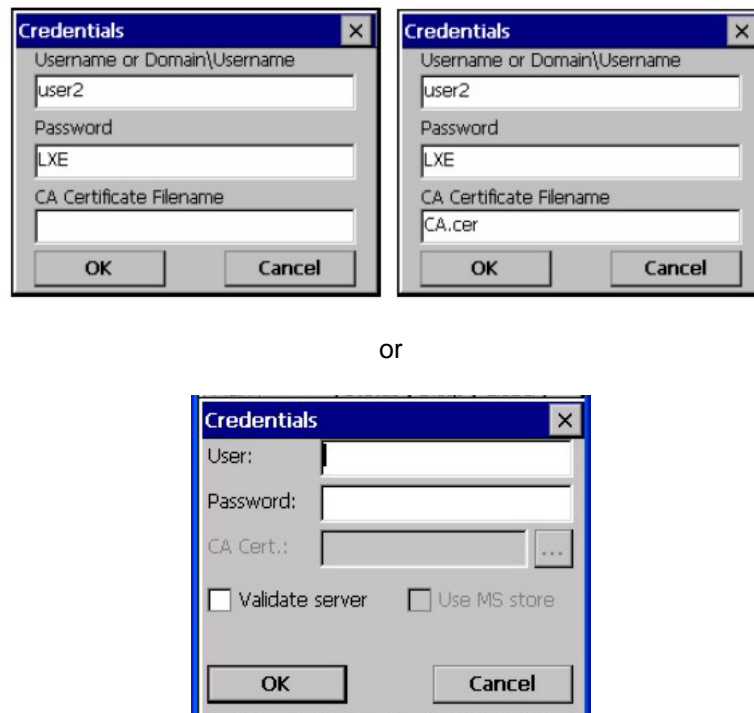


Figure 5-18 PEAP/MSCHAP Credentials Dialog

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.

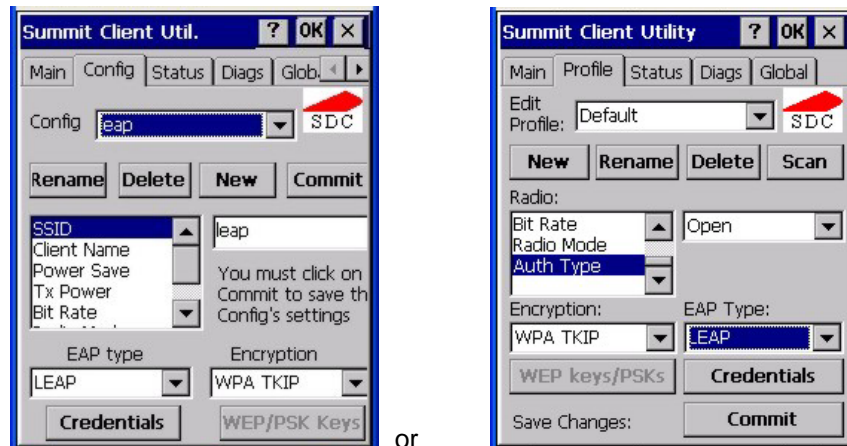
See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

WPA/LEAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.



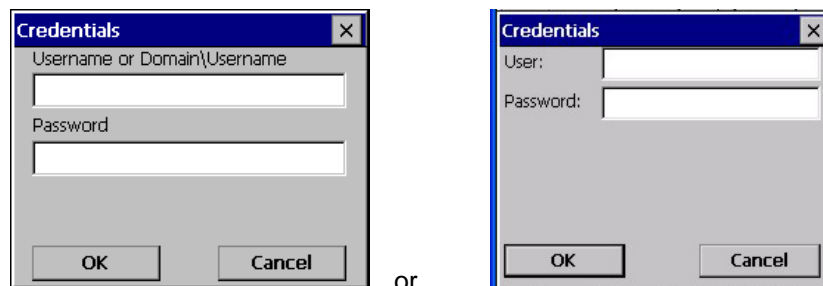
or

Figure 5-19 Configure a Summit Profile with LEAP w/ 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.



or

Figure 5-20 LEAP Credentials Dialog

Enter the **Username** or Domain \Username in the Credentials popup text entry box, if desired. Enter the **Password**, if desired. Tap **OK**.

Tap the **Commit** button to save the new profile configuration. Perform a **Warm Reset** (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.

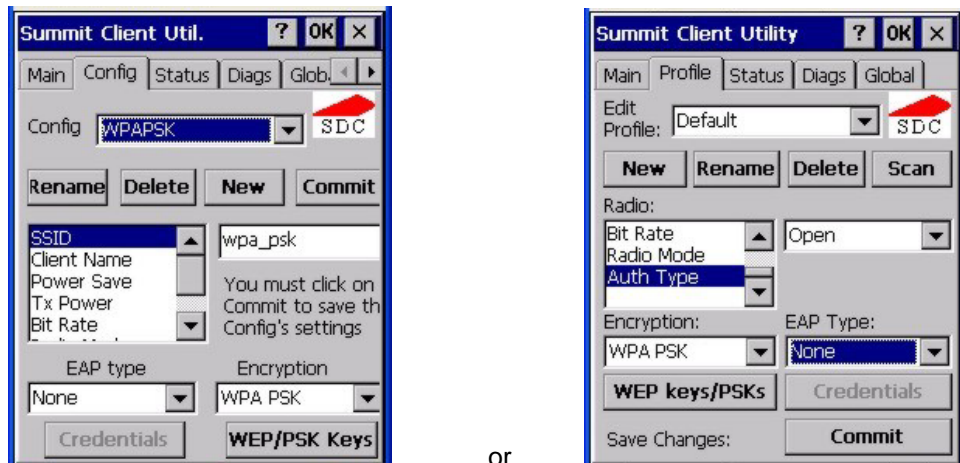
See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.



or

Figure 5-21 Configure a Summit Profile with WPA PSK Encryption

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to WPA PSK.

Tap the **WEP/PSK Keys** button.

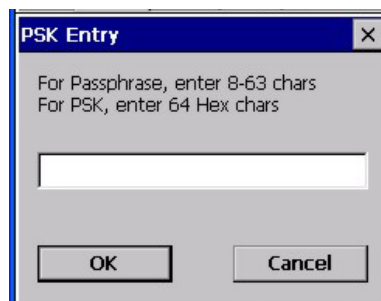


Figure 5-22 PSK Entry Dialog

Enter the Passphrase in the **PSK Entry** popup text entry box. This value can be a 64 hex character or an 8-63 byte ASCII value. Tap **OK**

Tap the **Commit** button to save the new profile configuration.

Perform a **Warm Reset** function 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 Admin Login **password** and tap OK.

Tap the **Config or Profile** tab.

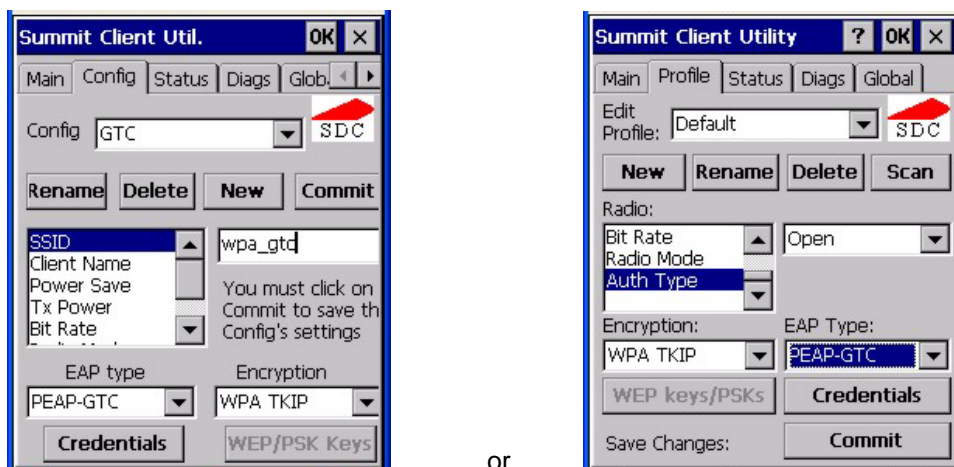


Figure 5-23 Configure a Summit Profile with PEAP/GTC

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.

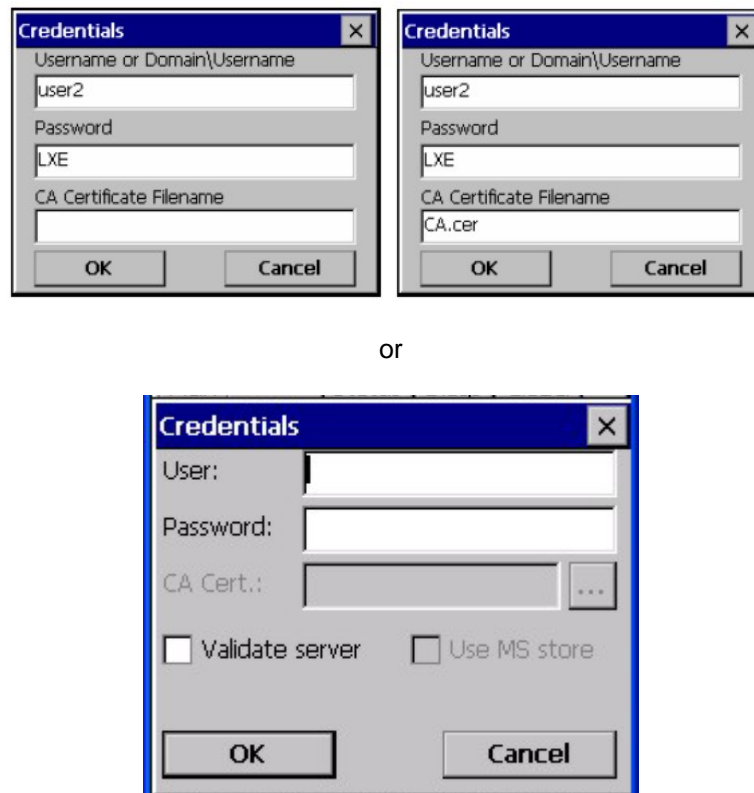


Figure 5-24 PEAP/GTC Credentials Dialog

Note: The date must be properly set on the device to authenticate a certificate.

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [. . .] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit**.

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

EAP-TLS Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Admin Login **password** and tap OK.

Tap the **Config** or **Profile** tab.

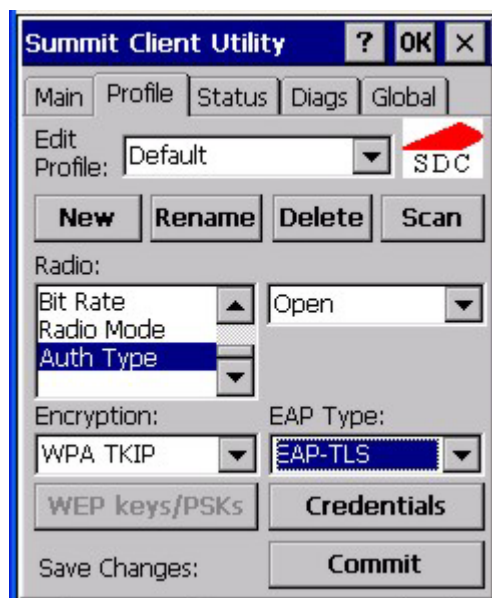


Figure 5-25 Configure a Summit Profile with EAP-TLS

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to EAP-TLS.

Set **Encryption** to WPA TKIP.

To use Stored Credentials, tap the **Credentials** button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network. If the username and password are left blank during setup, see *Sign-On vs. Stored Credentials* earlier in this chapter.

Note: The date must be properly set on the device to authenticate a certificate.

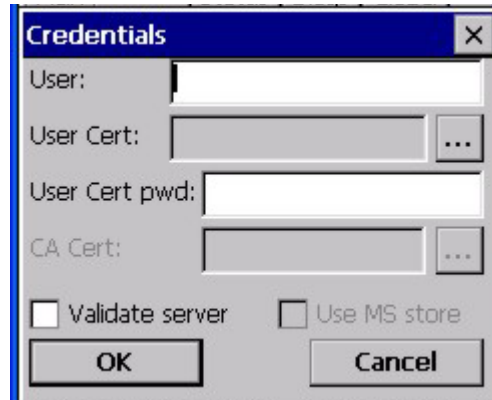


Figure 5-26 EAP-TLS Credentials Dialog

If using the **Windows certificate store**:

- Tap the Use MS store checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse [. . .] button.
- Uncheck the Use full trusted store checkbox.
- Select the desired certificate and tap Select. You are returned to the Credentials screen.

If using the **Certs Path option**:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Tap **OK** then tap **Commit**.

For information on generating a Root CA certificate, please see *Root CA Certificate* later in this chapter.

Perform a Warm Boot (or Suspend/Resume) function to connect using the new profile configuration.

The device should be authenticating the server certificate and using EAP-TLS for the user authentication.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

Funk Odyssey Client Configuration



Odyssey Client Icon

Start the Funk Odyssey client configuration by tapping the Odyssey Client icon on the desktop or in the taskbar at the bottom right corner of the screen.



To create a **Funk Odyssey Client user login**, please refer to Chapter 3 “System Configuration”, section titled “LXE Login Utility.”

For additional information on the Odyssey client see the Funk web site at www.funk.com.

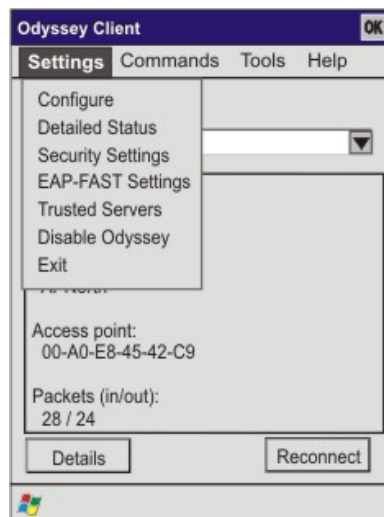
Note: LXE recommends using the Funk Odyssey client to configure the client device. Wireless Zero Config is not recommended for configuring the client device, although it can be used to reveal the IP address.

Prerequisites

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

Odyssey Client Menu

Settings



Factory Default Settings	
Settings	
<i>Configure</i>	
Networks	Blank
<i>Detailed Status</i>	
	Refresh
<i>Security Settings</i>	
Session Resumption	12 hours, Enabled
Automatic Reauthentication	Disabled
Temporary Trust	12 hours, Enabled
<i>EAP-FAST Settings</i>	
Acquire credentials from new server	Enabled
Replace credentials upon failure	Enabled
<i>Trusted Servers</i>	
	Blank
<i>Disable Odyssey</i>	Immediate disabling
<i>Exit</i>	

Figure 5-27 Odyssey Client Screens – Settings

Configure	Use this option to edit, add and delete networks.
Detailed Status	Configure advanced security options related to authentication.
Security Settings	This option allows the user to enable session resumption, automatic reauthentication and server temporary trust.
EAP-FAST Settings	Configure Odyssey to prompt for permission before acquiring new EAP-FAST credentials.

Trusted Servers	Use this option to edit, add and delete trusted servers and server certificates.
Disable Odyssey	Tapping this menu option disables Odyssey immediately. Odyssey should be disabled before setting Wireless Zero Config options.
Exit	Immediately exits the Odyssey client utility. Changes are saved when the panel closes. The Odyssey icon remains in the toolbar.

Commands

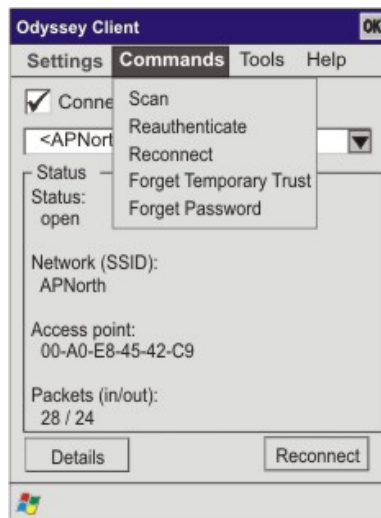


Figure 5-28 Odyssey Client Screens – Commands

Scan	Displays a list of all wireless networks that are currently reachable.
Reauthenticate	Selecting this option causes the Odyssey Client to reauthenticate your client over the existing connection without starting a new connection. If dynamic encryption keys are in use, they are refreshed.
Reconnect	The existing AP connection is disconnected and a new connection process to the selected wireless network is started.
Forget Temporary Trust	Use this command to immediately discard the list of temporarily trusted servers.
Forget Password	Use this command to immediately discard any typed passwords. This will remove them from memory.

Tools

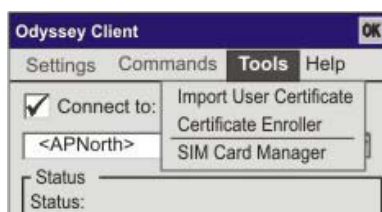


Figure 5-29 Odyssey Client Screens – Tools

Import User Certificate	See section titled “User Certificates” for instruction.
Certificate Enroller	Use this option to request a certificate from a server. See section titled “Root Certificates” for instruction.
SIM Card Manager	Manage the PIN on the SIM card hardware (if installed).

Help

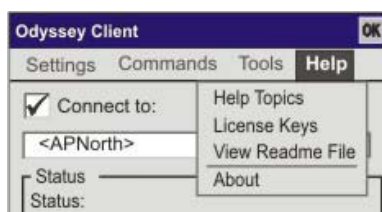



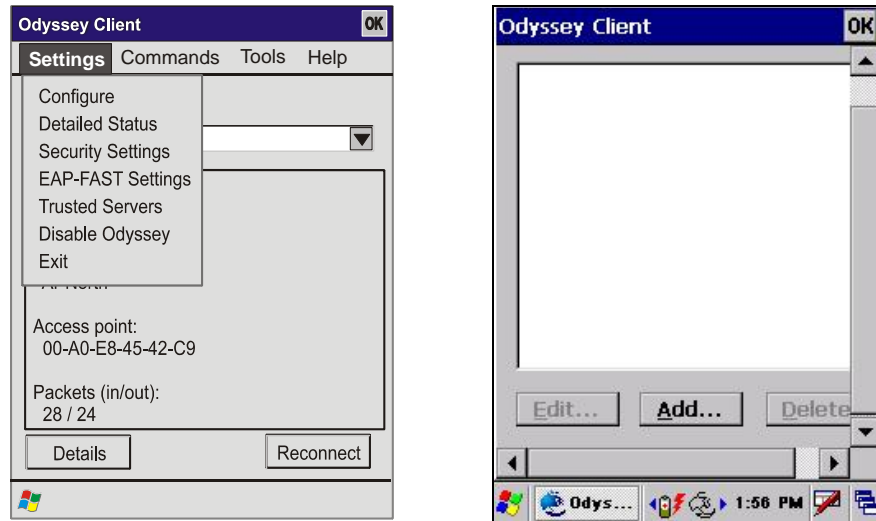
Figure 5-30 Odyssey Client Screens – Help

Help Topics	Odyssey local help.
License Keys	Displays a text sequence that represents the Odyssey Client software license. An option is available to enter a new license key.
View Readme Files	Readme.txt file is displayed.
About	Displays Odyssey Client version number and software license information.

Wireless Security

 Date/Time	<p>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.</p>
--	--

Set WEP



Funk Odyssey Client Settings Menu

Tap Add to Configure a Profile

Figure 5-31 Funk Odyssey Client Settings Menu

Start the Funk Odyssey client configuration by tapping the Odyssey Client icon.

Tap **Settings** | **Configure**.

Tap the **Add** button to configure a profile. The “Add Network Wizard” screen is displayed.

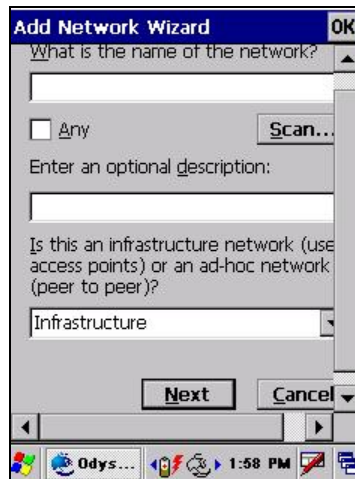


Figure 5-32 Add Network Wizard Screen

On the Add Network Wizard screen enter the **SSID** of the wireless network. If the SSID is being broadcast by the AP, tap Scan and choose the correct SSID.

Choose **Infrastructure** for the network type. Tap the Next button to continue or the Cancel button to ignore changes made on this screen.

No Encryption

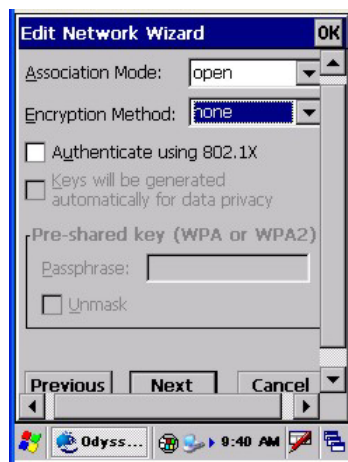


Figure 5-33 Set Encryption Mode to None

Set the **Association Mode** to Open. Set the **Encryption Method** to None. Disable the **Authenticate using 802.1X** checkbox. Disable the **Keys will ...** checkbox if needed.

Tap Next to continue. Status shows as “open”. Authentication is not in use. Encryption is not in use.

WEP Encryption

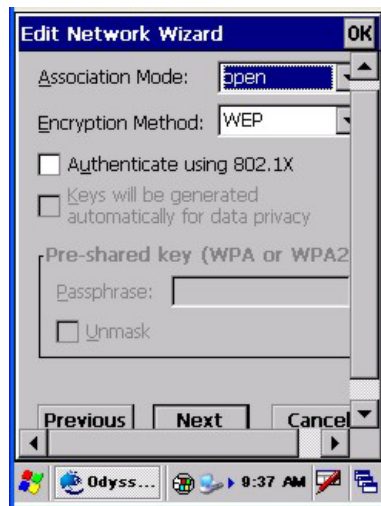


Figure 5-34 Set Encryption Mode to WEP

Set the **Association Mode** to Open.

Set the **Encryption Method** to WEP.

Disable the **Authenticate using 802.1X** checkbox.

Disable the **Keys will ...** checkbox if needed. Tap Next to continue.

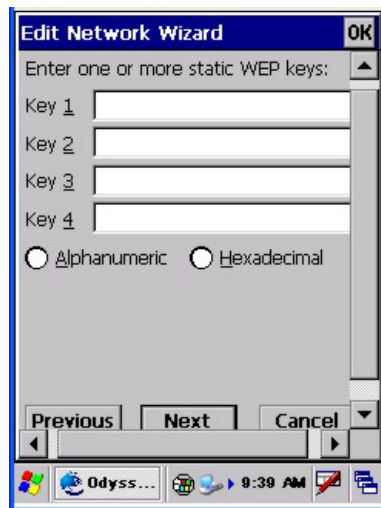


Figure 5-35 Setting Static WEP Keys

Enter a 40 bit or 128 bit WEP key. The default is blank for all keys and radio buttons.

If the WEP key is in *alphanumeric* format, enable the Alphanumeric radio button.

- 40 bit up to 5 characters
- 128 bit up to 13 characters

If the WEP key is in *hexadecimal* format, enable the Hexadecimal radio button.

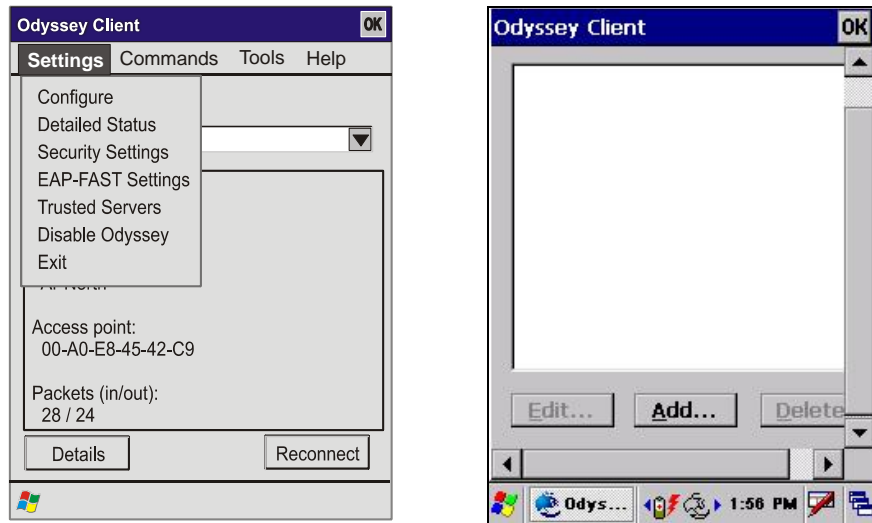
- 40 bit up to 10 characters
- 128 bit up to 26 characters

Enter the WEP key and tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.

After pressing Next, tap Finish to return to the Profile screen.

Tap OK to end assigning WEP for security.

Set LEAP



Funk Odyssey Client Settings Menu

Tap Add to Configure a Profile

Figure 5-36 Funk Odyssey Client Settings Menu

Start the Funk Odyssey client configuration by tapping the Odyssey Client icon.

Tap **Settings** | **Configure**.

Tap the **Add** button to configure a profile. The “Add Network Wizard” screen is displayed.

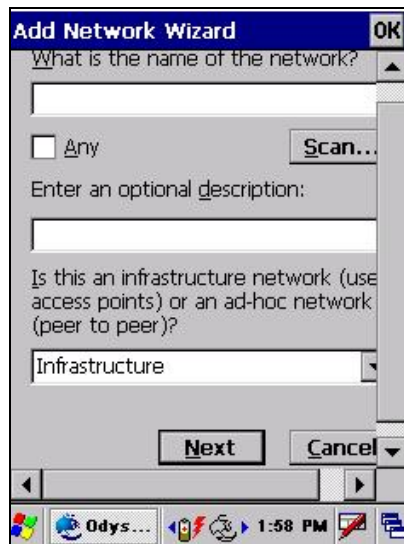


Figure 5-37 Add Network Wizard Screen

On the Add Network Wizard screen enter the **SSID** of the wireless network. If the SSID is being broadcast by the AP, tap Scan and choose the correct SSID.

Choose **Infrastructure** for the network type. Tap the Next button to continue or the Cancel button to ignore changes made on this screen.

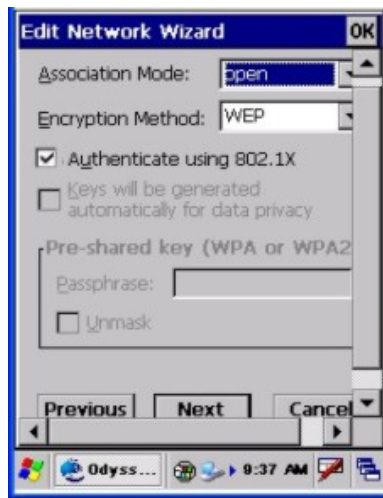


Figure 5-38 Set Encryption Mode to LEAP

Set the **Association Mode** to Open.

Set the **Encryption Method** to WEP.

Enable the **Authenticate using 802.1X** checkbox.

Enable the **Keys will ...** checkbox. Tap **Next** to continue.

WEP Authentication for LEAP

The Funk Odyssey supplicant authenticates a user with the LEAP protocol. Your system may have EAP-LEAP and/or LEAP in the method drop down list. EAP-LEAP protocol can be used for LEAP authentication.

Use the remove and add buttons to choose EAP-LEAP authentication. EAP-LEAP does not use server side authentication so the Validate server box is dimmed. Tap **Next**.



Figure 5-39 EAP-LEAP Method



Figure 5-40 Create Username and Password Method

Enter a Username.

For the username Password tap the radio button for either **Prompt for password** or **Use the following password**.

Tap the **OK** button then **Finish**.

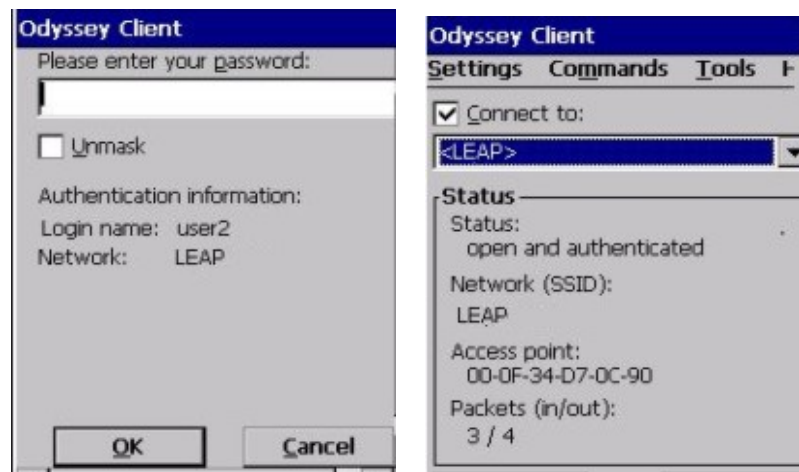


Figure 5-41 Enter Password for LEAP

When prompted for the password enter the valid password to authenticate.

Once authenticated the Status shows as “open and authenticated”.

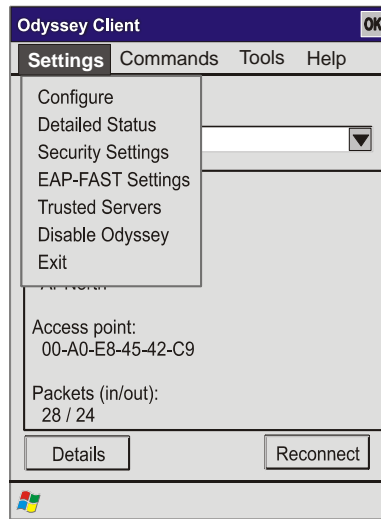
Set WPA

Figure 5-42 Funk Odyssey Client Settings Menu

Tap **Settings** | **Configure**.

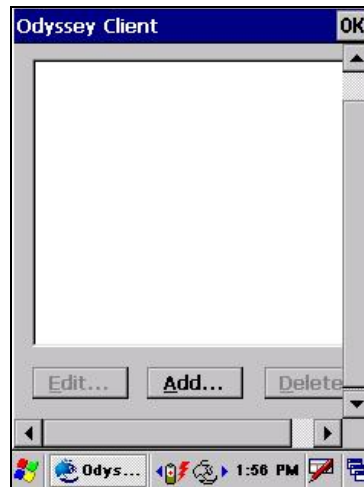


Figure 5-43 Tap Add to Configure a Profile

Tap the **Add** button to configure a profile. The “Add Network Wizard” screen is displayed.

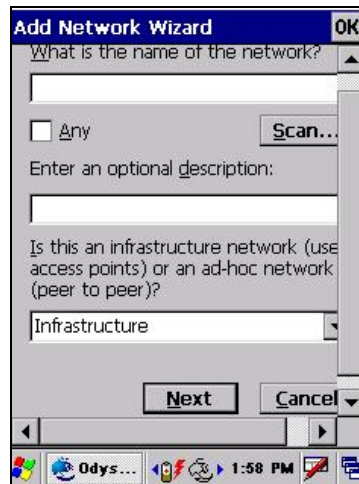


Figure 5-44 Add Network Wizard Screen

On the Add Network Wizard screen enter the **SSID** of the wireless network. If the SSID is being broadcast by the AP, tap Scan and choose the correct SSID.

Choose **Infrastructure** for the network type. Tap the Next button to continue or the Cancel button to ignore changes made on this screen.

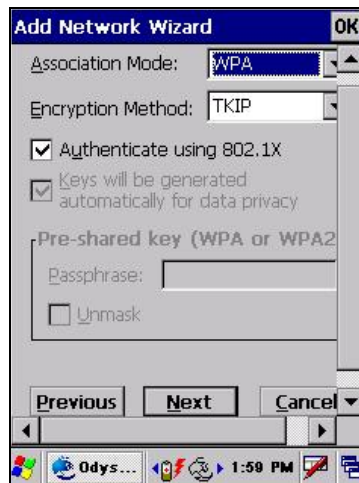


Figure 5-45 Set Association Mode to WPA

Set the **Association Mode** to WPA.

Set the **Encryption Method** to TKIP.

For all WPA authentications except WPA/PSK check the **Authenticate using 802.1X** box.

The **Keys will ...** box will be grayed out when the Encryption Method is set to TKIP.

In the following sections each authentication method configuration is described. Tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.

PEAP/MS-CHAP Authentication Configuration

The Funk Odyssey supplicant authenticates a user with the PEAP/MS-CHAP protocol.

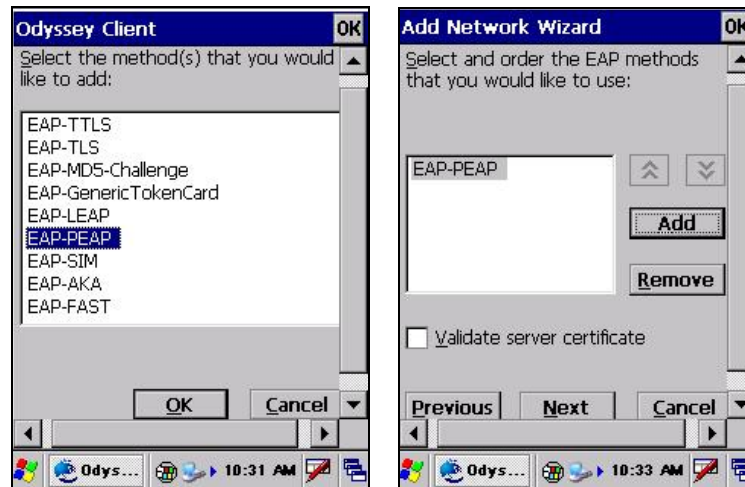


Figure 5-46 Select Method

Use the delete and add buttons to choose EAP-PEAP authentication.

Uncheck the Validate server certificate for now.

Tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.



Figure 5-47 User Name for Phase 1 Authentication

A screen appears asking for an **anonymous sign-on name**. This is for the outer (or Phase 1) authentication.

Enter the correct outer authentication (this could be the Phase 2 authentication as well).

Tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.

The next screen displayed is a configuration screen that allows you to choose the correct version of PEAP.

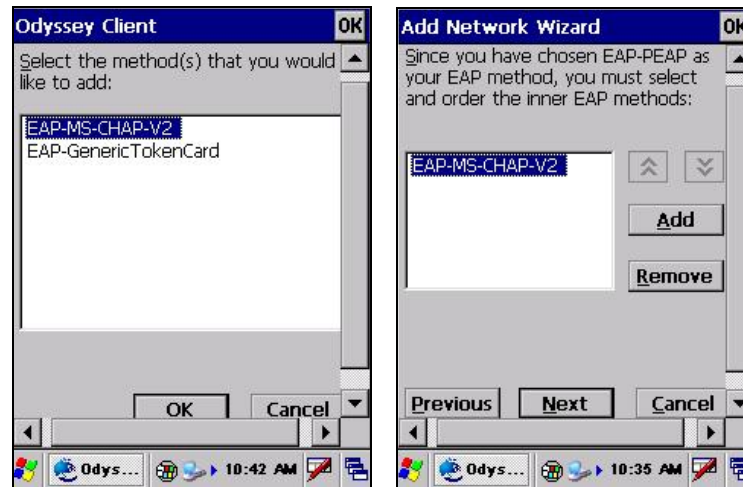


Figure 5-48 Select EAP-MS-CHAP-V2

For PEAP/MS-CHAP use the Add/Remove buttons to choose EAP-MS-CHAP-V2.

Tap **Next** to continue, **Previous** to return to the previous screen or **Cancel** to ignore changes made to this screen.



Figure 5-49 User Name and Password for Phase 2 Authentication

A screen appears asking for a user name. This is for the inner (or Phase 2) user name.

Under Password, choose “Prompt for password” or “Use the following password” radio buttons.

Tap the **OK** button.

Then tap **Finish** on the “The configuration of the new network is complete.” screen.

On the main configuration screen check the **Connect to** box and choose the profile just configured.

Once connected the status should change to open and authenticated as shown in the figure below.

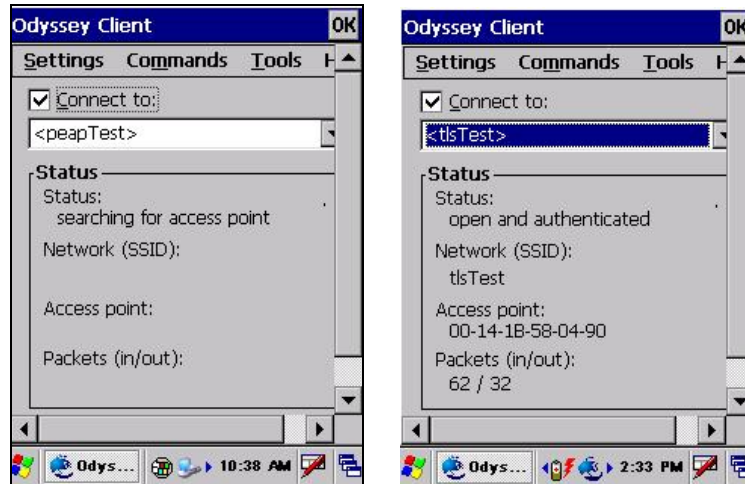


Figure 5-50 Connect to New Profile

Now that the connection works change the configuration to authenticate the server. See “Server Authentication.”

Server Authentication

To validate the server certificate the root CA certificate must be installed. For instructions for installing see section titled “Root Certificates”.

The RADIUS server certificate is not required, only the root CA which issued the server certificate.

Next configure the Root CA Certificate as a Trusted Root CA as described in the section titled “Trusted Server Configuration”.

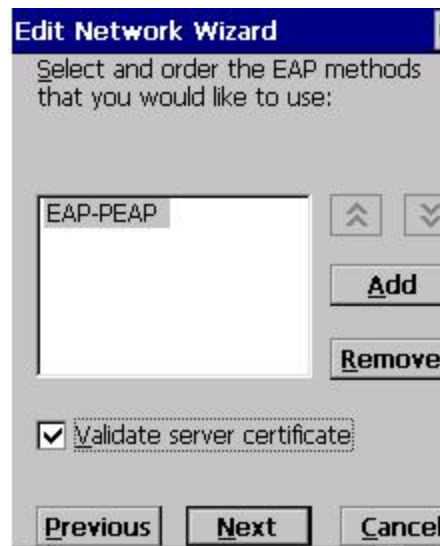


Figure 5-51 Validate Server Certificate

Navigate back to the authentication type screen and check the **Validate server certificate** box.

Tap **Next** to the end then the **Finish** buttons.

Tap **OK** to end the configuration process.

PEAP/GTC Authentication Configuration

The Funk Odyssey supplicant authenticates a user with the PEAP/GTC protocol. Use the delete and add buttons to choose PEAP/GTC authentication.

Uncheck the Validate server certificate for now.

Tap **Next**.

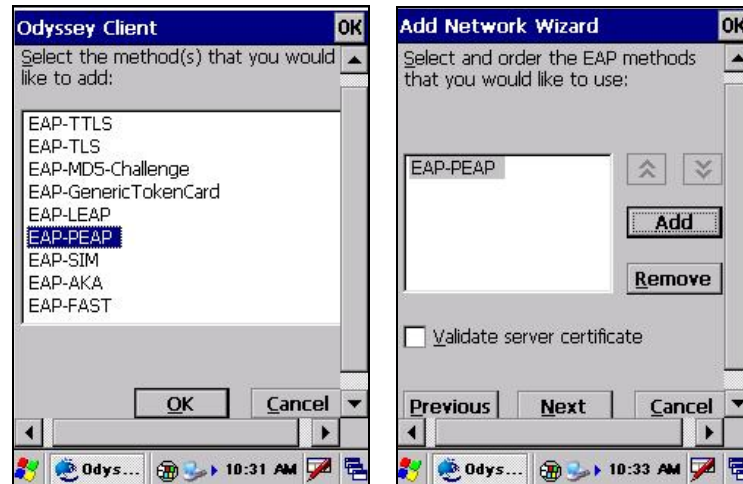


Figure 5-52 PEAP/GTC Authentication Configuration

Tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.



Figure 5-53 User Name for Outer Authentication

A screen appears asking for an **anonymous sign-on name**. This is for the outer (or Phase 1) authentication. Enter the correct outer authentication (this could be the Phase 2 authentication as well). Tap **Next** to continue, Previous to return to the previous screen or Cancel to ignore changes made to this screen.

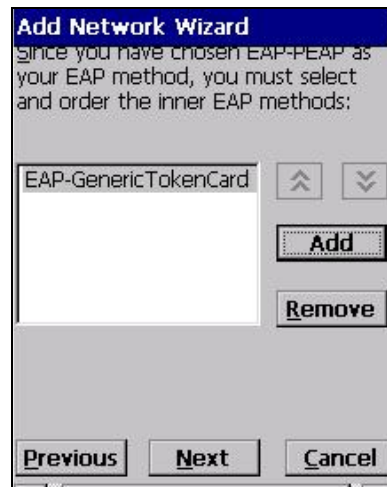


Figure 5-54 Choose Correct Version of PEAP

By choosing EAP-PEAP another configuration screen appears to chose the correct version of PEAP.

For PEAP/GTC use the Add/Remove buttons to choose **EAP-GenericTokenCard**.

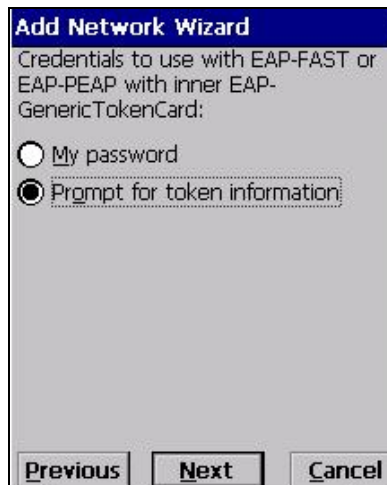


Figure 5-55 EAP-PEAP Credential Choice

Choose correct credential configuration.

To be prompted for the token, tap the "Prompt for token information" radio button.



Figure 5-56 Prompt for Password

Enter a **Username**.

For the username Password tap the radio button for “Prompt for password” or “Use the following password.”

Tap the **OK** button then Finish.

On the main configuration screen check the **Connect to** checkbox and choose the profile you just configured.

When prompted for the password enter it into the password field.



Figure 5-57 Enter the Profile Password

Use the Unmask checkbox to see the password in clear text as you type.



Figure 5-58 Authentication is Successful

When authentication is successful the Status on the main screen displays “open and authenticated.”

Server Authentication

To validate the server certificate the root CA certificate must be installed. For instructions for installing see section titled “Root Certificates”.

The RADIUS server certificate is not required, only the root CA which issued the server certificate.

Next configure the Root CA Certificate as a Trusted Root CA as described in the section titled “Trusted Server Configuration”.

Navigate back to the authentication type screen and check the “Validate server certificate” checkbox.

Tap **Next** to the end then Finish buttons. Tap **OK** to end the configuration process.

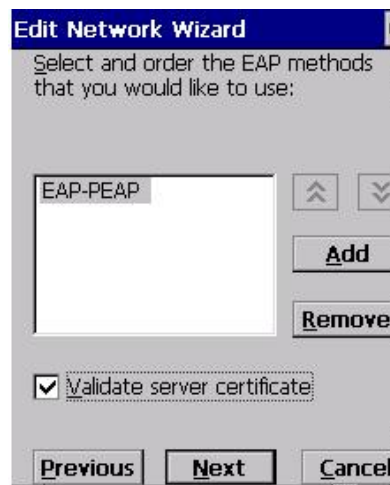


Figure 5-59 Validate Server Certificate for PEAP/GTC

Navigate back to the authentication type screen and **enable** the Validate server certificate checkbox.

Tap **Next** to the end then the Finish buttons.

Tap **OK** to end configuration.

EAP-LEAP Authentication

The Funk Odyssey supplicant authenticates a user with the EAP-LEAP protocol.

Use the delete and add buttons to choose EAP-LEAP authentication. Your system may have EAP-LEAP and/or LEAP in the method drop down list. EAP-LEAP protocol can be used for LEAP authentication.

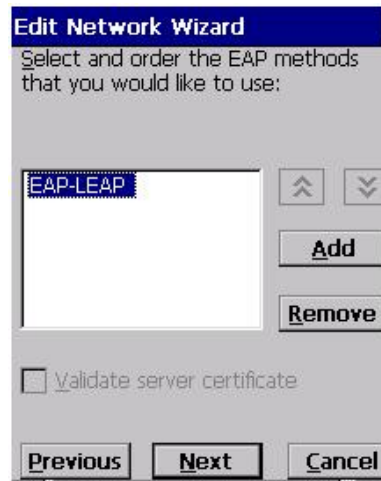


Figure 5-60 EAP-LEAP Method

EAP-LEAP does not use server side authentication so the Validate server box is grayed out.

Tap **Next**.

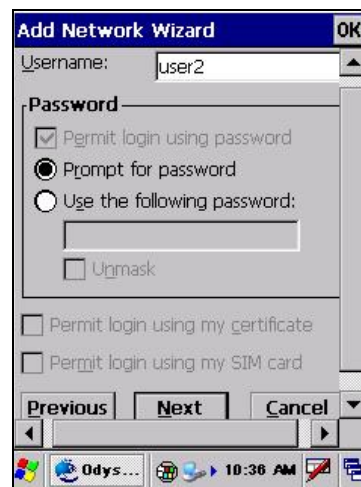


Figure 5-61 Create Username and Password Method

Enter a Username.

For the username Password tap the radio button for either **Prompt for password** or **Use the following password**.

Tap the OK button then Finish.

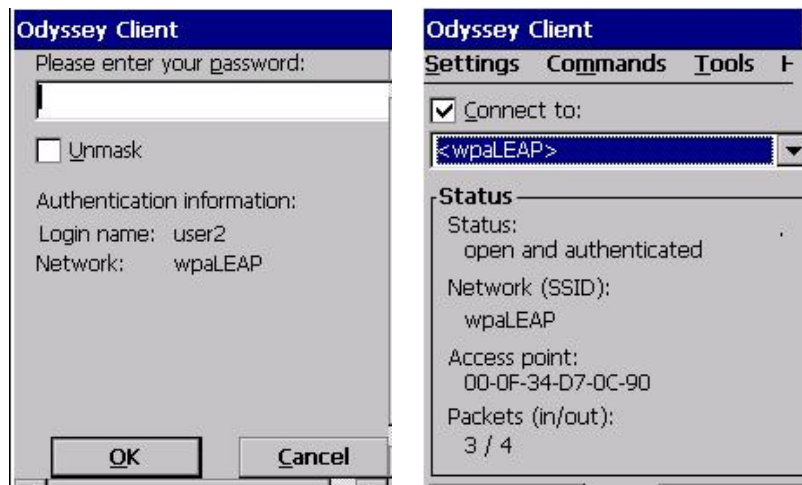


Figure 5-62 Enter Password for EAP-LEAP

When prompted for the password enter the valid password to authenticate.

Once authenticated the Status shows as “open and authenticated”.

EAP/TLS Authentication Configuration

To authenticate using the EAP/TLS protocol you will need a user certificate file and a private key file.

Once you have the user certificate files run the certificate installer from the Microsoft control panel as described in the section titled “Root Certificates”.

Note: It is important that all dates are correct on the CE devices when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Installing User Certificate

Navigate to **Start | Settings | Control Panel | Certificates**.

Choose **My Certificates** in the drop down list.

Tap the **Import** button.

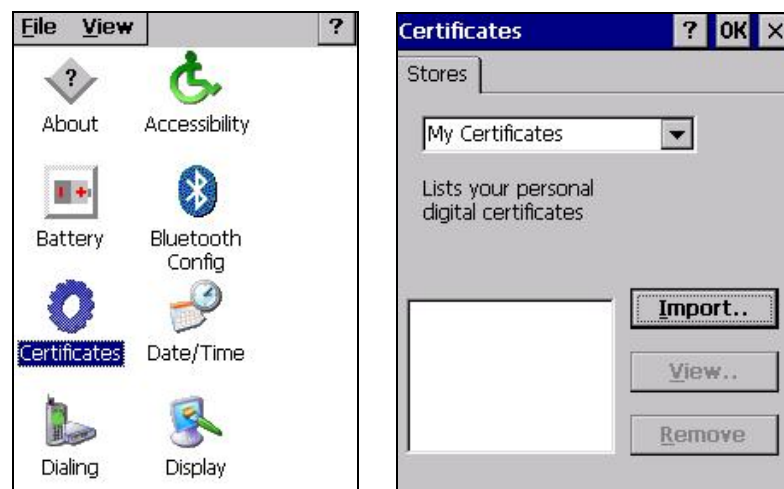


Figure 5-63 Install User Certificate

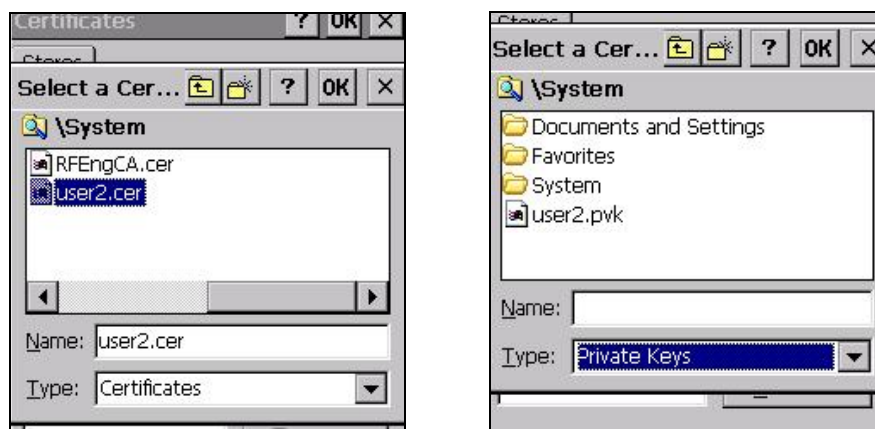


Figure 5-64 Install Private Key for Certificate

Tap **OK** to import from file.

Navigate to the location where the certificate file was copied.

Choose the certificate then navigate to the same place and choose to install the private key for the certificate.

Enter the password for the private key.

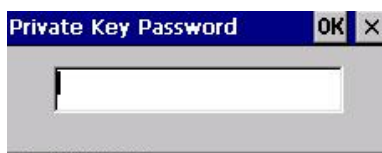


Figure 5-65 Enter Password for Private Key

To verify the user certificate navigate to **Start | Settings | Control Panel | Certificates – My Certificates**.

Tap the certificate and choose **View**.

Tap **Private Key** and look in the details pane to make sure the key is “Present.”

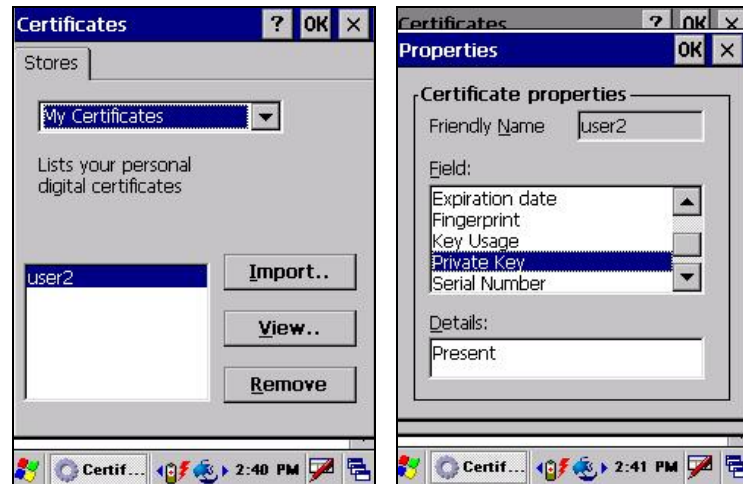


Figure 5-66 Verify User Certificate

Setting EAP/TLS Parameters

The Funk Odyssey supplicant authenticates a user with the EAP/TLS protocol.



Figure 5-67 Authenticate a User

Use the delete and add buttons to choose EAP/TLS authentication.

Uncheck the “Validate server certificate” for now.

Tap **Next**.

Enter the username on the user certificate to be used for authentication.

Tap **Next**.

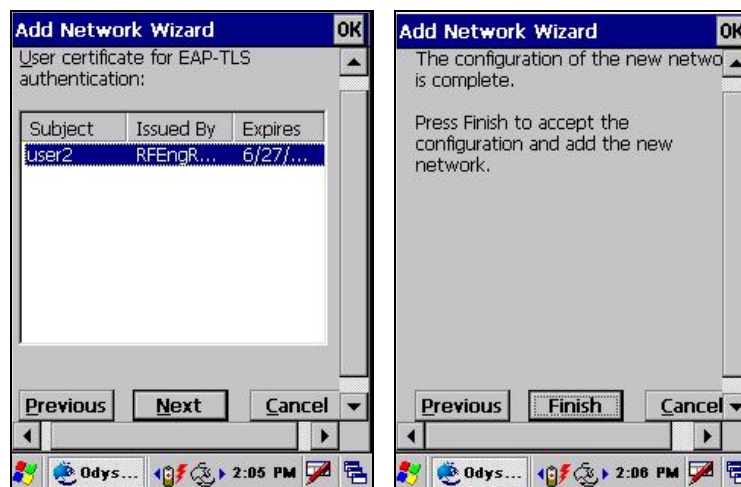


Figure 5-68 Completed Network Configuration

Choose the user certificate for authentication. Tap **Finish** to complete the configuration.

Explore the profile just created.

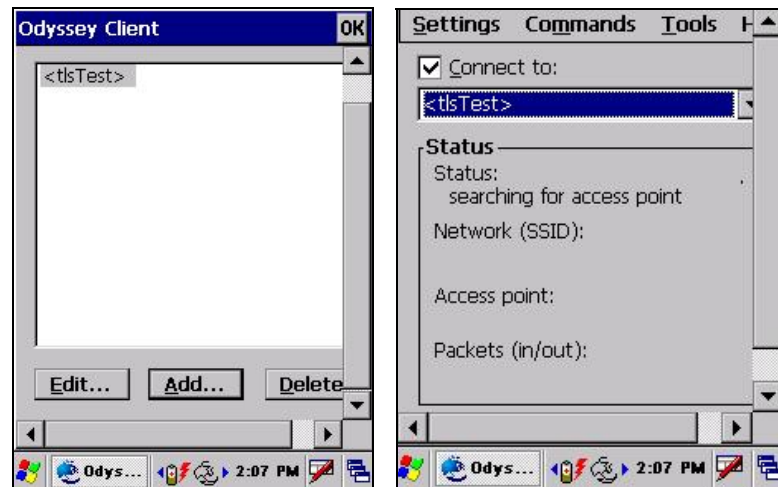


Figure 5-69 Choose the New Profile

Tap the **OK** button in the top right corner.

On the main configuration screen check the **Connect to** box and choose the profile just configured.

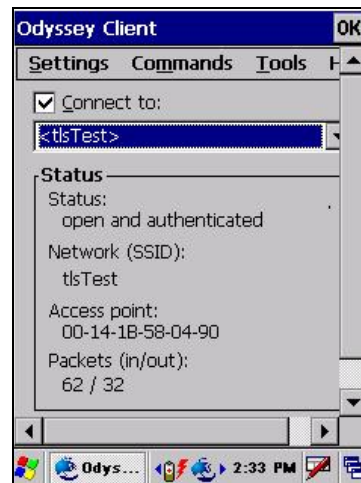


Figure 5-70 Status is open and authenticated

Once configured the status shows “authenticating” then once authenticated it shows “open and authenticated.”

To check the EAP-TLS status tap **Settings | Detailed Status**.

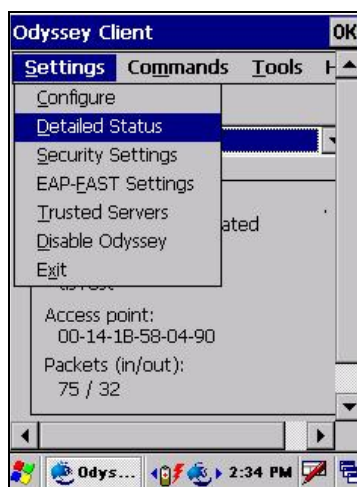


Figure 5-71 Settings – Detailed Status Menu Option

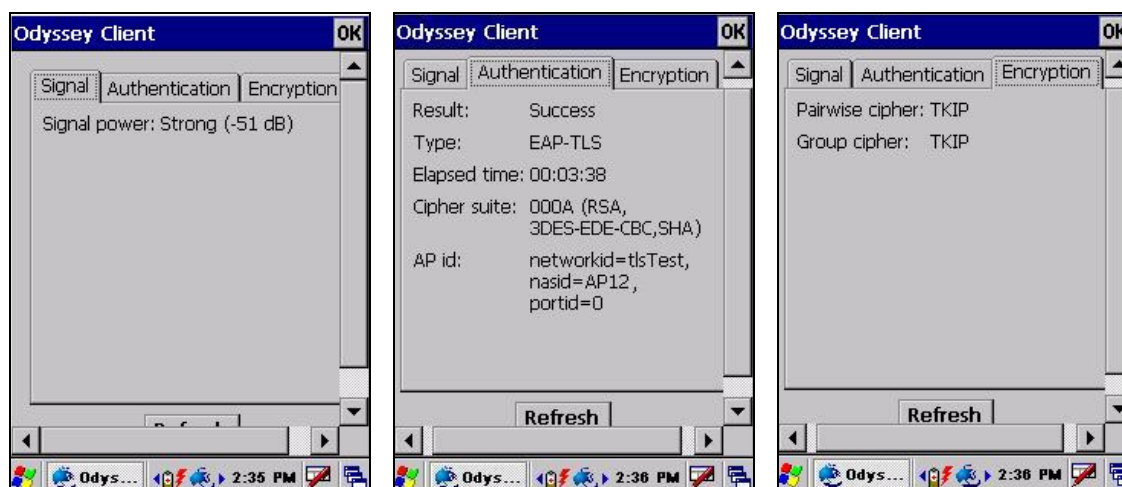


Figure 5-72 Detailed Status is Displayed – Signal, Authentication, Encryption

Validating the Server Certificate

To validate the server certificate the root CA certificate must be installed. For instructions for installing see section titled “Root Certificates”.

The RADIUS server certificate is not required, only the root CA which issued the server certificate.

Next configure the Root CA Certificate as a Trusted Root CA as described in the section titled “Trusted Server Configuration”.

Navigate back to the authentication type screen and check the “Validate server certificate” checkbox.

Tap **Next** to the end then Finish buttons. Tap **OK** to end the configuration process.



Figure 5-73 Enable the “Validate server certificate” Checkbox

WPA/PSK Configuration

To start the WPA/PSK configuration tap **Settings | Configure**.

Tap the **Add** button to configure a profile.

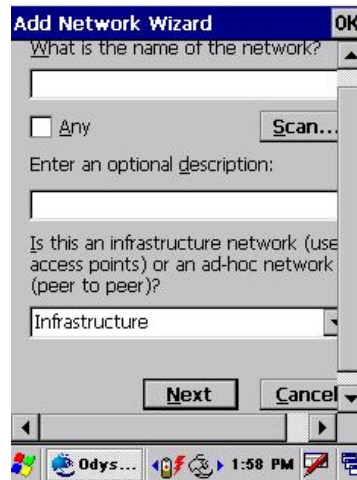


Figure 5-74 Enter Name of Network

On the Add Network Wizard screen type the SSID of the wireless network. If the SSID is being broadcast by the AP, press **Scan** and choose the correct SSID.

Choose **Infrastructure** for the network type.

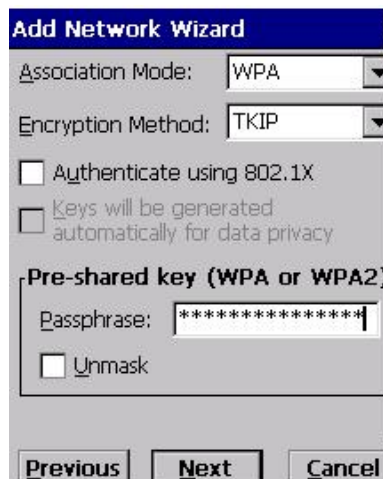


Figure 5-75 Set the Association Mode to WPA

Set the **Association** mode to “WPA” and **Encryption Method** to “TKIP”.

For WPA/PSK uncheck the “Authenticate using 802.1X” checkbox.

“Keys will ...” box is grayed out when the encryption method is set to TKIP. Enter the Pre-shared key as entered in the AP. Tap **Next** and Finish to complete the configuration.

Now you are ready to connect the MX7 to the AP.

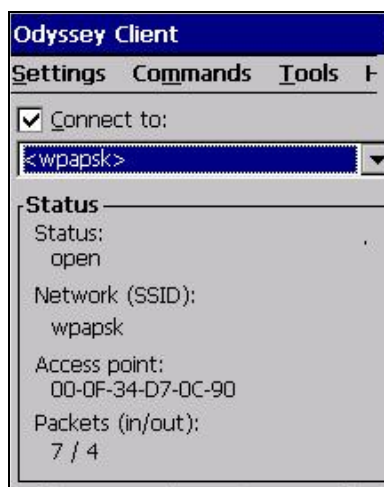


Figure 5-76 Connect the MX7 and the AP

Tap the "Connect to:" box and the MX7 then connects to the AP.

Trusted Server Configuration

To validate the server side certificates a Trusted Server must be configured. Install the Root CA certificate as described in the section titled “Root Certificates.” Then use the following directions to configure the Odyssey client to use the Root CA Certificate.

Navigate to **Settings | Trusted Servers**.

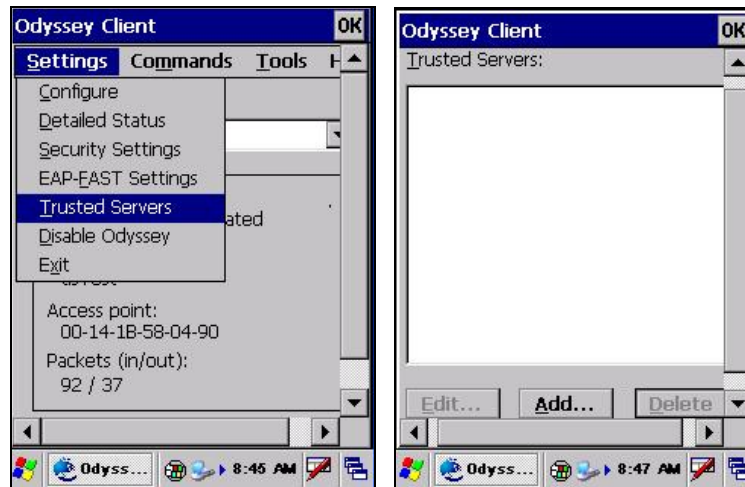


Figure 5-77 Settings – Trusted Servers Menu Option

Tap the **Add** button.

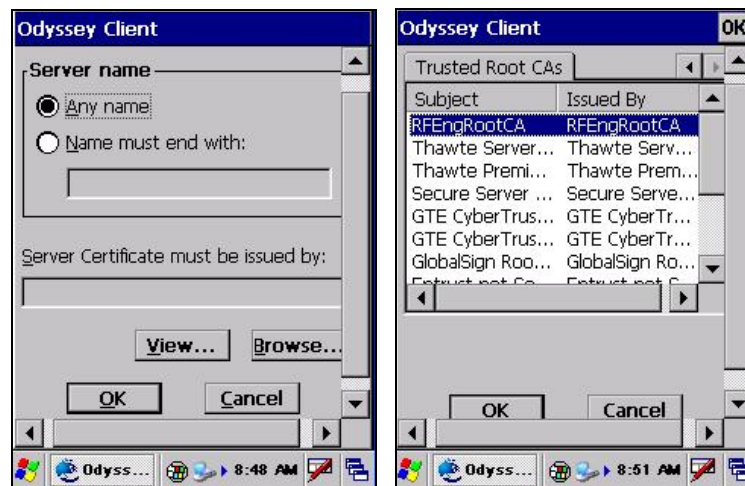


Figure 5-78 Select a Trusted Root CA

Tap **Browse**.

Tap the Trusted Root CAs tab.

Choose the correct Root CA certificate. Tap OK.

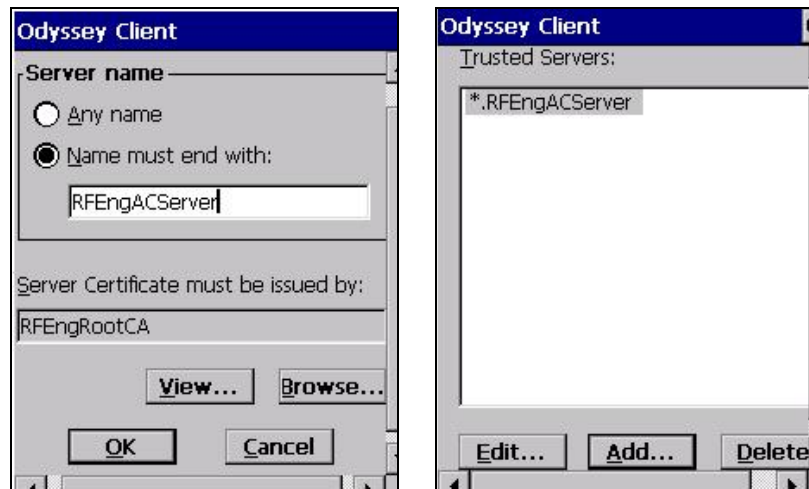


Figure 5-79 Configuring a Trusted Server Certificate

The Server Certificate is listed in the grayed box.


To authenticate the RADIUS server only, change the **Server name** button to “Name must end with:”.

Enter the **name of the RADIUS certificate** as shown in the screen titled “Trusted Servers.”


Tap the **OK** button. The server name should be listed in the box.

Tap the **OK** button. The trusted server certificate is configured for the MX7.

Root Certificates

 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>
--	---

Downloading a Root CA Certificate to a PC

	<p>Please refer to the “LXE Security Primer” for more information on obtaining and installing root certificates.</p>
---	--

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 5-80 Logon to Certificate Authority

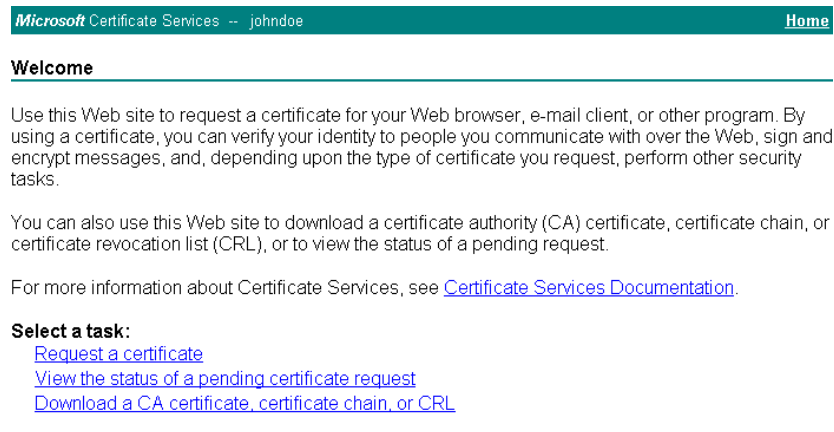


Figure 5-81 Certificate Services Welcome Screen

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.

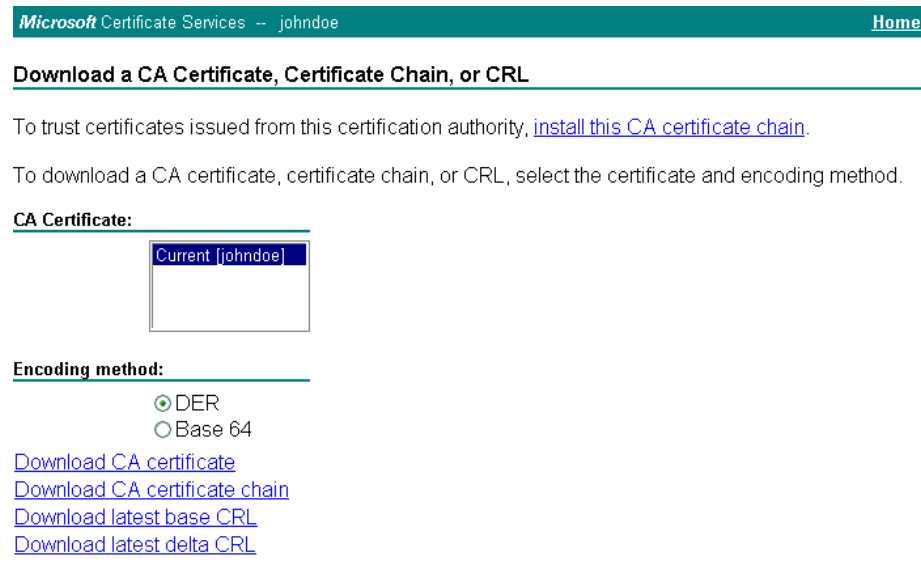


Figure 5-82 Select Encoding Method before Downloading

Tap the **DER** button.

To download the CA certificate, tap on the **Download CA certificate** link.

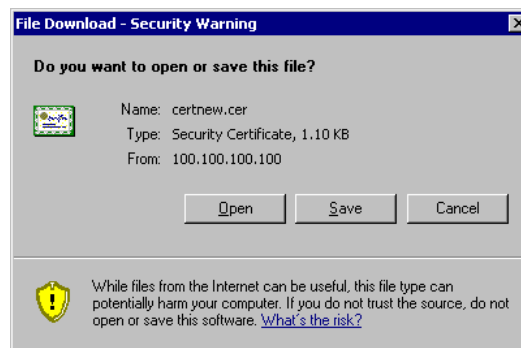


Figure 5-83 Download CA Certificate Screen

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 | Settings | Control Panel | Certificates**.

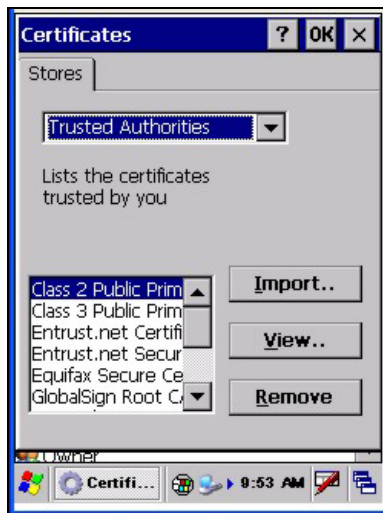


Figure 5-84 Certificate Stores

Tap the **“Import”** button.

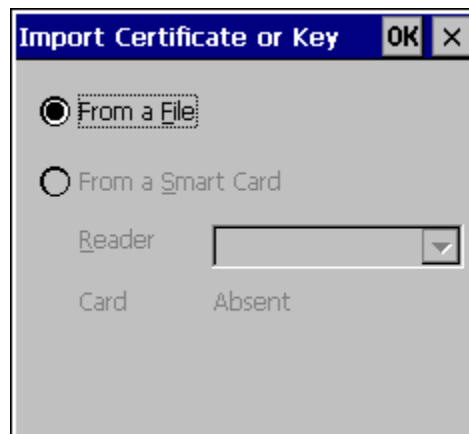


Figure 5-85 Import the Certificate

Make sure **“From a File”** is selected and tap OK.



Figure 5-86 Browse to the Certificate Location on the MX7


Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

When the text box appears asking if you want to ADD the following certificate to the Root Store, tap **Yes** to import the certificate.


Once the certificate is installed, return to the proper authentication section, described later in this chapter.

Note: There is no error message when the certificate is not found or the certificate name is entered incorrectly.

User Certificates

 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>
--	---

Generating a User Certificate for the Mobile Device

	<p>Please refer to the “LXE Security Primer” for more information on obtaining and installing user certificates.</p>
---	--

The easiest way to get the user certificate is to use a browser on a PC to navigate to the CA. To request the user certificate, open a browser to

`http://<CA IP address>/certsrv`

Sign into the CA with the username and password of the person who will be logging into the mobile device.

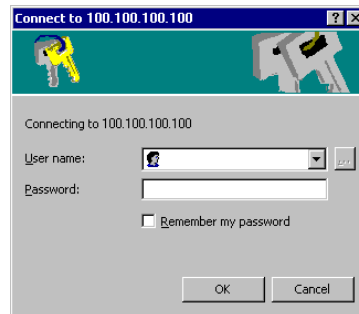


Figure 5-87 Logon to Certificate Authority

Important: This process saves a user certificate and a separate private key file. CE devices such as the MX7 require the private key to be saved as a separate file rather than including the private key in the user certificate.

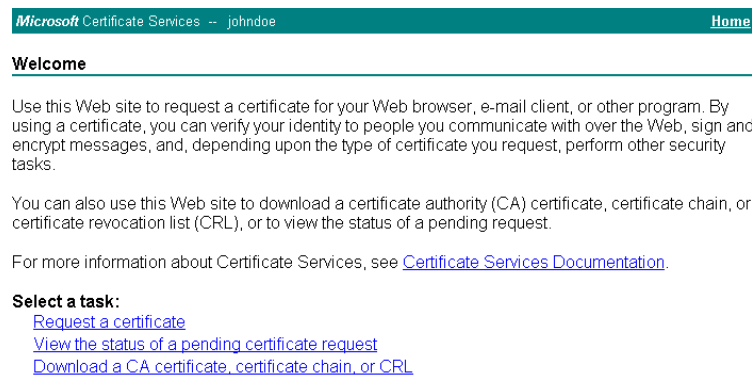


Figure 5-88 Certificate Services Welcome Screen

Tap the “**Request a certificate**” task link.

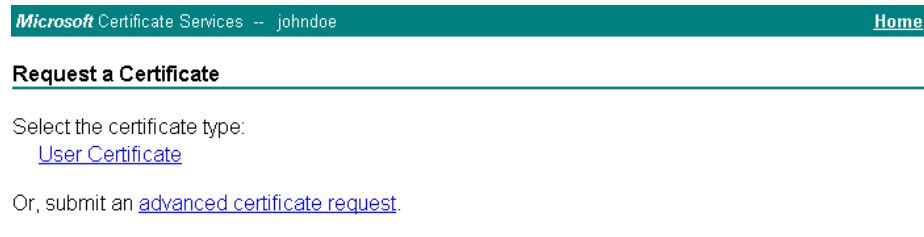


Figure 5-89 Request a Certificate Screen

Tap on the “**advanced certificate request**” link.

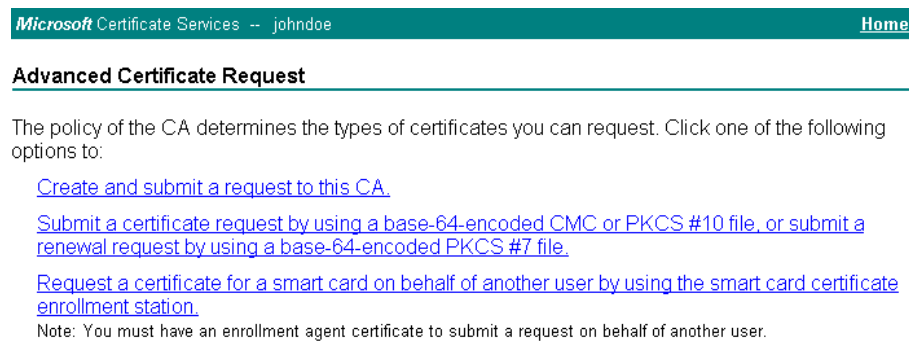


Figure 5-90 Advanced Certificate Request Screen

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:

Submit >

Figure 5-91 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 MX7USER.PVK. The certificate file created later in this process must be given the same name, for example, MX7USER.CER.

DO NOT check “Enable strong private key protection”.

Make any other desired changes and tap the “Submit” button.

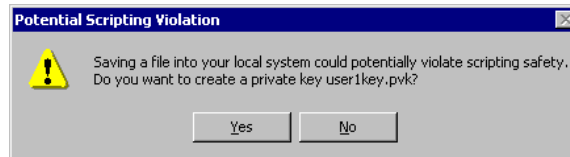
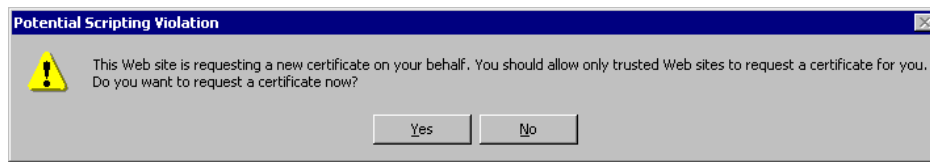


Figure 5-92 Script Warnings

If any script notifications occur, tap the “Yes” button to continue the certificate request.

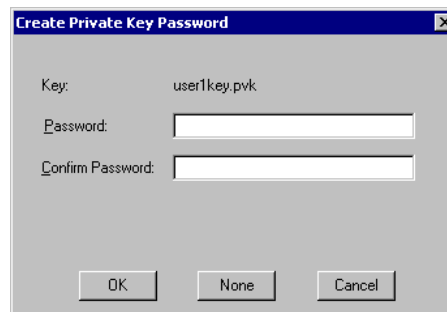


Figure 5-93 Script Warnings

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”.

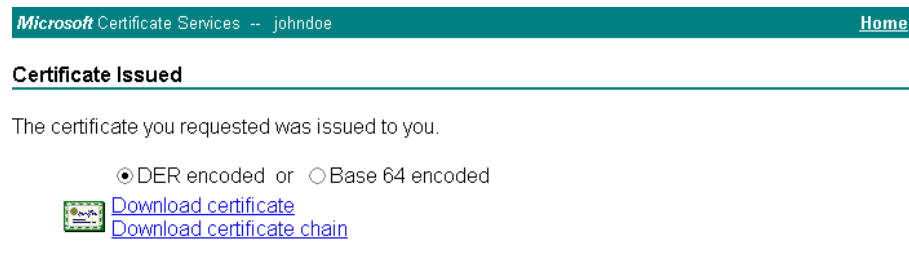


Figure 5-94 Certificate Issued

Tap the **Download certificate** link.

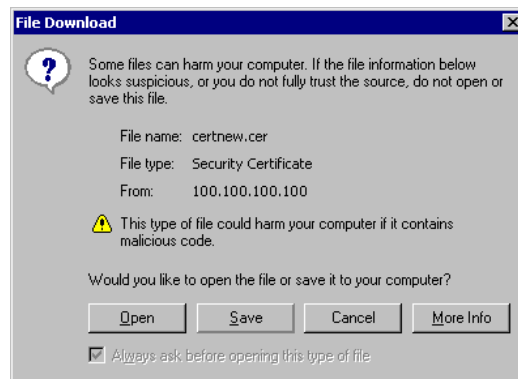



Figure 5-95 Certificate Download Security Warning

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.

	<p>Be sure 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 MX7USER.PVK then the certificate file created must be given the same name, for example, MX7USER.CER.</p> <p>Note: There is no error message when the certificate is not found or the certificate name is entered incorrectly.</p>
---	--

Installing a User Certificate on the Mobile Device (WPA-TLS Only)

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to **Start | Settings | Control Panel | Certificates**.



Select "My Certificates" from the pull down list.

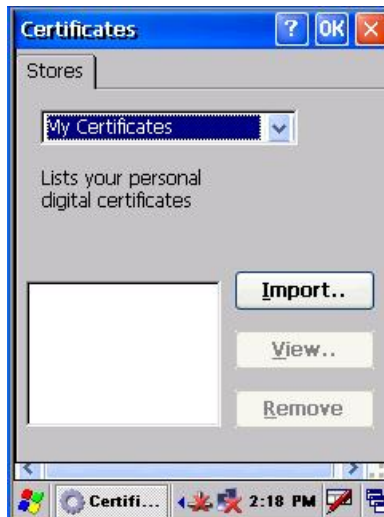


Figure 5-96 Certificates

Tap the "Import" button.

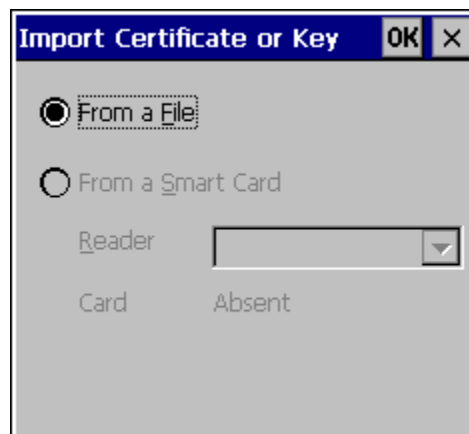


Figure 5-97 Import Certificate

Make sure "From a File" is selected and tap OK.

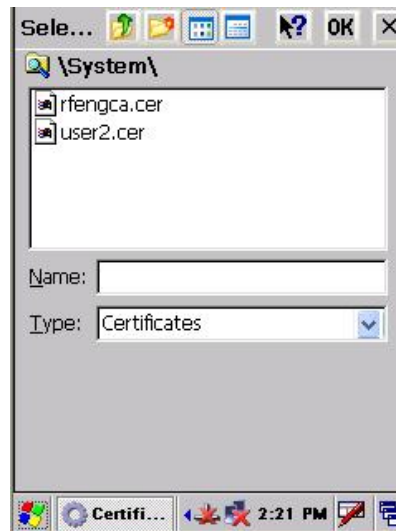


Figure 5-98 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

The certificate is now shown in the list.

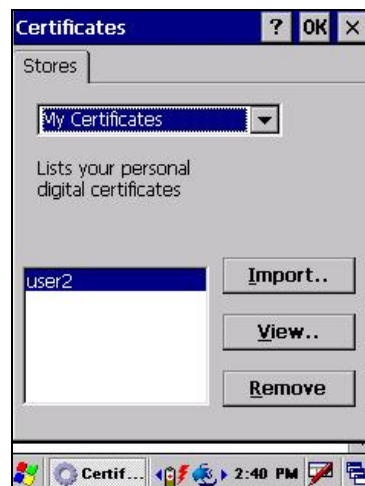


Figure 5-99 Certificate Listing

Highlight the certificate you just imported and tap the **View..** button.

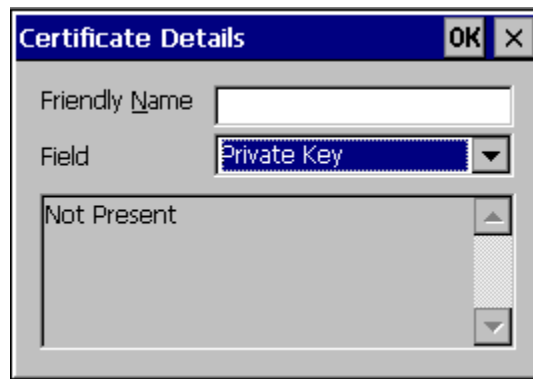


Figure 5-100 Private Key Not Present

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 5-101 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.

Enter the password for the certificate if appropriate.

Tap **View** to see the certificate details again.



Figure 5-102 Private Key Present

The private key should now say “Present”. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example *mx7user.cer* for the certificate and *mx7user.pvk* for the private key file. If the file names are not the same, rename the private key file and import it again.

IEEE 802.11g Wireless LAN Configuration Utility

Access: **WiFi toolbar icon** or **Start | Programs | Radio Config Utility**



WiFi icon in Toolbar

The Radio Config Utility can be used to set the wireless device power management, antenna diversity and roaming profiles. Currently, LXE recommends using the default values.

The WiFi utility is installed upon each cold reset and warm reset and the icon is minimized to the toolbar.

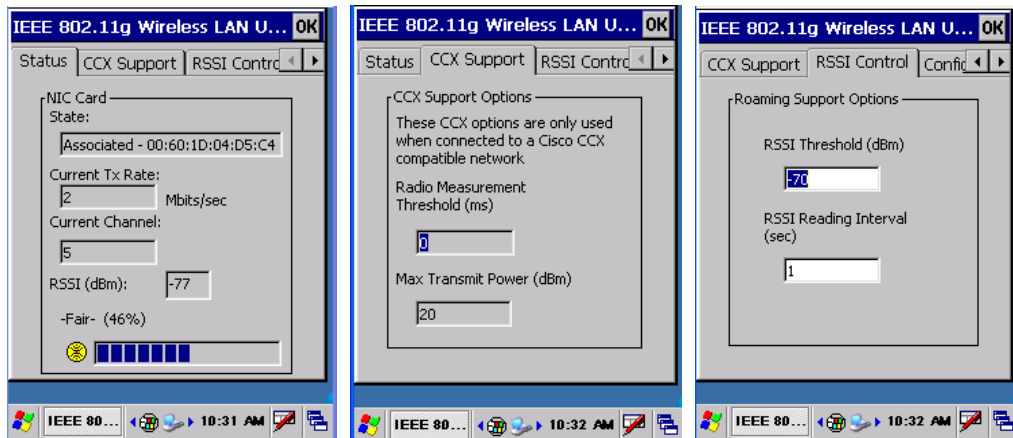


Figure 5-103 802.11g WiFi Configuration Utility Menus - Status, CCX, RSSI

The **Status** screen displays the current status of the network card, current data rate, the current AP channel that the client is operating on, RSSI threshold and signal strength. These values cannot be changed by the user.

The **CCX Support** options are only populated when the MX7 is connected to a Cisco CCX compatible network or AP. Radio Measurement Threshold and Max Transmit Power values cannot be changed by the user.

The **RSSI Control** panel allows the user to set roaming support options. RSSI Threshold default is -70. RSSI Reading Interval is 1 sec. When the threshold reaches -70, the mobile device begins searching for a stronger AP signal every second until it locates an AP with a stronger signal.

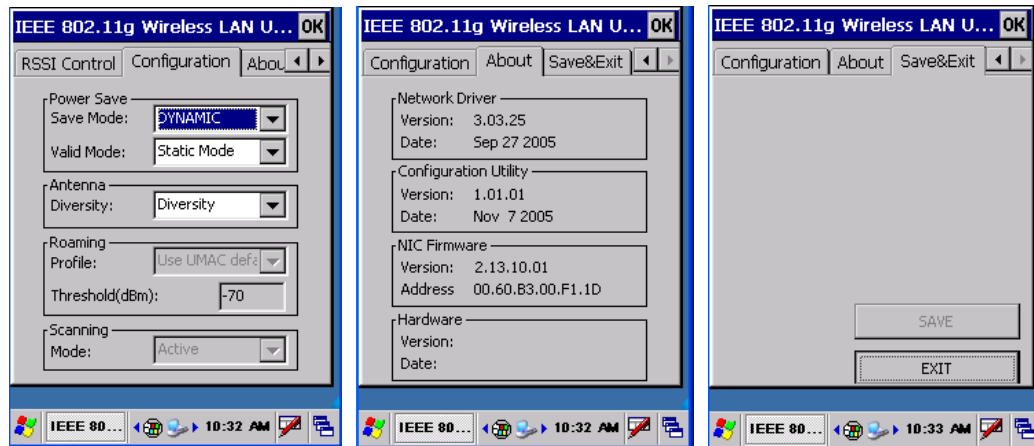


Figure 5-104 802.11g WiFi Configuration Utility Menus - Conf, About, Save&Exit

Configuration default options :

Power Save	Save Mode/Dynamic; Valid Mode/Static Mode. Dynamic save mode sets the network card to allow it to enter Power Save mode. LXE does not recommend using Maximum save mode.
Antenna	Diversity
Roaming	Profile displayed and greyed out; Threshold populated by RSSI Control panel setting
Scanning	Mode displayed and greyed out

The **About** screen displays version information. The values cannot be edited by the user.

Save&Exit buttons: The Save button is greyed out if there have been no changes made to the 802.11g parameters since the last reboot. If WiFi changes have been made, tap the Save button and then tap OK to save the changes. The WiFi icon minimizes to the taskbar. Tap the Exit button to close the WiFi utility and the WiFi icon is removed from the taskbar. LXE recommends the WiFi icon be visible in the taskbar at all times.

If the WiFi utility is closed accidentally you can *either* perform a Warm Reset to restart the WiFi utility *or* tap Start | Programs | Radio Config Utility.

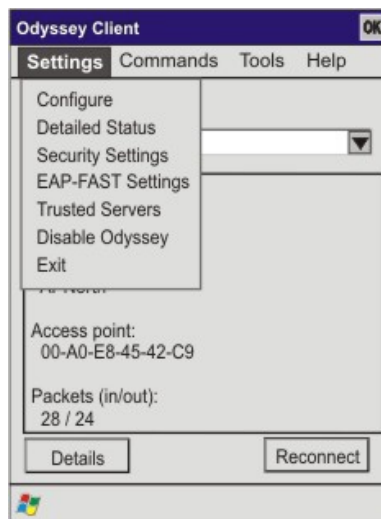
Wireless Zero Config Utility

Odyssey Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the application is available but not used for current client connection. To use the Wireless Zero Config Utility with the Odyssey Client, the Odyssey Client must be deliberately disabled by the user.

Note: LXE recommends using the Funk Odyssey client to configure the Odyssey Client. Wireless Zero Config icon is not recommended for configuring the client as it cannot be used to configure all supported security protocols.

To use Wireless Zero Config, first open the Odyssey Client Utility. Start the Odyssey client configuration by tapping the Odyssey Client icon on the desktop or in the taskbar at the bottom right corner of the screen.



Tap the **Disable Odyssey** option on the Settings menu.

Odyssey is disabled immediately and the Wireless Zero Config utility begins.

Summit Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled and the MX7 is not connected to a network. *LXE does not recommend use of the Wireless Zero Configuration Utility for configuring the client as it cannot be used to configure all supported security protocols.*

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 the client device.

To use Wireless Zero Config, first open the Summit Client Utility.



1. Select **ThirdPartyConfig** in the Active Config drop down box.
2. A message appears that a Power Cycle is required to make settings activate properly. Tap **OK**.
3. Tap the **Disable Radio** button to remove the connection to the Summit Client Utility. The text on the button changes to Enable Radio.
4. Tap the **Power** button to place the MX7 in **Suspend**, then tap the Power button to **wake the MX7** from Suspend mode.

The Wireless Zero Config utility begins.

Chapter 6 AppLock

Introduction

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 applications are automatically launched and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.



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

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.

*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.

Determine Your AppLock Version

If the Administrator Control Menu looks like this . . .	Go to
	Appendix C – Reference Material <i>AppLock – Single Application Version.</i>
	This chapter.


Setup a New Device

Prerequisites:

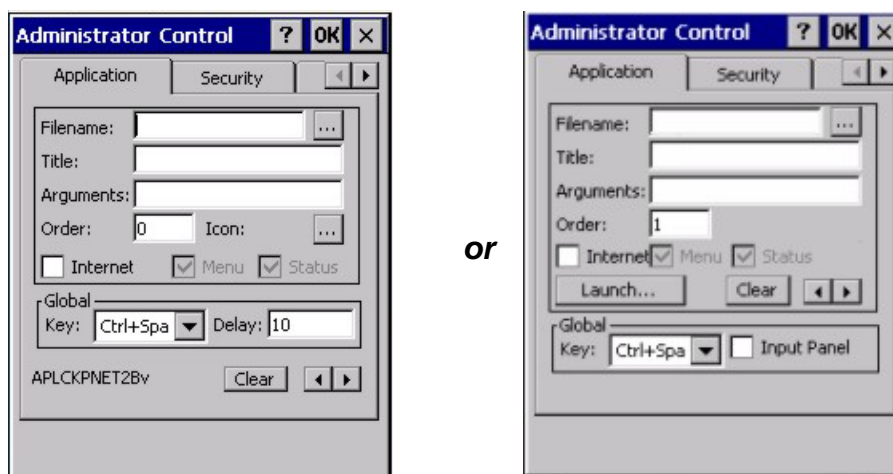
- The touch panel must be enabled.
- An MX7 default input method (Input Panel, Transcriber, or custom input method) is assigned.

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.

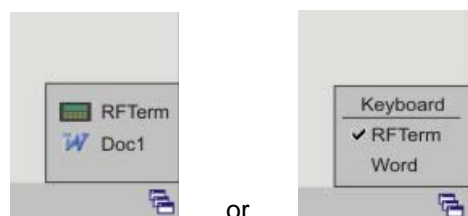
Briefly, the process to configure a new device is as follows:

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  | 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 **hotkey sequence** to launch AppLock and lock the configured application(s).
11. The device is now in **end-user mode**.

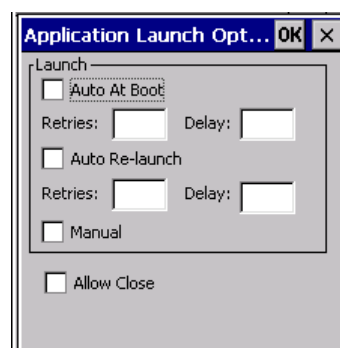
Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.



Application Panel



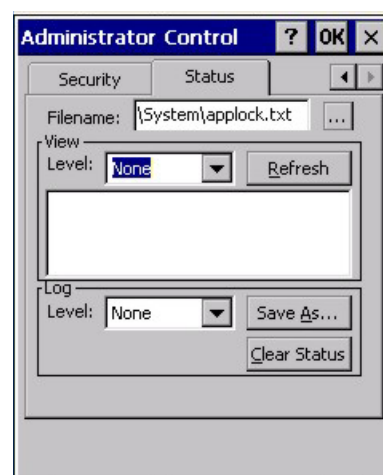
End User Switchpad



Application – Launch Panel



Security Panel



Status Panel

Figure 6-1 AppLock Screens

Administration Mode

Administration mode gives full access to the mobile device, hardware and software 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	55-key : Shift+Ctrl+A 32-key : Requires Alpha Mode
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. Each 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.

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

or

Ctrl+5 Ctrl+9 Ctrl+3

End-User Switching Technique

Note: The touch screen must be enabled.

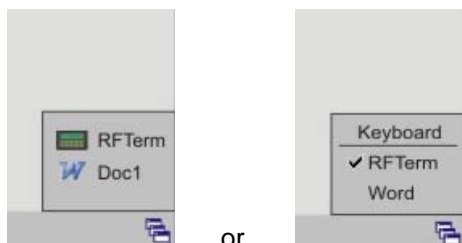


Figure 6-2 Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX7 default input method (Input Panel, Transcriber, or custom input method) is activated.

Using a Stylus Tap

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

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

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

See Also: *Application Panel / Launch / Manual (Launch) and Allow Close*

Using the Switch Key Sequence

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

See Also: *Application Panel / Global Key*

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

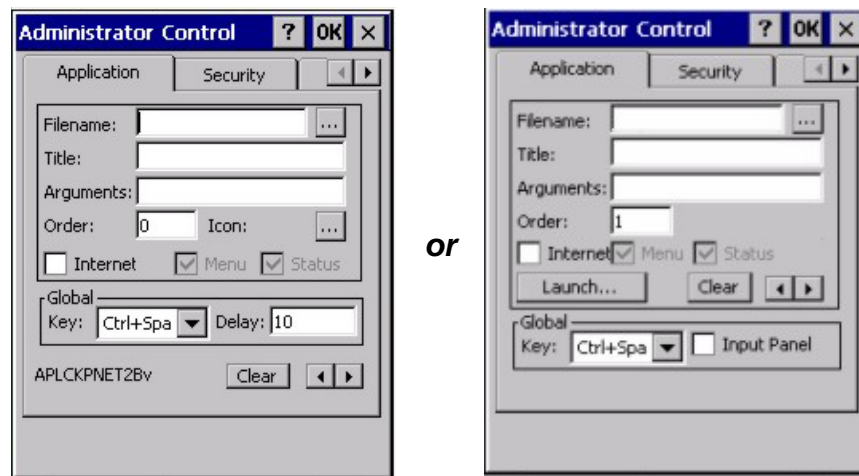


Figure 6-3 Application Panel – Multi-Application

Note: If your Application Panel does not look like the figures shown above, you may have the Single Application version.

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.

Option	Explanation
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 <i>End-user Internet Explorer (EUIE)</i> for more details.
Launch Button	See following section titled <i>Launch Button</i> . <i>Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.</i>
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the <i>Activation</i> key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. <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>
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

Note: The Launch button may not be available in all versions of Multi-AppLock. Contact your LXE representative for assistance, downloads and AppLock update availability.

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.

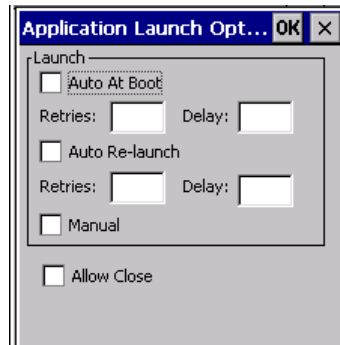


Figure 6-4 Application Launch Options

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 – Multi-Application

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 2nd 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 modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Setting a Password in 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 log file 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.

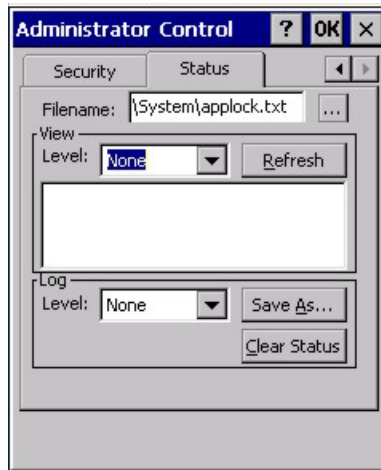


Figure 6-6 Status Panel – Multi-Application

Move the cursor to the **Filename** text box and either type the log file path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the log file from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version. Refer to Appendix C – Reference Material, AppLock - Single Application Version for instruction.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

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
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'... button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: *Appendix C – Reference Material*, sections titled *AppLock Error Messages* and *AppLock Registry Settings*.

Troubleshooting AppLock

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word and LXE RFTerm, 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.

See Also: *Appendix C – Reference Material*, sections titled *AppLock Error Messages* and *AppLock Registry Settings*.



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.

55-Key Alphanumeric Keymaps

ANSI / CE Keypad

When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.

When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.

Alphabetic keys default to lower case letters. Press the Shft key, then the alphabetic key for an uppercase letter.

When the computer boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with Blue plus Tab key sequence.

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
Power / Suspend							Power ⁵
Field Exit (default VK_PAUSE) MAP=Mappable	MAP	MAP			MAP		Diamond#1
Volume Adjust Mode	x	x					Scan Key ⁶ or V

⁵ 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).

⁶ Orange+Scan (and Blue+V) 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.

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
Display Backlight Brightness Adjust Mode	x						Scan Key ⁷
Toggle Blue Mode							Blue
Toggle Orange Mode							Orange
Toggle Shift Mode							Shft
Alt							Alt
Control							Ctl
Scan							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						I (letter i) or Ctl
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

⁷ 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 MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
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
F22		x			x		F2
F23		x			x		F3
F24		x			x		F4
a							A
b							B
c							C
d							D
e							E
f							F
g							G
h							H
i							I
j							J
k							K
l							L
m							M
n							N
o							O
p							P
q							Q
r							R
s							S
t							T
u							U
v							V
w							W
x							X
y							Y

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
z							Z
A					x		A
B					x		B
C					x		C
D					x		D
E					x		E
F					x		F
G					x		G
H					x		H
I					x		I
J					x		J
K					x		K
L					x		L
M					x		M
N					x		N
O					x		O
P					x		P
Q					x		Q
R					x		R
S					x		S
T					x		T
U					x		U
V					x		V
W					x		W
X					x		X
Y					x		Y
Z					x		Z
1							1
2							2
3							3
4							4
5							5
6							6
7							7
8							8
9							9
0							0

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
. period or . (period)		x					DEL or K
<	x						G
[x						Y
]	x						Z
>	x						H
=	x						T
{	x						W
}	x						X
/	x						J
-	x						Spc
+	x						Del
* (asterisk)		x			x		I (letter i) or 8
: (colon)		x					D
; (semicolon)		x					F
. (period)		x					K
?		x					L
` (accent)		x					N
_ (underscore)		x					M
, (comma)		x					J
' (apostrophe)		x					H
~ (tilde)		x					B
\		x					S
		x					A
“		x					G
!		x			x		Q or 1
@		x			x		W or 2
#		x			x		E or 3
\$		x			x		R or 4

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Caps Lock	
%		x			x		T or 5
^		x			x		Y or 6
&		x			x		U or 7
(x			x		O or 9
)		x			x		P or 0 (zero)

5250 Key Map for the 55-Key Keypad

Legend.....	Explanation.....	Key Sequence
Attn	Attention	Ctl + A
Clr	Clear	Ctl + C
Del	Delete	Ctl + D
Dup	Duplicate	Ctl + U
E-Inp	Erase Input	Ctl + Q
Field Exit	Enter	Diamond 1
Fld –	Field Minus	Ctl + M
Fld +	Field Plus	Ctl + L
Ins	Insert	Ctl + I
NL	New Line	Ctl + N
SysReq	System	Ctl + S

Please refer to the “RFTerm Reference Guide” for further information about 5250 key functions on the mobile device.

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 MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
Power / Suspend							Power ⁸
Field Exit (default VK_PAUSE)	MAP				MAP		Diamond#1 <i>MAP=Mappable</i>
= or (x	x			MAP		Diamond#2 Default is MAP <i>MAP=Mappable</i>
! or)	x	x			MAP		Diamond#3 Default is MAP <i>MAP=Mappable</i>
Volume Adjust Mode		x					Scan Key ⁹
Display Backlight Brightness Adjust Mode	x						Scan Key ¹⁰
Toggle Blue Mode							Blue
Toggle Orange Mode							Orange
Toggle Shift Mode							Shft
<u>Toggle Alpha Mode</u>							<u>Alph</u>
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

⁸ 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).

⁹ 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.

¹⁰ 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 MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
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
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

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
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
N					x	x	66
O					x	x	666
P					x	x	7
Q					x	x	77
R					x	x	777
S					x	x	7777

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
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
. (period)		x					Del
?		x					8
` (accent)	x						6

To Get This MX7 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctl	Alt	Shft	Alpha	
_ (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 MX7 SDK CD [MX7A504CE50SDK]

Introduction

A command-line compiler called KEYCOMP.EXE is provided on the MX7 SDK CD. Using this compiler, the System Administrator can convert a sample default key map text file into a custom key map text file which, when loaded onto the mobile device, can be chosen by the user to replace the default mobile device keymap and then switched back when they are finished using the customized keys. This custom key map file can be made to re-define the system return code for each of the 55-key keypad keys, key press or key press combinations. All keys, except the power key, can be re-mapped.

IMPORTANT – The keycomp utility included with the MX7 SDK is not the same as the one included with the MX3X SDK. This one only generates maps for the MX7.

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:

KEYCOMP DEFAULT.KEY (writes KEYCOMP.REG to local directory)



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=4
.
```

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 MX7 [MX7 is scancode = ((column << 3) + row)]

Note: The field MAPDESC needs to be unique, but MAPNAME does not.

SPECIAL Section

```
.
[ Special ]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
.
```

The second section is the **SPECIAL** section, which contains the row and column definitions for certain modifier keys which must be processed independent of the overall keymap. Currently, these are only modifier keys.

The only recognized names are: **KEYSHIFT**, **KEYALT**, **KEY2ND**, and **KEYCONTROL**, and these specify the row and column of these 4 specific modifier keys, in COLxROWx format. Note the row and column for these keys can be outside the keymap limits specified in the **GENERAL** section, since these are not loaded as part of the keymap proper.

MAP Section

```
.
[ Map ]
MAP=MAP_NORMAL
;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
.
```

There will be several (4 to 7) **MAP** sections, each defining the keymap for a given combination of modifier keys. The keyboard driver requires keymaps for normal (no modifiers), SHIFT only, 2ND only, and 2ND-SHIFT combined.

The CTRL modifier and ALT modifier do not have individual keymaps; the keystrokes are passed to the operating system, which is allowed to parse these keys according to Microsoft specifications (for example, ALT-keys are defined to only pulldown menus, with no other function).

The only recognized value names are **MAP** and **COLxROWx** (defining a key code). The only valid values for **MAP** are:

MAP_NORMAL	no modifier keys
MAP_2ND	2nd modifier only
MAP_SHIFT	shift modifier only
MAP_2NDSHIFT	2nd and shift modifiers together
MAP_NORMAL32	(MX7 only) no modifiers, 32-key map
MAP_ORANGE32	(MX7 only) orange modifier, 32-key map
MAP_BLUE32	(MX7 only) blue modifier, 32-key map
MAP_SHIFT32	(MX7 only) shift modifier, 32-key map

MAP_NORMAL55	(MX7 only) no modifiers, 55-key map
MAP_ORANGE55	(MX7 only) orange modifier, 55-key map
MAP_BLUE55	(MX7 only) blue modifier, 55-key map
MAP_SHIFT55	(MX7 only) shift modifier, 55-key map
MAP_ORANGESHFT	(MX7 only) orange and shift modifiers

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 (not on MX7)
MAP_CONTR (or) MAP_CONTRAST	special keymap for contrast adjustment (not on MX7)
MAP_BRITE (or) MAP_BRIGHT	special keymap for brightness adjustment (not on MX7)

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 Appendix C for valid codes)
'x'	a single ASCII character ('A','b','l','@',' ', etc.)
SHIFT+VK_code	for a shifted VK code (see Appendix C for valid codes)
SHIFT+'x'	for a shifted ASCII character (should not be needed)
ACTION+code	special function key (valid codes listed below)
CHANGE+mapname	for modifier keys, change keymaps to mapname, as specified above
OPEN	an unused key position, does nothing when pressed

Valid **ACTION** codes are as follows:

SCAN1	Scan key 1 (left side of screen on mobile device)
SCAN2	Scan key 2 (right side of screen on mobile device)
SCAN3	Handle trigger button (unused on mobile device, but specified)
POWER	power button
BACKLIGHT	backlight on/off function

Note that specifying the power button in a different location will affect suspend/resume functions. The "15-second hold to force reboot" function is controlled by hardware, and will only work with the default power button.

Keycomp Error Messages

Most error messages will specify the line within the keymap source file where the error occurred.

Duplicate key

A COLxROWx code was found in a MAP table, but that COL/ROW already has a value assigned.

GENERAL section must come before MAP

The GENERAL section must come first, or at least before any MAP sections. The GENERAL section defines parameters which are needed to process Maps

Header line missing close bracket

The section header line must have square brackets before and after the section name

Header line missing open bracket

The section header line must have square brackets before and after the section name

Invalid ACTION code %s

The key scan code is specified as ACTION+code, but the ACTION code parsed is not recognized. The following values are valid: SCAN1, SCAN2, SCAN3, POWER, or BACKLIGHT.

Invalid keycode %s

The keycode parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A' or '#').
- OPEN for unused entries (will not do anything when pressed)

Invalid MAP value %s

The MAP value parsed is not one the following list: MAP_NORMAL, MAP_2ND, MAP_SHIFT, MAP_2NDSHF, MAP_2NDSHIFT, MAP_VOLUM, MAP_VOLUME, MAP_CONTR, MAP_CONTRAST, MAP_BRITE, or MAP_BRIGHT.

Invalid MAPCNT (1-%d valid)

The specified MAPCNT exceeds the limits of the KEYCOMP compiler.

Invalid MAPCOLS (1-%d valid)

The specified MAPCOLS exceeds the limits of the KEYCOMP compiler.

Invalid MAPROWS (1-%d valid)

The specified MAPROWS exceeds the limits of the KEYCOMP compiler.

Invalid ROWCOL format

A COLxROWx was expected, but the format was not correct. The only valid formats are: COLxROWx, COLxxROWx, COLxROWxx, or COLxxROWxx, where xx are decimal numeric digits (0-9).

Invalid scan code

The scan code parsed is not recognized. The scan code can take one of the following formats:

- VK_code
- 'x'
- SHIFT+VK_code
- SHIFT+'x'
- ACTION+code
- CHANGE+mapname
- OPEN

Invalid section name %s

The section name parsed is invalid. The only recognized names are: GENERAL, SPECIAL, or MAP

Invalid SHIFT code %s

The key scan code is specified as SHIFT+code, but the SHIFT code parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A', '3', or '#').

Invalid value %s in GENERAL section

The value name parsed is invalid for the GENERAL section. The recognized names are: MAPNAME, MAPCNT, MAPCOLS, MAPROWS, or ALGOR

Invalid value %s in MAP section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: MAP and COLxxx.

Invalid value %s in SPECIAL section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: KEYSHIFT, KEYALT, KEY2ND, and KEYCONTROL.

Invalid VK_code %s

The VK code parsed is not recognized. See the VK Code Table (below) for valid values.

Map ended without MAP value

The MAP section must contain a MAP value, so the data fields can be parsed.

MAPNAME must be all numerics

Because of limitations in Microsoft Layout Manager, the map name must be all numeric (4, 5, or 6 digits). The name parsed did not fit this limitation.

No definition for map MAP_2ND

There is no 2nd keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_2NDSHIFT

There is no 2nd-SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_NORMAL

There is no Normal keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_SHIFT

There is no SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.key2nd

No 2ND modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyalt

No ALT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keycontrol

No CTRL modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keydnarrow

No down arrow definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keypower

No power key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan1

No Scan Key 1 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan2

No Scan Key 2 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan3

No Trigger Button definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyshift

No SHIFT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyuparrow

No up arrow definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No equal in value line

A value line must be of the form *value=data*. A value line was expected, but there was no equal in it. (*or*) A comment line did not begin with a semicolon (;).

No MAPNAME defined

There is no map name defined. The keyboard driver requires this name to be able to load the keymap tables. This message comes from the post-parse validation, so no line # is specified.

Scan code algorithm required

A COLxROWx data value was found before any ALGOR statement. ALGOR algorithm is parsed to decide how to encode COLxROWx into a keymap value.

Too many maps for specified MAPCNT

There are more MAP sections defined 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 MX7 default keyboard
;;
;;-----

;;-----
;; general parms give the size of arrays
;; all numeric values are decimal
;; these numbers are validated with the data below
;;           at compile time
;; MAPNAME must be 8-digits all numerics
;;-----
[General]
MAPDESC=Default
MAPNAME=00000409
MAPCNT=13
MAPCOLS=8
MAPROWS=8
ALGOR=MX3X

;;-----
;; ...still true for MX3X; not for MX7
;; ...but the old MX3X maps are included in the MX7
;;   map in case we ever merge...
;; special keys are accessed outside the map
;; this specifies the row and column
;; these should not need to change, but...
;;-----
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
KEY2ND=COL10ROW0
KEYCONTROL=COL11ROW0

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with no modifier
;;-----
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=VK_F7
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;
COL1ROW0='Q'
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3='T'
COL1ROW4='U'
COL1ROW5='4'
COL1ROW6='O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;
COL2ROW0='A'
COL2ROW1=open
COL2ROW2='D'
COL2ROW3='G'
COL2ROW4='J'
COL2ROW5='1'

```



```

COL2ROW6='L'
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=' '
COL3ROW1=open
COL3ROW2='X'
COL3ROW3='V'
COL3ROW4='N'
COL3ROW5='0'
COL3ROW6=VK_LEFT
COL3ROW7=VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=VK_F9
COL4ROW1='S'
COL4ROW2=VK_RIGHT
COL4ROW3='F'
COL4ROW4='H'
COL4ROW5='K'
COL4ROW6='2'
COL4ROW7=VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1='Z'
COL5ROW2=VK_BACK
COL5ROW3='C'
COL5ROW4='B'
COL5ROW5='M'
COL5ROW6=VK_PERIOD
COL5ROW7=VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=VK_F10
COL6ROW1='W'
COL6ROW2=VK_RETURN
COL6ROW3='R'
COL6ROW4='Y'
COL6ROW5='I'
COL6ROW6='5'
COL6ROW7='P'
;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0='E'
COL7ROW1=open
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4=VK_F6
COL7ROW5='7'
COL7ROW6=VK_F8
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only 2ND
;;-----
[Map]
MAP=MAP_2ND
;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_CAPITAL
COL0ROW2=ACTION+POWER
COL0ROW3=VK_PAUSE
COL0ROW4=open
COL0ROW5=open
COL0ROW6=VK_HYPHEN
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'1'
COL1ROW1=SHIFT+VK_EQUAL
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'5'
COL1ROW4=SHIFT+'7'
COL1ROW5=VK_EQUAL
COL1ROW6=SHIFT+'9'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;

```

```

COL2ROW0=SHIFT+VK_BACKSLASH
COL2ROW1=open
COL2ROW2=SHIFT+VK_SEMICOLON
COL2ROW3=SHIFT+VK_APOSTROPHE
COL2ROW4=VK_COMMA
COL2ROW5=VK_LBRACKET
COL2ROW6=SHIFT+VK_SLASH
COL2ROW7=SHIFT+VK_PERIOD
;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=VK_BACKQUOTE
COL3ROW5=SHIFT+VK_COMMA
COL3ROW6=VK_HOME
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=VK_BACKSLASH
COL4ROW2=VK_END
COL4ROW3=VK_SEMICOLON
COL4ROW4=VK_APOSTROPHE
COL4ROW5=VK_PERIOD
COL4ROW6=VK_RBRACKET
COL4ROW7=VK_PRIOR
;;;;;;;;;;;;;
COL5ROW0=SHIFT+VK_RBRACKET
COL5ROW1=open
COL5ROW2=VK_INSERT
COL5ROW3=open
COL5ROW4=SHIFT+VK_BACKQUOTE
COL5ROW5=SHIFT+VK_HYPHEN
COL5ROW6=VK_DELETE
COL5ROW7=VK_NEXT
;;;;;;;;;;;;;
COL6ROW0=ACTION+BACKLIGHT
COL6ROW1=SHIFT+ '2'
COL6ROW2=open
COL6ROW3=SHIFT+ '4'
COL6ROW4=SHIFT+ '6'
COL6ROW5=SHIFT+ '8'
COL6ROW6=SHIFT+VK_LBRACKET
COL6ROW7=SHIFT+ '0'
;;;;;;;;;;;;;
COL7ROW0=SHIFT+ '3'
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=CHANGE+MAP_CONTRAST
COL7ROW5=VK_SLASH
COL7ROW6=CHANGE+MAP_VOLUME
COL7ROW7=open

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with 2ND and SHIFT
;;-----
[Map]
MAP=MAP_2NDSHIFT
;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=open
COL0ROW5=open
COL0ROW6= '8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1= '9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=open

```

```

COL1ROW4=open
COL1ROW5='4'
COL1ROW6=open
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;
COL2ROW0=open
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=open
COL2ROW5='1'
COL2ROW6=open
COL2ROW7='3'
;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5='0'
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=open
COL4ROW3=open
COL4ROW4=open
COL4ROW5=open
COL4ROW6='2'
COL4ROW7=open
;;;;;;;;;;
COL5ROW0='6'
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;
COL6ROW0=open
COL6ROW1=open
COL6ROW2=open
COL6ROW3=open
COL6ROW4=open
COL6ROW5=open
COL6ROW6='5'
COL6ROW7=open
;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=SHIFT+VK_PAUSE
COL7ROW3=VK_SCROLL
COL7ROW4=VK_SNAPSHOT
COL7ROW5='7'
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only SHIFT
;;-----
[Map]
MAP=MAP_SHIFT
;;;;;;;;;;
COL0ROW0=SHIFT+VK_ESCAPE
COL0ROW1=SHIFT+VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_F2
COL0ROW4=SHIFT+VK_F5
COL0ROW5=SHIFT+VK_F7
COL0ROW6=SHIFT+'8'

```

```

COL0ROW7=ACTION+SCAN1
;;;;;;;;;;
COL1ROW0=SHIFT+'Q'
COL1ROW1=SHIFT+'9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'T'
COL1ROW4=SHIFT+'U'
COL1ROW5=SHIFT+'4'
COL1ROW6=SHIFT+'O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;
COL2ROW0=SHIFT+'A'
COL2ROW1=open
COL2ROW2=SHIFT+'D'
COL2ROW3=SHIFT+'G'
COL2ROW4=SHIFT+'J'
COL2ROW5=SHIFT+'L'
COL2ROW6=SHIFT+'L'
COL2ROW7=SHIFT+'3'
;;;;;;;;;;
COL3ROW0=SHIFT+' '
COL3ROW1=open
COL3ROW2=SHIFT+'X'
COL3ROW3=SHIFT+'V'
COL3ROW4=SHIFT+'N'
COL3ROW5=SHIFT+'0'
COL3ROW6=SHIFT+VK_LEFT
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;
COL4ROW0=SHIFT+VK_F9
COL4ROW1=SHIFT+'S'
COL4ROW2=SHIFT+VK_RIGHT
COL4ROW3=SHIFT+'F'
COL4ROW4=SHIFT+'H'
COL4ROW5=SHIFT+'K'
COL4ROW6=SHIFT+'2'
COL4ROW7=SHIFT+VK_UP
;;;;;;;;;;
COL5ROW0=SHIFT+'6'
COL5ROW1=SHIFT+'Z'
COL5ROW2=SHIFT+VK_BACK
COL5ROW3=SHIFT+'C'
COL5ROW4=SHIFT+'B'
COL5ROW5=SHIFT+'M'
COL5ROW6=SHIFT+VK_PERIOD
COL5ROW7=SHIFT+VK_DOWN
;;;;;;;;;;
COL6ROW0=SHIFT+VK_F10
COL6ROW1=SHIFT+'W'
COL6ROW2=SHIFT+VK_RETURN
COL6ROW3=SHIFT+'R'
COL6ROW4=SHIFT+'Y'
COL6ROW5=SHIFT+'I'
COL6ROW6=SHIFT+'5'
COL6ROW7=SHIFT+'P'
;;;;;;;;;;
COL7ROW0=SHIFT+'E'
COL7ROW1=open
COL7ROW2=SHIFT+VK_F3
COL7ROW3=SHIFT+VK_F4
COL7ROW4=SHIFT+VK_F6
COL7ROW5=SHIFT+'7'
COL7ROW6=SHIFT+VK_F8
COL7ROW7=open

;;-----
;; 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 MX7
;; 32-key keypad
;;-----
[Map]
MAP=MAP_NORMAL32
;;;;;;;;;;
COL0ROW0=KY_PROG1

```

```

COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=VK_RETURN
COL0ROW6='2'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=VK_SPACE
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0='4'
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4='9'
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;;
COL3ROW0=VK_SHIFT
COL3ROW1=open
COL3ROW2=VK_DELETE
COL3ROW3=VK_CONTROL
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;
COL4ROW0='1'
COL4ROW1=open
COL4ROW2=open
COL4ROW3='7'
COL4ROW4='8'
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_DOWN
;;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=KY_PROG2
COL5ROW2=VK_TAB
COL5ROW3='5'
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=VK_UP
;;;;;;;;;;;;;
COL6ROW0='3'
COL6ROW1=ACTION+KY_ALPHA
COL6ROW2=open
COL6ROW3='0'
COL6ROW4=open
COL6ROW5=open
COL6ROW6=open
COL6ROW7=VK_MENU
;;;;;;;;;;;;;
COL7ROW0='6'
COL7ROW1=KY_PROG3
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=open

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys modified with ORANGE

```

```

;; on the MX7 32-key keypad
;;-----
[Map]
MAP=MAP_ORANGE32
;;;;;;;;;;
COL0ROW0=SHIFT+'8'
COL0ROW1=VK_F6
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F7
COL0ROW4=VK_F10
COL0ROW5=open
COL0ROW6=VK_LBRACKET
COL0ROW7=CHANGE+MAP_VOLUME
;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=VK_BACK
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;
COL2ROW0=SHIFT+'3'
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=SHIFT+'4'
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;
COL3ROW0=VK_SHIFT
COL3ROW1=open
COL3ROW2=VK_PERIOD
COL3ROW3=VK_INSERT
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;
COL4ROW0=VK_BACKSLASH
COL4ROW1=open
COL4ROW2=open
COL4ROW3=SHIFT+VK_HYPHEN
COL4ROW4=SHIFT+VK_SLASH
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_NEXT
;;;;;;;;;;
COL5ROW0=open
COL5ROW1=VK_EQUAL
COL5ROW2=SHIFT+VK_TAB
COL5ROW3=SHIFT+'2'
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=VK_PRIOR
;;;;;;;;;;
COL6ROW0=VK_RBRACKET
COL6ROW1=VK_APOSTROPHE
COL6ROW2=open
COL6ROW3=SHIFT+VK_SEMICOLON
COL6ROW4=open
COL6ROW5=open
COL6ROW6=open
COL6ROW7=SHIFT+VK_BACKSLASH
;;;;;;;;;;
COL7ROW0=VK_COMMA
COL7ROW1=SHIFT+'1'
COL7ROW2=VK_F8
COL7ROW3=VK_F9
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=open

```

```

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys on the MX7 32-key keypad
;; modified with BLUE
;;-----
[Map]
MAP=MAP_BLUE32
;;;;;;;;;;;;
COL0ROW0=KY_PROG1B
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=VK_F15
COL0ROW5=open
COL0ROW6=VK_LBRACKET
COL0ROW7=CHANGE+MAP_BRITE
;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=VK_HYPHEN
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;
COL2ROW0=SHIFT+VK_LBRACKET
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=SHIFT+VK_BACKQUOTE
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;
COL3ROW0=VK_SHIFT
COL3ROW1=open
COL3ROW2=SHIFT+VK_EQUAL
COL3ROW3=SHIFT+'6'
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;
COL4ROW0=VK_SLASH
COL4ROW1=open
COL4ROW2=open
COL4ROW3=SHIFT+VK_COMMA
COL4ROW4=SHIFT+VK_PERIOD
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_LEFT
;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=SHIFT+'9'
COL5ROW2=VK_CAPITAL
COL5ROW3=SHIFT+VK_RBRACKET
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=VK_RIGHT
;;;;;;;;;;;;
COL6ROW0=VK_RBRACKET
COL6ROW1=SHIFT+VK_APOSTROPHE
COL6ROW2=open
COL6ROW3=VK_SEMICOLON
COL6ROW4=open
COL6ROW5=open
COL6ROW6=open
COL6ROW7=VK_ESCAPE
;;;;;;;;;;;;
COL7ROW0=VK_BACKQUOTE
COL7ROW1=SHIFT+'0'

```

```

COL7ROW2=VK_F13
COL7ROW3=VK_F14
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=open

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys on the MX7 32-key keypad
;; modified with SHIFT
;;-----
[Map]
MAP=MAP_SHIFT32
;;;;;;;;;;;;
COL0ROW0=KY_PROG1S
COL0ROW1=VK_F16
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F17
COL0ROW4=VK_F20
COL0ROW5=open
COL0ROW6=SHIFT+'2'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=VK_SPACE
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;
COL2ROW0=SHIFT+'4'
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=SHIFT+'9'
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;
COL3ROW0=VK_SHIFT
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;
COL4ROW0=SHIFT+'1'
COL4ROW1=open
COL4ROW2=open
COL4ROW3=SHIFT+'7'
COL4ROW4=SHIFT+'8'
COL4ROW5=open
COL4ROW6=open
COL4ROW7=VK_HOME
;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=KY_PROG2S
COL5ROW2=open
COL5ROW3=SHIFT+'5'
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=VK_END
;;;;;;;;;;;;
COL6ROW0=SHIFT+'3'
COL6ROW1=open
COL6ROW2=open
COL6ROW3=SHIFT+'0'
COL6ROW4=open

```



```

COL6ROW5=open
COL6ROW6=open
COL6ROW7=open
;;;;;;;;;;;;;
COL7ROW0=SHIFT+'6'
COL7ROW1=KY_PROG3S
COL7ROW2=VK_F18
COL7ROW3=VK_F19
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=open

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for unmodified keys on the
;; MX7 55-key keypad
;;-----
[Map]
MAP=MAP_NORMAL55
;;;;;;;;;;;;;
COL0ROW0=KY_PROG1
COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=open
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;
COL1ROW0='Q'
COL1ROW1='9'
COL1ROW2=open
COL1ROW3='T'
COL1ROW4='U'
COL1ROW5='4'
COL1ROW6='O'
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0='A'
COL2ROW1=open
COL2ROW2='D'
COL2ROW3='G'
COL2ROW4='J'
COL2ROW5='1'
COL2ROW6='L'
COL2ROW7='3'
;;;;;;;;;;;;;
COL3ROW0=' '
COL3ROW1=open
COL3ROW2='X'
COL3ROW3='V'
COL3ROW4='N'
COL3ROW5='0'
COL3ROW6=open
COL3ROW7=VK_TAB
;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1='S'
COL4ROW2=VK_DELETE
COL4ROW3='F'
COL4ROW4='H'
COL4ROW5='K'
COL4ROW6='2'
COL4ROW7=VK_DOWN
;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1='Z'
COL5ROW2=VK_MENU
COL5ROW3='C'
COL5ROW4='B'
COL5ROW5='M'
COL5ROW6=open
COL5ROW7=VK_UP

```

```

;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1='W'
COL6ROW2=VK_RETURN
COL6ROW3='R'
COL6ROW4='Y'
COL6ROW5='I'
COL6ROW6='5'
COL6ROW7='P'
;;;;;;;;;;;;;
COL7ROW0='E'
COL7ROW1=VK_SHIFT
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4='7'
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=VK_CONTROL

;;-----
;; 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_ORANGE55
;;;;;;;;;;;;;
COL0ROW0=KY_PROG10
COL0ROW1=VK_F6
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F7
COL0ROW4=VK_F10
COL0ROW5=open
COL0ROW6=open
COL0ROW7=CHANGE+MAP_VOLUME
;;;;;;;;;;;;;
COL1ROW0=SHIFT+'1'
COL1ROW1=open
COL1ROW2=open
COL1ROW3=SHIFT+'5'
COL1ROW4=SHIFT+'7'
COL1ROW5=open
COL1ROW6=SHIFT+'9'
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0=SHIFT+VK_BACKSLASH
COL2ROW1=open
COL2ROW2=SHIFT+VK_SEMICOLON
COL2ROW3=SHIFT+VK_APOSTROPHE
COL2ROW4=VK_COMMA
COL2ROW5=open
COL2ROW6=SHIFT+VK_SLASH
COL2ROW7=open
;;;;;;;;;;;;;
COL3ROW0=VK_BACK
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=VK_BACKQUOTE
COL3ROW5=open
COL3ROW6=open
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=VK_BACKSLASH
COL4ROW2=VK_PERIOD
COL4ROW3=VK_SEMICOLON
COL4ROW4=VK_APOSTROPHE
COL4ROW5=VK_PERIOD
COL4ROW6=open
COL4ROW7=VK_NEXT
;;;;;;;;;;;;;
COL5ROW0=open
COL5ROW1=open
COL5ROW2=open

```

```

COL5ROW3=open
COL5ROW4=SHIFT+VK_BACKQUOTE
COL5ROW5=SHIFT+VK_HYPHEN
COL5ROW6=open
COL5ROW7=VK_PRIOR
;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1=SHIFT+'2'
COL6ROW2=open
COL6ROW3=SHIFT+'4'
COL6ROW4=SHIFT+'6'
COL6ROW5=SHIFT+'8'
COL6ROW6=open
COL6ROW7=SHIFT+'0'
;;;;;;;;;;;;;
COL7ROW0=SHIFT+'3'
COL7ROW1=VK_SHIFT
COL7ROW2=VK_F8
COL7ROW3=VK_F9
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=VK_INSERT

;;-----
;; 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 MX7 55-key keypad
;; modified with BLUE
;;-----
[Map]
MAP=MAP_BLUE55
;;;;;;;;;;;;;
COL0ROW0=KY_PROG1B
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=VK_F15
COL0ROW5=open
COL0ROW6=open
COL0ROW7=CHANGE+MAP_BRITE
;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1=open
COL1ROW2=open
COL1ROW3=VK_EQUAL
COL1ROW4=open
COL1ROW5=open
COL1ROW6=open
COL1ROW7=open
;;;;;;;;;;;;;
COL2ROW0=open
COL2ROW1=open
COL2ROW2=open
COL2ROW3=SHIFT+VK_COMMA
COL2ROW4=VK_SLASH
COL2ROW5=open
COL2ROW6=open
COL2ROW7=open
;;;;;;;;;;;;;
COL3ROW0=VK_HYPHEN
COL3ROW1=open
COL3ROW2=SHIFT+VK_RBRACKET
COL3ROW3=CHANGE+MAP_VOLUME
COL3ROW4=open
COL3ROW5=open
COL3ROW6=open
COL3ROW7=VK_CAPITAL
;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=SHIFT+VK_EQUAL
COL4ROW3=open
COL4ROW4=SHIFT+VK_PERIOD
COL4ROW5=open

```

```

COL4ROW6=open
COL4ROW7=VK_LEFT
//////////
COL5ROW0=open
COL5ROW1=VK_RBRACKET
COL5ROW2=VK_ESCAPE
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=VK_RIGHT
//////////
COL6ROW0=open
COL6ROW1=SHIFT+VK_LBRACKET
COL6ROW2=open
COL6ROW3=open
COL6ROW4=VK_LBRACKET
COL6ROW5=VK_INSERT
COL6ROW6=open
COL6ROW7=SHIFT+VK_EQUAL
//////////
COL7ROW0=open
COL7ROW1=VK_SHIFT
COL7ROW2=VK_F13
COL7ROW3=VK_F14
COL7ROW4=open
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=open

;;-----
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys on the MX7 55-key keypad
;; modified with SHIFT
;;-----
[Map]
MAP=MAP_SHIFT55
//////////
COL0ROW0=KY_PROG1S
COL0ROW1=VK_F16
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F17
COL0ROW4=VK_F20
COL0ROW5=open
COL0ROW6=SHIFT+'8'
COL0ROW7=ACTION+SCAN1
//////////
COL1ROW0=SHIFT+'Q'
COL1ROW1=SHIFT+'9'
COL1ROW2=open
COL1ROW3=SHIFT+'T'
COL1ROW4=SHIFT+'U'
COL1ROW5=SHIFT+'4'
COL1ROW6=SHIFT+'O'
COL1ROW7=open
//////////
COL2ROW0=SHIFT+'A'
COL2ROW1=open
COL2ROW2=SHIFT+'D'
COL2ROW3=SHIFT+'G'
COL2ROW4=SHIFT+'J'
COL2ROW5=SHIFT+'1'
COL2ROW6=SHIFT+'L'
COL2ROW7=SHIFT+'3'
//////////
COL3ROW0=open
COL3ROW1=open
COL3ROW2=SHIFT+'X'
COL3ROW3=SHIFT+'V'
COL3ROW4=SHIFT+'N'
COL3ROW5=SHIFT+'0'
COL3ROW6=open
COL3ROW7=open
//////////

```

```

COL4ROW0=open
COL4ROW1=SHIFT+'S'
COL4ROW2=open
COL4ROW3=SHIFT+'F'
COL4ROW4=SHIFT+'H'
COL4ROW5=SHIFT+'K'
COL4ROW6=SHIFT+'2'
COL4ROW7=VK_HOME
;;;;;;;;;;;;;
COL5ROW0=SHIFT+'6'
COL5ROW1=SHIFT+'Z'
COL5ROW2=open
COL5ROW3=SHIFT+'C'
COL5ROW4=SHIFT+'B'
COL5ROW5=SHIFT+'M'
COL5ROW6=open
COL5ROW7=VK_END
;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1=SHIFT+'W'
COL6ROW2=open
COL6ROW3=SHIFT+'R'
COL6ROW4=SHIFT+'Y'
COL6ROW5=SHIFT+'I'
COL6ROW6=SHIFT+'5'
COL6ROW7=SHIFT+'P'
;;;;;;;;;;;;;
COL7ROW0=SHIFT+'E'
COL7ROW1=VK_SHIFT
COL7ROW2=VK_F18
COL7ROW3=VK_F19
COL7ROW4=SHIFT+'7'
COL7ROW5=KY_ORANGE
COL7ROW6=KY_BLUE
COL7ROW7=VK_CONTROL

;;-----
;; 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=open
COL0ROW1=VK_F21
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F22
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=open
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=VK_F23
COL7ROW3=VK_F24
COL7ROW4=open
COL7ROW5=open
COL7ROW6=open
COL7ROW7=open
```

Sample Output File

```
[HKEY_CURRENT_USER\Keyboard Layout\Keymaps\Default]
"HKL"="00000409"
"Head"=hex: 0D,08,08,40,00,00,02,27,2F,07,0F,0A,40,48,50,58
"Map0"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00
"Flag0"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
"Map1"=hex:\
    00,14,DF,13,00,00,BD,87,31,BB,89,35,37,BB,39,88,\
    DC,00,BA,DE,BC,DB,BF,BE,00,00,00,00,C0,BC,24,09,\
    00,DC,23,BA,DE,BE,DD,21,DD,00,2D,00,C0,BD,2E,22,\
    8A,32,00,34,36,38,DB,30,33,00,00,00,00,BF,00,00
"Flag1"=hex:\
    00,00,A0,00,00,00,00,A0,10,10,A0,10,10,00,10,A0,\
    10,00,10,10,00,00,10,10,00,00,00,00,00,10,00,10,\
    00,00,00,00,00,00,00,10,00,00,00,10,10,00,00,\
    A0,10,00,10,10,10,10,10,00,00,00,8E,00,8D,00
"Map2"=hex:\
    00,7A,DF,7B,00,00,38,87,00,39,89,00,00,34,00,88,\
    00,00,00,00,00,31,00,33,00,00,00,00,00,30,00,00,\
    00,00,00,00,00,00,32,00,36,00,00,00,00,00,00,\
    00,00,00,00,00,00,35,00,00,00,13,91,2C,37,00,00
"Flag2"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,10,00,00,00,00,00
"Map3"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00
"Flag3"=hex:\
    10,10,A0,10,10,10,10,A0,10,10,A0,10,10,10,10,A0,\
    10,00,10,10,10,10,10,10,10,00,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,00,10,10,10,10,10,00
"Map4"=hex:\
    E9,70,DF,71,74,0D,32,87,00,00,00,20,00,00,00,00,\
    34,00,00,00,39,00,00,00,10,00,2E,11,00,00,00,00,\
    31,00,00,37,38,00,00,28,00,ED,09,35,00,00,00,26,\
    33,F1,00,30,00,00,00,12,36,EF,72,73,00,F2,F3,00
"Flag4"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,A0,00,00,00,00,00,00,00,00,00,00,00,00,00,00
"Map5"=hex:\
    38,75,DF,76,79,00,DB,00,00,00,00,08,00,00,00,00,\
    33,00,00,00,34,00,00,00,10,00,BE,2D,00,00,00,00,\
    DC,00,00,BD,BF,00,00,22,00,BB,09,32,00,00,00,21,\
    DD,DE,00,BA,00,00,00,DC,BC,31,77,78,00,F2,F3,00
"Flag5"=hex:\
    10,00,A0,00,00,00,00,8D,00,00,00,00,00,00,00,00,\
    10,00,00,00,10,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,10,10,00,00,00,00,00,10,10,00,00,00,\
    00,00,00,10,00,00,00,10,00,10,00,00,00,00,00,00
"Map6"=hex:\
    EC,7A,DF,7B,7E,00,DB,00,00,00,00,BD,00,00,00,00,\
    DB,00,00,00,C0,00,00,00,10,00,BB,36,00,00,00,00,\
    BF,00,00,BC,BE,00,00,25,00,39,14,DD,00,00,00,27,\
    DD,DE,00,BA,00,00,00,1B,C0,30,7C,7D,00,F2,F3,00
"Flag6"=hex:\
    00,00,A0,00,00,00,00,8F,00,00,00,00,00,00,00,00,\
    10,00,00,00,10,00,00,00,00,00,10,10,00,00,00,\
    00,00,00,10,10,00,00,00,00,10,00,10,00,00,00,\
    00,10,00,00,00,00,00,00,00,10,00,00,00,00,00,00
```

```

"Map7"=hex:\
EA,7F,DF,80,83,00,32,87,00,00,00,20,00,00,00,00,\
34,00,00,00,39,00,00,00,10,00,00,00,00,00,00,\
31,00,00,37,38,00,00,24,00,EE,00,35,00,00,00,23,\
33,00,00,30,00,00,00,00,36,F0,81,82,00,F2,F3,00
"Flag7"=hex:\
00,00,A0,00,00,00,10,A0,00,00,00,00,00,00,00,\
10,00,00,00,10,00,00,00,00,00,00,00,00,00,\
10,00,00,10,10,00,00,00,00,00,00,10,00,00,00,\
10,00,00,10,00,00,00,00,10,00,00,00,00,00,00
"Map8"=hex:\
E9,70,DF,71,74,00,38,87,51,39,00,54,55,34,4F,00,\
41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,00,09,\
00,53,2E,46,48,4B,32,28,36,5A,12,43,42,4D,00,26,\
00,57,0D,52,59,49,35,50,45,10,72,73,37,F2,F3,11
"Flag8"=hex:\
00,00,A0,00,00,00,00,A0,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00
"Map9"=hex:\
EB,75,DF,76,79,00,00,00,31,00,00,35,37,00,39,00,\
DC,00,BA,DE,BC,00,BF,00,08,00,00,00,C0,00,00,09,\
00,DC,BE,BA,DE,BE,00,22,00,00,00,00,C0,BD,00,21,\
00,32,00,34,36,38,00,30,33,10,77,78,00,F2,F3,2D
"Flag9"=hex:\
00,00,A0,00,00,00,00,8D,10,00,00,10,10,00,10,00,\
10,00,10,10,00,00,10,00,00,00,00,00,00,00,10,\
00,00,00,00,00,00,00,00,00,00,00,00,00,10,10,00,\
00,10,00,10,10,10,00,10,10,00,00,00,00,00,00
"Map10"=hex:\
EC,7A,DF,7B,7E,00,00,00,00,00,00,00,BB,00,00,00,\
00,00,00,BC,BF,00,00,00,BD,00,DD,00,00,00,00,14,\
00,00,BB,00,BE,00,00,25,00,DD,1B,00,00,00,00,27,\
00,DB,00,00,DB,2D,00,BB,00,10,7C,7D,00,F2,F3,00
"Flag10"=hex:\
00,00,A0,00,00,00,00,8F,00,00,00,00,00,00,00,\
00,00,00,10,00,00,00,00,00,00,10,8D,00,00,00,\
00,00,10,00,10,00,00,00,00,00,00,00,00,00,00,\
00,10,00,00,00,00,00,10,00,00,00,00,00,00,00
"Map11"=hex:\
EA,7F,DF,80,83,00,38,87,51,39,00,54,55,34,4F,00,\
41,00,44,47,4A,31,4C,33,00,00,58,56,4E,30,00,00,\
00,53,00,46,48,4B,32,24,36,5A,00,43,42,4D,00,23,\
00,57,00,52,59,49,35,50,45,10,81,82,37,F2,F3,11
"Flag11"=hex:\
00,00,A0,00,00,00,10,A0,10,10,00,10,10,10,10,00,\
10,00,10,10,10,10,10,10,00,00,10,10,10,10,00,\
00,10,00,10,10,10,10,00,10,10,00,10,10,10,00,\
00,10,00,10,10,10,10,10,10,00,00,00,10,00,00
"Map12"=hex:\
00,84,DF,85,00,00,00,00,00,00,00,00,00,00,00,\
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,\
00,00,00,00,00,00,00,00,00,00,86,87,00,00,00
"Flag12"=hex:\
00,00,A0,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00

```


Appendix B Technical Specifications

Physical Specifications

Features		Specifications	Comments	
CPU		Intel Xscale operating at 400 MHz	32 bit CPU (with on-chip cache)	
Memory	RAM	128 MB / 512MB / 1GB SDRAM		
Display	LCD	Transmissive Color – optimized for indoor use	Transmissive LCD with touchscreen. Customer Configurable Display LED Backlighting	
Mass Storage	Removable SD Card	128MB 32MB available for customer use	SD Flash Card FAT file system	
PCMCIA Interface		None		
Weights		Unit with network card, battery, SE1524ER scanner and handle	1.6 lbs (26.1 oz)	740g
		Unit with network card, battery, SE1524ER scanner and handstrap	1.4 lbs (22.6 oz)	640g
		Battery	4.3 oz	122g
		Handle	4 oz	110g
		Summit client - 2.4GHz USB 802.11b/g	0.35 oz	9.9g
		Cisco client – 2.4GHz CF 802.11b/g	.5 oz	15g
		SD Flash Card	1 oz	28g
External Connectors/Interface		RS-232 COM1 mini D serial port	20 Position “D” (female) Connector. Provides cabled connection to external devices such as an audio headset, printer, USB/power connection, RS-232/power connection.	
Dimensions		Length	8.8”	22.3 cm
		Width at display	3.4”	8.6 cm
		Width at handgrip	2.8”	7.1 cm
		Depth at Scanner	2”	5.1 cm
		Depth at Battery	1.7”	4.3 cm

Features		Specifications	Comments
Scanner		No Scanner Intermec EV-15 Linear Imager HHP 5380 SF 2D Imager Symbol SE824 Short Range Symbol SE1524ER Lorax Symbol SE955 Short Range	Integrated SE955 replaced SE824 in July 2006.
Batteries	Main	Li-Ion battery pack 7.4V 2.4Ah	In-Unit Chargeable or Externally Chargeable
	Backup (CMOS)	Internal Nickel Cadmium (NiCd) 1.42V max.	Automatically charges from main battery during normal operation. Requires AC power for re-charging. Memory operational for 24 hours when main battery is depleted. Minimal life expectancy is 2 years.
Network card	802.11 b/g LXE	2.4GHz (USB 2.0 device in PCMCIA Card)	Supports diversity. Dynamic control for power management.
	802.11 b/g LXE	2.4GHz (Compact Flash device in PCMCIA Adapter Card)	Supports diversity. Dynamic control for power management.

Display Specifications

Type	LCD – Active Transmissive Color / LED Backlight
Resolution	320 (Vertical) x 240 (Horizontal) pixels
Size	1/4 VGA portrait
Diagonal Viewing Area	3.5 in (8.9cm)
Dot Pitch	0.22mm
Dot Size	0.20mm x 0.20mm
Color Scale	Reflective – 256 colors

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
Operating Frequency	2.402 – 2.480 GHz
Operating Temperature	see MX7 Environmental Specifications
Storage Temperature	see MX7 Environmental Specifications
Bluetooth Version	2.0 + EDR

Environmental Specifications

MX7

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 “MX7 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

Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Thermal 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	+12V, regulated
Output Current	0 Amps min, 1.25 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)

Network Device Specifications

Summit 802.11 b/g

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless 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 MX7 Environmental Specs
Storage Temperature	see MX7 Environmental Specs
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Summit 802.11 a/b/g

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 - 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0 GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	see MX7 Environmental Specs
Storage Temperature	see MX7 Environmental Specs
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Odyssey Client

Bus Interface	USB Interface
Wireless Frequencies	2.400GHz to 2.4835GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	18 dBm 64mW Max
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	see Environmental Specs
Storage Temperature	see Environmental Specs
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Appendix C Reference Material

Introduction

Contents of this Appendix include:

- AppLock – Single Version Application.
- Includes information and instruction for an MX7 using AppLock to manage a single application. AppLock error messages and registry settings are also included.
- MX7 Reference Guide Revision History

and the following charts:

- Valid VK Codes for CE
- ASCII Control Codes
- Hat Encoding
- Decimal-Hexadecimal Chart

AppLock - Single Application Version

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



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. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified application is automatically launched and run in full screen mode when the device completes the boots up process.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

Determine Your AppLock Version


If the Administrator Control Menu looks like this . . .	Go to . . .
	This appendix.
	Chapter 6 - AppLock

Determine Your AppLock Version

Setup a New Device

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies a password, an application to lock, and the device is rebooted or the hotkey is pressed, the mobile 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*.
2. Connect an external power source to the device (if required). See *Chapter 1 - Introduction*.
3. Adjust screen display, audio volume and other parameters if desired. See *Chapter 1 - Introduction*.
4. Tap  | Settings | Control Panel | Administration icon.
5. Assign an application on the **Control** tab screen. See *Control Panel*.
6. Assign a password on the **Security** tab screen. See *Security Panel*.
7. Select a view level on the **Status** tab screen, if desired. See *Status Panel*.
8. Tap OK.
9. Press the hotkey sequence to launch AppLock and lock the configured application. See *Security Panel*.
10. The mobile device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software 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 to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	55-key : Shift+Ctrl+A 32-key : Requires Alpha Mode
Password	none
Application path and name	none
Application command line	none

End User Mode

End-user mode locks the end-user into the configured application. The end user can still reboot and respond to dialog boxes. The application is automatically launched, and runs in full screen mode after the boot up sequence completes.

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 application 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 hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- 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.

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

or

Ctrl+5 Ctrl+9 Ctrl+3

Application Configuration

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three attempts) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Administrator Control Panels

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

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



Administrator Control Panels – Single Application

Control Panel



Control Panel – Single Application

Note: If your Administrator Control Panel does not look like the figure shown above, you may have the Multi-Application version.

Use the Control tab options to select the application to launch when the device boots up.

Move the cursor to the Application text box and either type the application path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.

Enter the command line parameters for the application in the Command Line text box.

Enter the number of seconds the selected Application must wait before starting to run upon reboot.

If no application is specified when the Administrator Control panel is closed, the device reboots into Administrator mode. If a password has been set, but the application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

End User Internet Explorer

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode, End-user Internet Explorer (EUIE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by simply checking the "Internet" checkbox in the Control tab of the Administrator applet. The internet application should then be entered in the "Application" text box. If the standard Internet Explorer that is shipped with the device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel



Security Panel – Single Application

Specify 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 2nd 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 modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

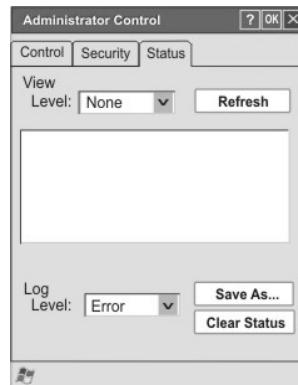
Setting a Password

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords

Status Panel



Status Panel – Single Application

Note: If your Status Panel does not look like the figure shown above, you may have the Multi-Application version.

Use the Status panel to view the log of previous AppLock operation and to configure which messages are to be recorded during AppLock operation.

As the status information is stored in the registry and accumulates during AppLock configuration and operation, it is very important that the administrator periodically clear the status information to reduce the amount of registry space used. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Levels

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is '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
- Error

- Processing
- Extended
- All

Save As

When the 'Save As'... button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: AppLock Error Messages

AppLock 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 triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX

Message	Explanation and/or corrective action	Level
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX

Message	Explanation and/or corrective action	Level
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX

Message	Explanation and/or corrective action	Level
In app hook:WM_WINDOWPOSCANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. 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

Message	Explanation and/or corrective action	Level
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR

Message	Explanation and/or corrective action	Level
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

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 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\\Administration\\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=
```

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
DC3	13	^S	Device Control 3, normally XOFF	Ctrl-s
DC4	14	^T	Device Control 4	Ctrl-t
NAK	15	^U	Negative AcKnowledge	Ctrl-u
SYN	16	^V	SYNchronous idle	Ctrl-v
ETB	17	^W	End Transmission Block	Ctrl-w

Char	Hex	Control-Key	Control Action	
CAN	17	^X	CANcel line	Ctrl-x
EM	19	^Y	End of Medium	Ctrl-y
SUB	1a	^Z	SUBstitute	Ctrl-z
ESC	1b	^[ESCape	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1b VK_PACKET up VK_CONTROL up
FS	1c	^\	File Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1c VK_PACKET up VK_CONTROL up
GS	1d	^]	Group Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1d down WM_CHAR (0x1d) up VK_PACKET up VK_CONTROL up
RS	1e	^^	Record Separator	VK_CONTROL (0x11)down VK_SHIFT (0x10) down WM_CHAR 0x36 down WM_CHAR 0x36 up VK_SHIFT up VK_CONTROL up
US	1f	^_	Unit Separator	VK_CONTROL (0x11) down VK_SHIFT (0x10) down VK_PACKET (0xe7) down WM_CHAR 0x1f VK_PACKET (0xe7) up VK_SHIFT (0x10) up VK_CONTROL (0x11) up

Hat Encoding

The MX7 supports only 7-bit hat encoding which means only ^@ through ^_ (underscore) are supported.

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^_ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
-	AF	~/
°	B0	~0 (Zero)
±	B1	~1
²	B2	~2

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTs	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~\$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z
Û	DB	~[

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

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

Decimal - Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42 ¹¹	0x2A	82	0x52	122	0x7A
3	0x03	43	0x2B	83	0x53	123	0x7B
4	0x04	44	0x2C	84	0x54	124	0x7C
5	0x05	45	0x2D	85	0x55	125	0x7D
6	0x06	46	0x2E	86	0x56	126	0x7E
7	0x07	47	0x2F	87	0x57	127	0x7F
8	0x08	48	0x30	88	0x58	128	0x80
9	0x09	49	0x31	89	0x59	129	0x81
10	0x0A	50	0x32	90	0x5A	130	0x82
11	0x0B	51	0x33	91	0x5B	131	0x83
12	0x0C	52	0x34	92	0x5C	132	0x84
13	0x0D	53	0x35	93	0x5D	133	0x85
14	0x0E	54	0x36	94	0x5E	134	0x86
15	0x0F	55	0x37	95	0x5F	135	0x87
16	0x10	56	0x38	96	0x60	136	0x88
17	0x11	57	0x39	97	0x61	137	0x89
18	0x12	58	0x3A	98	0x62	138	0x8A
19	0x13	59	0x3B	99	0x63	139	0x8B
20	0x14	60	0x3C	100	0x64	140	0x8C
21	0x15	61	0x3D	101	0x65	141	0x8D
22	0x16	62	0x3E	102	0x66	142	0x8E
23	0x17	63	0x3F	103	0x67	143	0x8F
24	0x18	64	0x40	104	0x68	144	0x90
25	0x19	65	0x41	105	0x69	145	0x91
26	0x1A	66	0x42	106	0x6A	146	0x92
27	0x1B	67	0x43	107	0x6B	147	0x93
28	0x1C	68	0x44	108	0x6C	148	0x94
29	0x1D	69	0x45	109	0x6D	149	0x95
30	0x1E	70	0x46	110	0x6E	150	0x96
31	0x1F	71	0x47	111	0x6F	151	0x97
32	0x20	72	0x48	112	0x70	152	0x98
33	0x21	73	0x49	113	0x71	153	0x99
34	0x22	74	0x4A	114	0x72	154	0x9A
35	0x23	75	0x4B	115	0x73	155	0x9B
36	0x24	76	0x4C	116	0x74	156	0x9C
37	0x25	77	0x4D	117	0x75	157	0x9D
38	0x26	78	0x4E	118	0x76	158	0x9E
39	0x27	79	0x4F	119	0x77	159	0x9F

Decimal - Hexadecimal Chart (0 to 159 Decimal)

¹¹ The Answer to Life, the Universe and Everything.

160	0xA0	200	0xC8	240	0xF0
161	0xA1	201	0xC9	241	0xF1
162	0xA2	202	0xCA	242	0xF2
163	0xA3	203	0xCB	243	0xF3
164	0xA4	204	0xCC	244	0xF4
165	0xA5	205	0xCD	245	0xF5
166	0xA6	206	0xCE	246	0xF6
167	0xA7	207	0xCF	247	0xF7
168	0xA8	208	0xD0	248	0xF8
169	0xA9	209	0xD1	249	0xF9
170	0xAA	210	0xD2	250	0xFA
171	0xAB	211	0xD3	251	0xFB
172	0xAC	212	0xD4	252	0xFC
173	0xAD	213	0xD5	253	0xFD
174	0xAE	214	0xD6	254	0xFE
175	0xAF	215	0xD7	255	0xFF
176	0xB0	216	0xD8		
177	0xB1	217	0xD9		
178	0xB2	218	0xDA		
179	0xB3	219	0xDB		
180	0xB4	220	0xDC		
181	0xB5	221	0xDD		
182	0xB6	222	0xDE		
183	0xB7	223	0xDF		
184	0xB8	224	0xE0		
185	0xB9	225	0xE1		
186	0xBA	226	0xE2		
187	0xBB	227	0xE3		
188	0xBC	228	0xE4		
189	0xBD	229	0xE5		
190	0xBE	230	0xE6		
191	0xBF	231	0xE7		
192	0xC0	232	0xE8		
193	0xC1	233	0xE9		
194	0xC2	234	0xEA		
195	0xC3	235	0xEB		
196	0xC4	236	0xEC		
197	0xC5	237	0xED		
198	0xC6	238	0xEE		
199	0xC7	239	0xEF		

Decimal - Hexadecimal Chart (160 to 255 Decimal)

Revision History

Revision F, November 2007

- Chapter 1 – Introduction -- Updated *Bluetooth* segment. Added Mobile Bluetooth Barcode Readers to *Accessories*.
- Chapter 3 – System Configuration -- Added *Bluetooth to Optional Software* segment. Updated *GrabTime* segment. Terminology update: Avalanche Mobility Center. Terminology update: Bluetooth.
- Chapter 4 – Scanner -- Added *Length Based Barcode Stripping*.
- Chapter 5 – Wireless Network Configuration -- Added EAP-FAST and EAP-TLS instruction. Updated *Summit Client Utility* to reflect version differences.

Revision E, May 2007

- Chapter 1 – Introduction -- Added Bluetooth information. Updated Accessories. Added reference to MX7 Cradle Reference Guide.
- Chapter 2 – Physical Description and Layout -- Added Bluetooth information. Renamed “Passive Vehicle Mount Cradle” section to “MX7 Cradles”.
- Chapter 3 – System Configuration -- Added Bluetooth information. Added Keypad backlight information to Keyboard Properties panel. Added Remote Display to Start Menu | Communications.
- Chapter 6 – AppLock -- Added AppLock Launch support. Moved AppLock Single Application Version section to Appendix C – Reference Material.
- Appendix C – Reference Material -- New.

Revision D, February 2007

- Notices – Updated trademark statements.
- Chapter 1 – Introduction -- Added 2D Imager instruction.
- Chapter 2 – Physical Description and Layout -- Added 2D Imager information and instruction to “Scanner/Imager Port”.
- Chapter 4 – Scanner -- Added 2D Imager information.
- Chapter 5 – Wireless Network Configuration -- Added EAP-FAST. Updated Summit Client Utility to reflect version update changes.

Revision C, December 2006

- Notices -- Updated trademark statements.
- Chapter 1 – Introduction -- “Connecting an External Power Source” edited to ensure external power adapter is receiving AC power before AC power is cabled to the MX7 I/O port.
- Chapter 2 – Physical Description -- Added Primary Event tables to “Power Modes” sections where applicable.
- Chapter 3 – System Configuration -- Added “AppLock (Option)” and “Wavelink Avalanche Enabler (Option)”. Added “Determine Your Scanner Software Version” chart at beginning of “Control Panel | Scanner” section. Noted the newest scanner applet is now in Chapter 4 “Scanner”. Added “Wavelink Avalanche Enabler Configuration”.
- Chapter 4 – AppLock -- Renumbered Chapter 4 “AppLock” to Chapter 6. No change to contents.
- Chapter 4 – Scanner -- New.
- Chapter 5 – Wireless Network Configuration -- Changed “radio” to “wireless” or “client” in context, if suitable. Added “Sign-on Screen for LEAP, PEAP/MS-CHAP, PEAP/GTC”. Added configuration instruction for PEAP/GTC on Summit devices. Updated parameters and options based on Summit version 1.2.10 differences.

- Chapter 6 – AppLock -- Chapter number change. No change to contents.
- Appendix B – Technical Specifications -- Added “Hat Encoding” and “Decimal-Hexadecimal Chart” for Chapter 4 “Scanner” user. Added “Revision History”.
- Entire Manual -- Changed “radio” to “wireless” or “client” in context, if suitable. Changed Chapter cross-references to match Chapter number changes.

Revision B, August 2006

- Notices -- Added WEEE statement. Added trademarked statement for Summit Data Communications and Odyssey Client.
- Entire Manual -- Noted the replacement of SE824 scanner with SE955 scanner where applicable. Removed references to Bluetooth except to state that it is not supported.
- Chapter 1 – Introduction -- Added section titled “Features” Added Multi AppLock activation key instruction. Added Summit Client Desktop panel to section titled “Quick Start”. “Installing Trigger Handle”: Added: “*Equipment Needed*: Torque wrench capable of torquing to 3 ± 1 in/lb ($.34\pm .11$ N/m)”. Removed “and washers” from step 5 and included torque instruction in step 6. Expanded end-user instruction for voice data entry using audio cable and headsets. Accessories: Updated to reflect ROHS compliance. Added voice accessories. Removed MX7A309PSACWW. Added 9000A302PSACWW - AC/DC power supply, int’l, no power cord. Added SE955 scanner. Noted the replacement of SE824 scanner with SE955 scanner where applicable.
- Chapter 2 – Physical Description and Layout -- Removed statement referring to low battery warning dialog box and edited “Power Supply” section for clarification.
- Chapter 3 – System Configuration -- Added user information for JAVA option. Updated battery charge panels – Battery Panel and Power Panel. Updated scanner panels with barcode wedge enhancement. Moved Odyssey Client menu information and Summit Client menu information from “Start | Control Panel” section to Chapter 5 “Wireless Network Configuration”. Corrected Order statement for Utilities | LXE Login Install and LXE Login. Updated “LAUNCH.EXE” persist settings. Added new sections to Utilities: “Enabling GrabTime”, “Configuring CapsLock Behavior”, “Launch App / Launch Command” and “Configuring IPv6”. Added Summit Client panel to section titled “Network and Dial-Up Connections”.
- Chapter 4 – AppLock -- Added Multi AppLock instruction.
- Chapter 5 – Wireless Network Configuration -- Added instruction for Summit Client Utility software. Odyssey Client: Added instructions for setting No Security and WEP-LEAP. Instructions for LEAP with WPA are included in section for EAP-LEAP.
- Appendix A – Keymaps -- Added section titled “Creating Custom Keymaps”.
- Appendix B – Technical Specifications -- Added technical specifications for the *LXE CF Radio in PCMCIA Adapter card*. Added note about SE955 scanner replacing SE824 scanner where applicable.

Revision A, Initial Release, December 2005

Index

2D Imager	38
32-key keypad.....	57
55-key 5250 keypad.....	57
55-key keypad.....	57

A

About	
software, hardware, version, network IP	96
AC External Power Supply, How to.....	15
AC Power Adapter	
Assembly.....	15
Accessibility settings	97
Accessories	41
Electrostatic Discharge	10
Installing	10
Activation Key	
AppLock	11, 306
ActiveSync	
Backup Data Files	146
Cables.....	145
Cold Boot and Loss of Host Re-connection.....	147
Connect cables	145
Connection, serial or USB	144
Disconnect, how to	147
Explore.....	145
Help.....	143
Initial installation	144
instruction	143
IR port transmission.....	83
partnership prerequisite.....	146
Setup Wizard.....	143, 144
Troubleshooting	148
ActiveSync Help.....	83
Adapters	
Avalanche	174
Add a certificate to the Root Store	280
Admin Hotkey	
AppLock	298, 301, 354, 356
Administration	
AppLock	97
Administrator	
Summit client utility.....	211
Align	
touchscreen	21
Allow Close	305
Allow PC Connection.....	122
Alpha Mode LED	62
Alphanumeric 32-key keypad.....	59

Alt key function	63
ANSI Keypad	58
Antenna	
Diversity.....	291
API calls	181
API Routines.....	76
Appearance options	110
Application Panel	301
AppLock	
End-user mode	298, 354
EUIE	305
Passwords.....	299, 355
Setup	295, 352
AppLock Administrator.....	78
AppLock panels.....	297
AppLock Registry settings	369
ASCII Control Codes in hex.....	371
Asian fonts.....	115
Assemble	
AC Power Adapter.....	15
Headset and microphone.....	17
Printer connection	17
RS232 connection	16
USB connection	16
assign key sequences to Diamond keys	116
Audible verification signals	49
Audio Cable	
Install	17
audio codecs	49
Audio headset interface	48
Audio support	49
Audio Volume settings	23
Audio/Microphone Connector.....	348
Auto hide	92
Auto-reconnect, Bluetooth.....	105
Autorun files at startup	82
Avalanche Enabler installation	162
Avalanche update settings	167

B

Background and Window colors	109, 110
Backlight display timer.....	22
Backlight properties.....	110
Backlight timers.....	110
Backup Battery	
Nickel Cadmium	47
Time Limit	68
Backup Data Files.....	146

Backup software77
Barcode
 Enable or Disable189
Barcode – Symbology Settings192
Barcode Data Match list195
Barcode processing overview185
Barcode Tab189
Batteries348
battery
 trickle charging13
Battery
 Backup, details69
 charge before using13
 Charge or Discharge buttons for backup battery
 maintenance98
 Charger70
 Charging47
 Check status and power reading13
 Compartment13
 Critical Suspend state68
 Hotswapping68
 Important3
 Life Approximate67
 Lithium-Ion (Li-ion)67
 Lithium-Ion (Li-Ion)47
 Low or Very Low68
 Low Warning timing67
 Main67
 Main Battery Pack, details67
 Publication69
 Safety69
 status67
 status LED13
Battery Auto Turn Off110
Battery Power Scheme22
Battery voltage and status display98
Baud Rate125, 183
Bluetooth
 barcode reader setup33
 devices32
 Initial Use29
 LX EZ Pairing specification51
 Options30
 Subsequent Use31
Bluetooth control panel99
Bluetooth Device Specifications350
Bluetooth Properties panel102
Bluetooth Scanners and Printers39
Bluetooth Settings, Chart103
Boot loader, responsibility77

C

CAB files151
CAB Files on the Flash Card142

Cable
 Adapter, Audio8
 Multipurpose RS-232 and Power8
 Multipurpose USB and Power8
 RS232 PC port to D9 male8
Cables44
Calibrate touchscreen21
Calibration137
CapsLock
 Configuring155
CapsLock mode function65
CCX Support290
Certificates106
 Root CA277
 User281
Change the Time and Date10
Change the volume setting23
Character Recognition
 Touchscreen91
Charger
 battery70
Charging Battery
 Time Required47
Check battery status67
Clean display and aperture66
Clear Contents of Document Folder93
Clear Internet cache112
Clear registry settings181
Client
 and Network Setup25
Client ports47
Code Enable133
Code ID, Enable191
Code IDs200
Cold Storage73
Coldboot40
COLDBOOT.EXE52, 156
COM Ports125, 183
 Configurations48
COM1 port settings188
Command Prompt87
Components5
Computer Friendly Name104
Config tab
 Summit212
Configuration
 Single User AppLock356
Connect
 ActiveSync83
 LX EConnect85
 Remote Display84
Connect External PS15
Connect Using122
Connection
 Avalanche168
Contact LX E41

Continuous Scan Mode.....	190
Control Char mapping	190
Control characters.....	131, 198
Control Panel	
Single User AppLock.....	357
Control Panel options	94
Controls, Physical	52
Copyrights	140
Core Logic	45
CPU	347
CPU Xscale.....	45
Cradle Accessories	44
Create a dialup, direct, or VPN connection	119
Create Connection option	119
Ctrl Char Mapping.....	198
Ctrl key function.....	63, 64
Cumulative mode timers	123
Current Time.....	107
Custom identifier	190
Custom Identifiers	200
Custom Key Mapping.....	322
Custom Parameter Option.....	220
Customize dates, times, currency	124

D

Data Bits	125, 183
Data entry	
imager	38
keypad.....	36
laser scanner.....	38
stylus	37
virtual keyboard	36
Data entry	36
Data Loss	
Cold Reset.....	10
Date and Time default settings	107
Daylight Savings.....	107
Decimal - Hexadecimal Equivalent	
0 - 159	375
160 - 255	376
DEFAULT.KEY.....	323
Desktop.....	80
Device Name and description	140
Diaqs tab	
Summit.....	218
Dialing properties	108
Diamond keys	60
Digital certificates.....	106
Dimensions	348
Disable Odyssey Client.....	89
Disable Summit Client.....	90
Discharged, recharged and conditioned.....	69
Discover and Query	100
Display.....	347

Avalanche	172
Features.....	66
Pixels.....	66
Specifications.....	348
Display Backlight Timer.....	66
display owner notes	21
Display properties.....	109
Display Timer	66
display timer expires	22
Dome switch	70
Double-click sensitivity for stylus taps.....	118
Download a root certificate	277
Dynamic Save Mode.....	291

E

EAP-FAST Authentication, Summit	233
Edit Diamond key parameters.....	60
electrostatic discharge.....	10
Enable Code ID	191
Enable Code ID drop-down box	189
Enable Internal Scanner sound	187
Enable or Disable specific symbology.....	189
Enabler	
communication.....	165
Network adapter status, link speed	177
Enabler Configuration	162, 165
Enabler installation	162
Enabler passwords	166
Enabler Uninstall Process	162
End user switching	
Touch	300
Entering Data.....	36
Environmental Specifications	349
Error Messages	
AppLock	361
EUIE	305
Example	
Barcode processing	202
Control Code Replacement	201
Execution	
Avalanche	169
Expand Control Panel.....	93
eXpress Config	
and Wavelink Avalanche	180
External Auto Turn Off	110
External Connector/Interface.....	347
External modem	
not supported.....	76
External PS	15

F

Factory Default, reset registry to	181
--	-----

Features	
MX7	1, 2
Field Exit key function	64
Flash	347
Flash and Reflash.....	182
Folders copied at startup.....	78
Fonts and keymaps	115
Forms entry.....	36
FTP server	86
Function	
2 nd Key	64
Alt Key.....	63
CapsLock Mode	65
Ctrl Key.....	63
Field Exit Key	64
Shift Key	63

G

General system parameter.....	138
Getting Help	41
Getting Started.....	10
Getting the Most from Your Batteries	69
Global Settings tab	
Summit.....	219
Glossary	41
Good scan Bad scan.....	187
GrabTime utility	154

H

Handle, How to.....	12
Handling Batteries	69
Handstrap, Install.....	14
Hardware	
Configuration	45
Hat Encoding and RFID	373
Help	41
Hexadecimal - Decimal Equivalent	
0x00 to 0x9F	375
0xA0 to 0xFF.....	376
HKEY_LOCAL_MACHINE	96
Hotkey	
Single User AppLock.....	358
Hotswapping	
allowed for Main Battery	68
hotswapping not allowed	
flash cards	54
network card	47
scanners.....	50
HyperTerminal	
ActiveSync	149

I

Icons	
Desktop	80
Idle Time.....	110
IEC IP54	349
IEEE 802.11g Wireless LAN Configuration	
Utility.....	290
Imager Aperture, clear	7
Inbox	
Outlook	87
Input panel	
virtual keyboard	36
Input Panel properties.....	111
Install ActiveSync on Desktop or Laptop.....	144
Install MX7 LXEbook	24
Integrated barcode scanner port.....	50
Internal modems	
not supported by LXE.....	108
Internal SD flash card and port.....	53
Internet connectivity	112
Internet Explorer.....	87
AppLock	305
Network card and ISP required.....	87
Single User AppLock.....	357
Internet popup blocker.....	112
Internet privacy	112
Internet Security	112
IO Components	45
IPv6 configuration	155

J

Java Option	76
JEM-CE	78

K

key repeat delay and rate	114
Keyboard	
Onscreen only	111
KEYCOMP compiler.....	370
KEYCOMP.EXE.....	322
Keymap	
32-key Keymap	317
5250 key functions.....	316
55-key	311
Keypad	
and entering data	36
Keypads	
Shortcuts	20

L

Launch APP and Launch CMD	155
LAUNCH.EXE	150
LCD	
Multi-charger	71
LCD Messages	71
LED	
Alpha mode	62
Battery Status	67
Multi-charger	71
Scan status	62
System status	62
LED Functions	71
Length Based Barcode Stripping	203
Levels, Logging	
Single User AppLock	359
Li-Ion battery life	13
List of configured ActiveSync connections	122
Logging	
AppLock	308
Login Utility	157
Loss of Host Re-connection	147
Low Battery Warning	68
LXE Login Utility	157
LXE Manuals CD	41
LXE Security Primer	207
LXE ServicePass	41
LXEbook – MX7 Users Guide	24
LXEConnect	85

M

MAC address	96
Main	125, 183
Main Battery Pack	47
Main tab	
Summit	210
Mappable Diamond Keys	60
Mass Storage	347
Match list	195
Match list rules	196
Media Player	88
Memory	347
allocate for programs or storage	139
Memory installed	138
Memory system parameter	138
Menu Options	
Start	82
Microphone adjustment	18
Microsoft File Viewers and password protected	
files	82
Mixer record gain	117
mode	
Block	129, 130

Key Message	129, 130
Mode	
Off	56
On	56
Suspend	56
Mode Key Functions	65
Modes	
AppLock	298, 354
MX7 Cold Storage	73
MX7 hand held device	50, 183
MX7 Multi-charger	
described	70
MX7 Options tab	150
My Certificates	27
My Device	
Folders	81

N

Network Device Specifications	350
Network driver properties	119
Network Profile	
Avalanche	175, 176
No Security	
Summit	229

O

Odyssey	
Client Icon	243, 292
Commands	244
Configured and authenticated	270
Connect the MX7 to the AP	274
EAP/TLS protocol	266, 269
EAP-LEAP protocol	264
EAP-MS-CHAP-V2	256
Help	245
Installing User Certificate	266
LXE Login Utility	157
No Encryption	247
password for the private key	267
PEAP/MS-CHAP protocol	255
PEAP-GTC protocol	259
Private Key	268
Server authentication	258, 263
Server certificate validation	272
Set WEP	246
Set WPA	253
Settings	243
Signal, Authentication, Encryption	271
Sim Card Manager	245
startup	25
Tools	245
Trusted Server configuration	275

Unmask client password	261
User Certificate, installing	266
Validate the server side certificates.....	275
WEP Authentication for LEAP.....	251
WEP Encryption	248
WPA/PSK configuration.....	273
Odyssey Client.....	89
Disable for Enabler	176
Odyssey Client Configuration	243, 292
Off Mode	56
ON Mode characteristics	56
Operating Temperature	
MX7.....	349
US AC to DC	349
Optional	
Software	78
Optional Software	
RFTerm.....	78
WaveLink Avalanche Enabler	79
Orange and Blue keys.....	64
Owner	
Identification	120
Network ID and password	120
Notes	120
Owner information	21

P

Parity.....	125, 183
Password.....	121
AppLock	299, 355
AppLock Save As	308, 360
At Power On	121
Single User AppLock.....	358
Summit Admin mode	211
Passwords lost at cold boot.....	156
PC Card	
Storage	54
PEAP-MSCHAP for WPA	235
Pen Stylus	20
Pen Stylus and data entry.....	37
Pen Stylus Pressure limit	66
Permanent storage of drivers and utilities.....	142
Phase 2 authentication	255
Physical Specifications	347
Pin 9 power unavailable	125, 183
Pistol Grip Handle, How To	12
Place in Suspend Mode.....	19
Port and cables.....	8
Power key	52
Power key location	19
Power Mode Properties	123
Power Modes	56
Power Modes diagram	55
Power Off	

schemes.....	22
Power Port 1 while asleep	126, 186
Power Save mode	291
Power Supply	
Battery Pack.....	47
Prefix and Suffix.....	129
Prefix and Suffix Control	197
Pre-loaded Files	76
Private key	28
Processor speed.....	45
processor type	138
Programmable Keys.....	60
Prompt	
Command	87
Proprietary boot loader	77
Protective Film.....	24
Putting it all together	12

Q

Quick Start Instructions	10
--------------------------------	----

R

Radio Config Utility	89
Reboot.....	52
Recalibration.....	137
Reflash the Mobile Device	182
Reflash, How To.....	182
REGEDIT.EXE	154
Regional settings, defaults	124
Registry and save settings.....	40
Registry content	
back up location	142
Registry settings	
AppLock	369
REGLOAD.EXE	154
Remote Display	84
Remove a program.....	124
Request the user certificate	281
Reset warm and reset cold	52
Review System and mobile device data and	
revision levels.....	138
RFTerm.....	25, 78
Roaming, WiFi	291
Root CA Certificates	
Downloading.....	277
Installing on mobile device	279
RS-232 and Power port.....	48
RSSI Reading Interval	290
RSSI Threshold.....	290

S

- Save settings40
- Save&Exit buttons291
- Scan
 - Good and Bad Scan sounds141
- Scan Aperture, red or clear7
- Scan Status LED62
- SCANBAD.WAV141
- SCANGOOD.WAV141
- Scanner
 - Main tab127, 187
 - Port.....187
 - Send Key Messages187
 - WEDGE187
- Scanner Control Characters Tab131, 198
- Scanner engine type348
- Scanner, factory defaults125, 183
- Scanning and data entry38
- Scanning status, LED39
- Schemes tab123
- Screwdriver
 - Phillips, for handstrap14
- SCU (Summit Client Utility)208
- SD card interface46
- SD Cards
 - Install and remove.....54
- SD flash card location.....53
- SD Flash Cards, CAB Files and Programs142
- SE824, SE955, SE152450, 183
- Second key function, described64
- Security options, supported207
- Security Panel
 - AppLock306
- Security Single User AppLock358
- Select a font114
- Select a key map114
- Send Key Messages and Wedge126, 186, 187
- Serial cables for serial port8
- Server contact
 - Avalanche170
- Set Owner information21
- Set time zone21
- Settings Menu
 - Status tab.....177
- Setup
 - AppLock295, 352
- Setup Software.....75
- Shift key function63
- Shortcuts
 - Avalanche173
 - Show Clock92
 - Shutdown time limits.....68
 - Single Application AppLock356
 - Soft Keyboard.....111
- Software
 - and Files76
 - Applications77
 - Folders copied at startup78
 - Load76
 - supported by the MX776
- Sounds and Volume default values.....141
- speaker49
- Speaker location23
- Special functions.....63
- SSID214
- Standard keys
 - functions.....63
- Start Menu
 - Shutdown80
- Start Menu, described82
- Startup and shutdown
 - Avalanche171
- Static screen protector.....66
- Static WEP Keys249
- Status
 - Avalanche177
 - Single User AppLock.....359
- Status Panel
 - AppLock307
- Status tab
 - Summit217
- Stereo and mono settings for headsets.....117
- Stop Bits125, 183
- Stop the Enabler Service.....163
- Storage Temperature
 - MX7349
 - US AC to DC349
- Stored certificates106
- Storing PC Cards54
- Strip Leading and Trailing Control.....194
- Strip Leading, Strip Trailing.....129
- Stylus20
- Stylus and data entry.....37
- Stylus pressure.....66
- Stylus sensitivity.....137
- Stylus, How to20
- Suffix and Prefix.....129
- Summit
 - Client configuration208
 - EAP-FAST Authentication233
 - LEAP without WPA Authentication.....231
 - No Security229
 - PEAP GTC Authentication239, 241
 - PEAP MSCHAP Authentication.....235
 - startup.....25
 - WEP keys.....230
 - WPA LEAP Authentication.....237
 - WPA PSK Authentication.....238
- Summit Client90
- Summit Client Utility (SCU)208

Suspend	
and the LXE Login Utility	158
Suspend button	80
Suspend mode	56
Suspend mode and ActiveSync	52
Switch applications	
Multi AppLock	11
Symbology	192
strip leading strip trailing	194
Symbology settings	190
System Configuration	75
System Hardware Configuration	45
System Memory	46
System Status LED	62

T

Taskbar defaults	92
Technical specifications	
bootloader	77
version control	77
Technical Specifications	347
Terminal Emulation parameters	25
Tethered scanners	39, 44
Three keypads	57
Tile	109, 110
Time Zone	107
Timer	
battery power timer	22
cumulative effect	22
external power timer	22
Touch Screen and data entry	37
Touchscreen	66
adjustment	21
Keypad Shortcuts	20
Touchscreen, stylus tap	20
Transcriber	91
Translate All	131, 198
Translate control codes	131, 198
Transmissive Display	66
Troubleshooting	
ActiveSync	148
AppLock	11
AppLock Password	299, 355
Coldboot	156
Login utility	11
Multi-Application AppLock	309
Password, screensaver	121
RFTerm	11
Startup	11
turbo mode switching	45

U

Uninstall a program	124
Update monitoring	163
USB Client and Power port	48
User access	
power up password	121
user certificate and a separate private key file	281
User Certificate on the MX7	286
User Certificates	
Generating	281
User certificates and private keys	26
User-specific application version information	96
Utilities	
Coldboot	156
Launch	150
MX7 Options tab	150
Regedit	154
Regload	154
Warmboot	154
WavPlay	154

V

Version control	77
Version window information	96
Vibration	187, 205
Good scan and bad scan	187
Video Subsystem	46
View	
Display	66
Virtual keyboard	
Input panel	36
Virtual Keyboard	111
VK_Code List	370
Voice	
Accessories	41
Voice data	39
Voice data entry and the microphone	18
Volume	
adjust audio volume	23
using the keypad	23
Volume and Sounds default values	141
Volume control	49
Volume Mixer	117

W

Wake the device from Suspend	80
Wake up action for display backlight	56
Warm Reset	52
Warmboot	40
WARMBOOT.EXE	52, 154
Warning	

Low Battery	68	Wireless LAN Configuration Utility	290
Warnings and Labels		Wireless Network Configuration	207
Laser Scanner	38	Wireless Security	
Wavelink Avalanche Enabler installation	162	Summit Client	225
WAVPLAY.EXE	154	Wireless Zero Config Utility	89, 90
Wedge	126, 186, 187	Odyssey Client	292
Weights	347	Summit Client	293
When to use this guide	3	WLAN Networks	25
WiFi icon	89, 290	WLAN Profiles	25
Windows CE on-line Help	75, 154	WordPad	88
Windows Explorer	91	Writing new bootloader	182
Windows OS version	138	WZC icon	89, 90, 292, 293
Wireless communication	72		

