

MX5X Reference Guide

(Microsoft® Windows® CE .NET 4.2 / CE 5.0 Equipped)



Copyright © 2007 by LXE Inc.
All Rights Reserved
E-EQ-MX5CERG-D



Notices

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

Copyright:

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

Copyright © 2007 by LXE Inc. An EMS Technologies Company.

125 Technology Parkway, Norcross, GA 30092 U.S.A. (770) 447-4224

Trademarks:

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

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

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.

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

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

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

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.

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

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

Note: The original equipment's User Manuals are copyrighted by Itronix® Corporation. This manual has been amended by LXE® Inc., for the MX5X and MX5 Cradles with permission from Itronix Corporation.



Inspect enclosure for signs of deterioration such as cracking, warping, swelling or softening. Do not use in Hazardous (Classified) Locations if there are any signs of deterioration.



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

Notices	Added PowerScan registered trademark information.
Chapter 1 – Introduction	Added “MX5X Features.” Added “Upgrading an MX5X to CE 5.0.” Updated AppLock application switching instruction to include AppLock Launch function. Updated Accessories.
Chapter 3 – System Configuration	Added Windows CE 5.0 information or instruction where applicable.
Chapter 5 – Wireless Network Configuration	Added EAP-FAST and EAP-TLS instruction. Updated Summit Client Utility to reflect version differences.
Chapter 6 - AppLock	Added AppLock Launch function. Moved AppLock Single Application Version section to Appendix C – Reference Material
Appendix C – Reference Material	New.
Entire Manual	Changed Reference Guide title to MX5X Reference Guide . Changed name of device to MX5X where applicable. DocID did not change.



Table of Contents

CHAPTER 1 INTRODUCTION	1
Overview	1
Important Battery Information	2
Li-Ion Battery	2
When to Use This Guide	2
Document Conventions	3
Identify Your Device	4
MX5X Features	5
Upgrading an MX5X to CE 5.0	6
MX5X Hazardous Location Device	7
Getting Started	8
Windows CE .NET 4.2	8
Windows CE 5.0	8
Troubleshooting Start-up	9
Setup the Client and Network	9
Access Terminal Emulation Parameters	10
Saving Settings	10
Components	11
Power Key	14
Assembly	15
Insert Main Battery	15
About Lithium-Ion Batteries	15
Connect External Power Supply (Optional)	16
Install Pistol Grip Handle (Optional)	17
Install Handstrap	18
How To	20
Tap the Touchscreen with a Stylus	20
Keypad Shortcuts	20
Calibrate the Touchscreen	20
Set Time Zone (Optional)	21
Enter Owner Information (Optional)	21
Set the Display and Keypad Backlight Timers	21
Set the MX5X Power Schemes Timers	22
Toggle the Display and Keypad Backlight On and Off	22
Increase or Decrease Keypad and Display Backlight Intensity	22
Connect Audio Jack (Optional)	22
Set The Audio Speaker Volume	23
Troubleshooting Volume Adjust	23
Enter the Multi AppLock Activation Key	24
Using a Stylus Tap	24
Using the Switch Key Sequence	24
Copy the MX5X LX Ebook to the MX5X (Optional)	25
Enter Data	26
Keypad Entry	26
Stylus Data Entry	26
Scanner Entry	27
Data Entry and Tethered Scanners	27
Input Panel	28

RS-232 Data Entry	28
Getting Help.....	29
Manuals.....	29
Accessories.....	30
MX5X Standard.....	30
MX5X ISAFE Device	31
CHAPTER 2 PHYSICAL DESCRIPTION AND LAYOUT	33
Hardware Configuration	33
System Hardware	33
Central Processing Unit.....	33
Core Logic.....	33
System Memory	34
Video Subsystem.....	34
Power Supply	34
COM Ports	35
Audio Interface	35
Power Key.....	36
Reboot Sequence.....	36
Warm Reset.....	36
Cold Reset.....	36
PCMCIA and Flash Cards.....	37
Installation / Removal	38
PCMCIA Cards	38
Flash Cards	38
Accessing the Data on CF and PCMCIA Cards.....	39
ATA CF Card.....	39
Hatch CF Card.....	39
Hatch PCMCIA Card	39
COM Ports	40
USB Port	40
Integrated Scanner Port (Optional)	41
Tethered Scanners (Optional)	41
Data Entry and Tethered Scanners	42
RS-232 Serial Ports.....	42
COM1.....	42
COM4.....	42
USB Port.....	43
IR Port.....	43
Programmable Buttons	44
Power Modes	45
On Mode	45
The Display	45
The MX5X.....	45
LED Indicators	46
Suspend Mode.....	46
The MX5X.....	46
Off Mode.....	46
The Keypad.....	47
Scan Key Function	47
Enter Key Function	47
2 nd Key Function	48

Ctrl Key Function.....	48
Alt Key Function.....	48
Shft Key Function	48
Spc Key Function.....	48
Field Exit Function.....	48
Mode Key Functions.....	49
Caps Key and CapsLock Mode.....	49
Keypress Sequences.....	49
Input Panel	49
Accessing Files on the Compact Flash Card.....	50
Touchscreen.....	50
Display and Keypad Backlight Timer.....	50
Cleaning the Glass Display/Scanner Aperture	51
Speaker	51
Set The Audio / Speaker Volume.....	52
Using the Keypad	52
Using the Touch Screen.....	52
Troubleshooting	52
Power Supply	53
Checking Battery Status.....	53
Important Battery Information.....	53
Handling Batteries Safely	53
Main Battery Pack.....	54
Battery Hot-Swapping.....	54
Low Battery Warning.....	55
Battery Status LEDs.....	55
Backup Battery.....	55
Battery Maintenance Publication.....	55
Battery Chargers.....	56
MX5 Multi-Charger (Optional).....	56
External Power Supply for MX5X and Cradle	57
Cradles.....	58
Tethered Barcode Scanner Data Entry Using the MX5 Cradle.....	59
CHAPTER 3 SYSTEM CONFIGURATION	61
Introduction	61
Windows Operating System	61
2.4 GHz Network Configuration.....	61
Installed Software	61
Software Load.....	62
Software Applications.....	62
Optional.....	62
AppLock (Option).....	62
JAVA (Option).....	63
LXE RFTerm (Option).....	63
Wavelink Avalanche Enabler (Option).....	63
Desktop.....	64
My Computer Folders (CE .NET 4.2).....	65
Folders Copied at Startup	65
My Device Folders (CE 5.0)	66
Start Menu Program Options	67
Communication	67

ActiveSync	68
Synchronizing from the MX5X	68
Get Connected	68
Remote Desktop Connection	69
Command Prompt	69
Inbox	69
Internet Explorer	69
Media Player	70
Windows Explorer	70
Transcriber	70
Taskbar	71
Advanced Tab	71
Expand Control Panel	71
Clear Contents of Document Folder	71
Control Panel Options	72
Accessibility	73
Administration – for AppLock	74
Audio	75
Certificates	76
Date/Time	77
Dialing	78
Display	79
Display Properties	79
Background	79
Backlight	79
Handheld	80
How to Disable Touch and / or Calibration upon Cold Reset	80
Disable Touch Panel and Calibration	80
Disable Touch Panel Only	80
How to Re-enable Touch and / or Calibration upon Cold Reset	80
Bootloader Version 1.02	81
Versions tab	81
Comms tab	81
Radios tab	82
Misc tab	82
Bootloader Version 1.01	83
Versions tab	83
Comms tab	83
Radios tab	83
Misc tab	83
Input Panel	84
Internet Options	85
Windows CE .NET 4.2 Defaults	85
Windows CE 5.0 Defaults	85
Keyboard	86
Mouse	87
Network and Dialup Connections	87
Create a Communication Option	87
Owner	88
Password	89
PC Connection	89
Power	91

Status	91
Battery	91
Schemes	91
Regional Settings	92
Remove Programs	92
Scanner	93
Determine Your Scanner Software Version	93
Factory Default Settings	94
Main	95
Keys	96
Change a Virtual Key (F20 or F21) Value	96
Advanced	97
Translate Control Codes	97
Strip Leading / Strip Trailing Characters	97
Prefix / Suffix	98
COM Ports	99
Good Scan and Bad Scan Sounds	99
Storage Manager	100
Stylus	101
Double Tap	101
Calibration	101
System	102
General	102
Memory	102
Device Name	103
Copyrights	103
Compact Flash Cards, CAB Files and Programs	104
Access Files on the CF Card	104
CF Files	104
Bluetooth Manager (CE .NET 4.2 only)	105
API Calls	105
ActiveSync / Get Connected Process	106
Introduction	106
Initial Install	107
Install ActiveSync on Desktop/Laptop	107
Serial Connection	107
USB Connection	107
Connect – Initial Install Process	108
Change Connection Parameters	108
Backup MX5X Files Using ActiveSync	109
Prerequisites	109
MX5X and PC Partnership	109
Serial Port Transfer	109
Infrared Port Transfer	109
USB Transfer	109
Ethernet Transfer	109
Connect	109
Ethernet or Wireless Connection	110
Explore	110
Disconnect	110
Serial Connection	110
IRDA Connection	110

USB Connection	110
Wireless Device Connection	110
Ethernet Connection	110
Cold Boot and Loss of Host Re-connection	111
Troubleshooting ActiveSync	111
iRescue	113
Start iRescue	113
Backup Your Mobile Device using iRescue	113
Change Backup Settings	114
Manage Backups	114
Restore Backups	114
Wavelink Avalanche Enabler Configuration	115
Briefly	115
Enabler Install Process	115
Enabler Uninstall Process	115
Stop the Enabler Service	116
Update Monitoring Overview	116
Mobile Device Wireless and Network Settings	117
Enabler Configuration	118
File Menu Options	119
Avalanche Update Settings	120
Menu Options	120
Connection	121
Execution	122
Server Contact	123
Startup/Shutdown	124
Scan Config	125
Display	125
Shortcuts	126
Adapters	127
Status	130
Troubleshooting Avalanche Enabler	130

CHAPTER 4 SCANNER **131**

Introduction	131
Determine Your Scanner Software Version	131
Barcode Processing Overview	132
Factory Default Settings	133
Main Tab	134
Parameters	134
Good Scan and Bad Scan Sounds	135
Keys Tab	135
Change a Virtual Key (F20 or F21) Value	136
COM1/COM4 Tab	137
Barcode Tab	138
Buttons	138
Enable Code ID	139
Options	139
Barcode – Symbology Settings	140
Parameters	141
Strip Leading/Trailing Control	142
Barcode Data Match List	143

Barcode Data Edit Buttons.....	143
Match List Rules	144
Add Prefix/Suffix Control.....	145
Barcode – Ctrl Char Mapping	146
Translate All.....	146
Barcode – Custom Identifiers.....	148
Parameters	148
Buttons.....	149
Control Code Replacement Examples.....	149
Barcode Processing Examples	150

CHAPTER 5 WIRELESS NETWORK CONFIGURATION 153

Introduction	153
Summit Client Configuration	154
Summit Client Utility.....	154
Help.....	154
Summit Tray Icon	155
Wireless Zero Config Utility and the Summit Client	155
Main Tab.....	156
Admin Login	157
Config or Profile Tab	158
Buttons.....	158
Config/Profile Parameters	160
Status Tab.....	162
Diags Tab	163
Buttons.....	163
Global or Global Settings Tab.....	164
Factory Default Settings.....	164
Global Parameters	165
Summit Wireless Security.....	168
Sign-On vs. Stored Credentials	169
Windows Certificate Store vs. Certs Path	171
User Certificates	171
Root CA Certificates.....	171
No Security	172
WEP Keys	173
LEAP w/o WPA Authentication.....	174
EAP-FAST Authentication.....	175
PEAP/MSCHAP Authentication	177
WPA/LEAP Authentication	179
WPA PSK Authentication	180
PEAP/GTC Authentication	181
EAP-TLS Authentication	183
Cisco Client Configuration.....	185
Aironet Client Utility (ACU).....	185
Profiles Tab	185
Firmware Tab	185
Status Tab	185
Statistics Tab	185
Survey Tab.....	186
Cisco Wireless Security	186

System Requirements	186
Installing Cisco Wireless Client Drivers	186
Checking for the Cisco PEAP Supplicant	187
Cisco WPA Configuration.....	188
PEAP/MS-CHAP Authentication Configuration	191
Configuring the PEAP/MS-CHAP Supplicant	191
Server Authentication	193
PEAP / GTC Authentication Configuration	194
Configuring the PEAP/GTC Supplicant	194
Server Authentication	196
WPA/LEAP	197
Cisco ACU.....	197
EAP-TLS Authentication Configuration	199
User Certificate	199
Setting EAP/TLS Parameters.....	200
Validating the Server Certificate	202
WPA PSK Configuration	203
Symbol Client	204
IP Information Tab	204
IPv6 Information Tab.....	204
Configuring IPv6.....	204
Wireless Information Tab	204
View Log.....	205
Add a new connection	205
Disable WEP.....	205
Enable WEP.....	205
Continue.....	205
Select a User Certificate	205
Certificates	206
Root Certificates	206
Download a Root CA Certificate.....	206
Installing a Root CA Certificate on the Mobile Device	208
User Certificates.....	210
Generating a User Certificate for the MX5X	210
Installing a User Certificate on the MX5X (WPA-TLS Only).....	215
CHAPTER 6 APPLOCK	219
Introduction	219
Determine Your AppLock Version	219
Setup a New Device	220
Administration Mode	222
End User Mode.....	222
Passwords	223
AppLock Password Troubleshooting	223
End-User Switching Technique	224
Using a Stylus Tap	224
Using the Switch Key Sequence	224
Multi-Application Configuration	225
Application Panel	225
Launch Button	227
Auto At Boot	227
Auto Re-Launch	228

Manual (Launch).....	228
Allow Close.....	229
End User Internet Explorer (EUIE)	229
Security Panel.....	230
Setting an Activation Hotkey.....	230
Setting a Password in the Security Panel	231
Status Panel	231
View.....	231
Log.....	232
Save As	232
Troubleshooting AppLock	233
APPENDIX A KEY MAPS	235
Keypad	235
Key Map 101-Key Equivalencies	236
IBM Keypad Overlays	240
3270 Keypad	240
5250 Keypad	242
APPENDIX B TECHNICAL SPECIFICATIONS	243
Physical Specifications	243
Display Specifications	244
Environmental Specifications	244
MX5X	244
AC Wall Adapter	244
Network Card Specifications	245
Summit Client 2.4GHz Type II.....	245
Symbol Client 2.4GHz Type II	245
Cisco Client 2.4GHz Type II	245
APPENDIX C REFERENCE MATERIAL	247
Introduction	247
AppLock - Single Application Configuration	248
Determine Your AppLock Version.....	248
Setup a New Device.....	249
Administration Mode	249
End User Mode	250
Passwords.....	250
Password Troubleshooting	250
Single Application Configuration	251
Administrator Control Panels.....	251
Control Panel.....	252
End User Internet Explorer.....	252
Security Panel	253
Specify a Hotkey Sequence	253
Setting a Password.....	253
Status Panel	254
View	254
Levels	255
Save As.....	255

AppLock Error Messages	256
AppLock Registry Settings	261
Valid VK Codes for CE	262
ASCII Control Codes	263
Hat Encoding	265
Decimal – Hexadecimal Chart	267
Revision History	269

INDEX**273****Illustrations**

Figure 1-1 Identify your Device.....	4
Figure 1-2 Features	5
Figure 1-3 Front of MX5X.....	11
Figure 1-4 Scan Aperture and Audio Jack	11
Figure 1-5 Ports.....	12
Figure 1-6 Back w/Optional Handle or Hand Strap	12
Figure 1-7 Handle (Optional).....	13
Figure 1-8 Power Key Location.....	14
Figure 1-9 Main Battery Pack.....	15
Figure 1-10 AC/DC 12V External Power Supply	16
Figure 1-11 Battery Charging LED.....	16
Figure 1-12 Trigger Handle Attach Points.....	17
Figure 1-13 MX5X With Handstrap Installed.....	18
Figure 1-14 Upper Strap Bracket.....	18
Figure 1-15 Strap Inserted in Upper Bracket	19
Figure 1-16 Connect Audio Jack.....	22
Figure 1-17 End-User Multi AppLock Touch Panel Segment.....	24
Figure 1-18 Scan Beam.....	27
Figure 1-19 Scanner LED Location	27
Figure 1-20 Input Panel.....	28
Figure 2-1 System Hardware	33
Figure 2-2 COM Ports – Left and Right	35
Figure 2-3 PCMCIA Wireless Client Card and Flash Card Location	37
Figure 2-4 COM Ports.....	40
Figure 2-5 RS-232 Ports	42
Figure 2-6 DB26 RS-232 Pinouts	42
Figure 2-7 MX5X USB Port	43
Figure 2-8 USB-Serial Cable Pinouts	43
Figure 2-9 IR Port on MX5X.....	43
Figure 2-10 Scan Buttons.....	44
Figure 2-11 Power Modes – On, Suspend and Off	45
Figure 2-12 The ANSI / Batch Keypad.....	47
Figure 2-13 Touchscreen	50
Figure 2-14 Speaker Location.....	51
Figure 2-15 LXE Multi-Charger	56
Figure 2-16 Insert Battery Pack in Charging Pocket.....	56
Figure 2-17 AC/DC 12V Power Supply	57
Figure 3-1 Desktop Icons.....	64
Figure 3-2 Pocket CMD Prompt Screen	69
Figure 3-3 Taskbar and Start Menu Properties	71
Figure 3-4 Accessibility Options	73

Figure 3-5 Audio Properties.....	75
Figure 3-6 Digital Certificates	76
Figure 3-7 Date/Time Properties.....	77
Figure 3-8 Dialing Properties.....	78
Figure 3-9 Display Properties	79
Figure 3-10 Handheld Properties – Version 1.02.....	81
Figure 3-11 Input Panel.....	84
Figure 3-12 Keyboard Properties	86
Figure 3-13 Owner Properties.....	88
Figure 3-14 PC Connection / Change Connection	90
Figure 3-15 Power Properties.....	91
Figure 3-16 Remove/Delete User Installed Programs.....	92
Figure 3-17 Determine Your Scanner Software Version	93
Figure 3-18 Scanner Properties / Main Tab	95
Figure 3-19 Scanner Properties / Keys Tab	96
Figure 3-20 Scanner Properties / Advanced tab.....	97
Figure 3-21 Scanner Properties / COM Port Settings	99
Figure 3-22 Storage Properties.....	100
Figure 3-23 Stylus Properties / Calibration Start / Calibration Begin	101
Figure 3-24 System / Memory	102
Figure 3-25 System / Device Name	103
Figure 3-26 iRescue Backup	113
Figure 3-27 Avalanche Enabler Opening Screen.....	118
Figure 3-28 Connection Options.....	121
Figure 3-29 Execution Options (Dimmed).....	122
Figure 3-30 Server Contact Options.....	123
Figure 3-31 Startup / Shutdown Options.....	124
Figure 3-32 Scan Config Option.....	125
Figure 3-33 Window Display Options	125
Figure 3-34 Application Shortcuts	126
Figure 3-35 Adapters Options – Network.....	127
Figure 3-36 Avalanche Network Profile Displayed.....	128
Figure 3-37 Manual Settings Properties Panels	129
Figure 3-38 Status Display.....	130
Figure 4-1 Scanner Control / Main	134
Figure 4-2 Scanner Properties / Keys Tab	135
Figure 4-3 Scanner Control / COM1 and COM4.....	137
Figure 4-4 Scanner Control / Barcode tab.....	138
Figure 4-5 Barcode Tab – Symbology Settings	140
Figure 4-6 Strip Leading / Trailing and Barcode Data.....	142
Figure 4-7 Barcode Data Match List.....	143
Figure 4-8 Add Prefix/Suffix Control	145
Figure 4-9 Barcode Tab – Ctrl Char Mapping	146
Figure 4-10 Barcode Tab – Custom Identifiers.....	148
Figure 4-11 Control Code Replacement Examples.....	150
Figure 4-12 Barcode Processing Examples.....	151
Figure 5-1 Summit Client Utility (SCU).....	154
Figure 5-2 SCU – Main Tab.....	156
Figure 5-3 Main Tab – Enter Admin Password	157
Figure 5-4 SCU – Config / ProfileTab	158
Figure 5-5 SCU - Scan	159
Figure 5-6 SCU – Status Tab	162
Figure 5-7 SCU – Diags Tab.....	163
Figure 5-8 SCU – Global /Global Settings Tab	164
Figure 5-9 Sign-On Screen	170
Figure 5-10 Choose Certificate	171
Figure 5-11 Configure a Summit Profile with No Security	172

Figure 5-12 Summit WEP Key Dialog	173
Figure 5-13 Configure a Summit Profile for LEAP w/o WPA	174
Figure 5-14 LEAP Credentials Dialog	174
Figure 5-15 Configure a Summit Profile for EAP-FAST	175
Figure 5-16 Summit EAP-FAST Credentials.....	176
Figure 5-17 Configure a Summit Profile for PEAP/MSCHAP.....	177
Figure 5-18 PEAP/MSCHAP Credentials Dialog.....	178
Figure 5-19 Configure a Summit Profile with LEAP for WPA TKIP	179
Figure 5-20 LEAP Credentials.....	179
Figure 5-21 Configure a Summit Profile with WPA PSK Encryption.....	180
Figure 5-22 Summit PSK Entry Dialog	180
Figure 5-23 Configure a Summit Profile with PEAP/GTC.....	181
Figure 5-24 PEAP/GTC Credentials Dialog.....	182
Figure 5-25 Configure a Summit Profile with EAP-TLS.....	183
Figure 5-26 EAP-TLS Credentials Dialog.....	184
Figure 5-27 Cisco PEAP Authentications.....	187
Figure 5-28 Cisco ACU Profile Selection.....	188
Figure 5-29 Cisco ACU Reboot Message.....	188
Figure 5-30 Cisco Wireless Information Screen	189
Figure 5-31 Cisco Advanced Wireless Settings.....	189
Figure 5-32 Cisco Wireless Network Properties.....	190
Figure 5-33 Cisco PEAP/MSCHAP Wireless Network Properties.....	191
Figure 5-34 Cisco Authentication Settings	191
Figure 5-35 Cisco Wireless Network Login	192
Figure 5-36 Cisco IP Information Tab	192
Figure 5-37 Cisco Authentication Settings, Validate Server.....	193
Figure 5-38 Cisco Advanced Wireless Settings, Authenticated SSID	193
Figure 5-39 Cisco PEAP/GTC Wireless Network Properties	194
Figure 5-40 Cisco Authentication Settings	194
Figure 5-41 Cisco Wireless Network Login	195
Figure 5-42 Cisco IP Information Tab	195
Figure 5-43 Cisco Authentication Settings, Validate Server.....	196
Figure 5-44 Cisco Advanced Wireless Settings, Authenticated SSID	196
Figure 5-45 Cisco Renaming Profile.....	197
Figure 5-46 Cisco Profile Properties Screen	198
Figure 5-47 Cisco Login Screen	198
Figure 5-48 Cisco Certificate Stores	199
Figure 5-49 Cisco EAP/TLS Configuration.....	200
Figure 5-50 Cisco Authentication Settings	200
Figure 5-51 Cisco Select Certificate	201
Figure 5-52 Cisco Authentication Settings, Certificate Details	201
Figure 5-53 Cisco Validate Server.....	202
Figure 5-54 Cisco SSID Authenticated.....	202
Figure 5-55 Logon to Certificate Authority	206
Figure 5-56 Certificate Services Welcome Screen.....	206
Figure 5-57 Download CA Certificate Screen.....	207
Figure 5-58 Download CA Certificate Save to Desktop.....	207
Figure 5-59 Certificate Stores	208
Figure 5-60 Import Certificate From a File.....	208
Figure 5-61 Browsing to Certificate Location	209
Figure 5-62 Logon to Certificate Authority	210
Figure 5-63 Certificate Services Welcome Screen.....	210
Figure 5-64 Request a Certificate Type	211
Figure 5-65 Advanced Certificate Request Screen	211
Figure 5-66 Advanced Certificate Details.....	212
Figure 5-67 Script Warnings.....	213
Figure 5-68 Script Warnings.....	213

Figure 5-69 User Certificate Issued	214
Figure 5-70 Download Certificate Security Warning	214
Figure 5-71 Certificate Stores	215
Figure 5-72 Import User Certificate.....	215
Figure 5-73 Browsing to Certificate Location	216
Figure 5-74 User Certificate Listing	216
Figure 5-75 Browsing to Private Key Location	217
Figure 6-1 Determine Your AppLock Version	219
Figure 6-2 AppLock Panels	221
Figure 6-3 Switchpad Menu.....	224
Figure 6-4 Application Panel – Multi-Application	225
Figure 6-5 Application Launch Options.....	227
Figure 6-6 Security Panel – Multi-Application.....	230
Figure 6-7 Status Panel – Multi-Application	231



Chapter 1 Introduction

Overview

Note: At the bottom of the MX5X is a label that indicates the operating system resident on the mobile device. This guide is directed toward an MX5X with Windows CE on the label.

The LXE® MX5X is a rugged, portable, hand-held Microsoft® Windows® CE .NET 4.2 or CE 5.0 equipped mobile computer capable of wireless data communications. The MX5X can transmit information using a 2.4 GHz wireless client (with dual internal antennas) and it can store information for later transmission using an RS-232 serial port, Ethernet, RF, IRDA or a USB port.

The MX5X is vertically oriented and features backlighting for the display and the keypad. The touch-screen display supports graphic features and icons that the Windows operating system supports. A stylus is attached to the MX5X to assist in entering data and configuring the unit.



The MX5X is powered by a 2800 mAh Lithium-Ion main battery pack and an internal backup battery.

MX5X Hazardous Location unit can be distinguished from the standard MX5X by the blue keypad overlay and the safety approval labeling on the back of the unit. The MX5X that is approved for use in Hazardous Locations does not accept tethered scanner or external power connection. See section titled *Identify Your Device*.

Warning: Standard MX5X units are not approved for Hazardous Location use.

Note: Until the main battery and backup battery are completely depleted, the MX5X is always drawing power from the batteries (On). This unit is to be used with a power supply (LXE P/N MX5A305PSACUS / MX5A305PSACWW).

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

Important Battery Information

Important: If the main battery has been out of the MX5X for an extended period of time or becomes fully discharged or dead, a fully charged backup battery in the MX5X will last for up to 24 hours. If this happens, the device will cold reset the next time power is applied from either AC power or a charged main battery. A cold reset will cause loss of data and custom programs. Always store unused mobile devices with a fully charged main battery pack installed. The MX5X requires periodic connection to an external power source to maintain an optimum backup battery charged status.

- Until the main battery and backup battery are completely depleted, the MX5X is always drawing power from the batteries (On).
- New batteries must be fully charged prior to use ¹.
- Whenever possible, use the AC power adapter with the MX5X to conserve the main battery and charge the backup battery.
- When a new battery is installed in the MX5X for the first time (or when the backup battery is completely depleted), the Time and Date reverts to its default values.

Li-Ion Battery

When disposing of the MX5X main battery, the following precautions should be observed: The battery should be disposed of properly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

When to Use This Guide

As the reference for LXE's MX5X 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 MX5X, 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 MX5X.

Daily operation, installation and safety instructions for the general user are covered in the *MX5X User's Guide*.

This chapter, **Introduction**, describes this reference guide's structure, contains initial setup instruction, MX5X assembly and use, briefly describes data entry processes, and explains how to get help.

Chapter 2 - Physical Description and Layout, describes the function and layout of the MX5X, controls and connectors. Also describes the power supplies and docking options for the MX5X.

Chapter 3 - System Configuration takes you through the Windows CE operating system setup and the MX5X file structure. The Avalanche Enabler is included.

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

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

Chapter 6 - AppLock covers all aspects of the LXE AppLock program.







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

Appendix B - Technical Specifications lists MX5X and optional device technical specifications.

¹ If the MX5 has a dead main battery and is as cold as the extended operating temperature's lowest value, the unit must be warmed to above -20°C (-4°F) before installing a new main battery pack and pressing the On button.

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/folders, 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 Italics	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.
Note:	Keyword that indicates immediately relevant information.
CAUTION 	Keyword that indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
WARNING 	Keyword that indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
DANGER 	Keyword that indicates a imminent hazardous situation which, if not avoided, will result in death or serious injury.

Identify Your Device

At the front bottom of the MX5X is a label indicating the operating system resident on the mobile device. This document is one in a series covering the MX5X family of computers:

	<p>Label : Windows CE .NET</p> <p>For MX5X computers equipped with Microsoft Windows CE .NET 4.2 or CE 5.0 Operating System :</p> <ul style="list-style-type: none"> • MX5X User's Guide • MX5X Reference Guide • LXEbook – MX5X User's Guide (can be downloaded to the MX5X device from the LXE Manuals CD.)
	<p>Label : I-SAFE</p> <p>For MX5X Intrinsic Safe (MX5-IS) computers equipped with Microsoft Windows CE .NET 4.2 or CE 5.0 Operating System:</p> <ul style="list-style-type: none"> • MX5X Intrinsic Safe User's Guide • MX5X Reference Guide • LXEbook – MX5X I-Safe User's Guide (can be downloaded to the MX5-IS device from the LXE Manuals CD.) <p>The MX5X Intrinsic Safe Hazardous Location unit (MX5-IS) is distinguished from the standard MX5X by the blue keypad overlay and the safety approval labeling on the back of the MX5-IS. Please refer to the <i>MX5X Intrinsic Safe User's Guide</i> for cautions, warnings, explanation and instruction when using the MX5-IS device.</p> <p><i>Warning: Standard MX5X units, powered cradles, tethered scanners, multichargers, headsets, belt battery system, USB devices and external power supplies are not approved for Hazardous Location use.</i></p>
	<p>Label : Pocket PC (Obsolete December 2005)</p> <p>For MX5 computers equipped with Microsoft Windows Pocket PC 2000/2002 operating Systems:</p> <ul style="list-style-type: none"> • MX5 PPC User's Guide • MX5 PPC Reference Guide • LXEbook – MX5 PPC User's Guide (can be downloaded to the MX5 Pocket PC device from the LXE ServicePass website.)

Figure 1-1 Identify your Device

The following manuals are interchangeable for MX5X computers (except where noted in the manuals):

- MX5 Cradle Reference Guide
- MX5 Multi-charger Reference Guide
- MX5 Belt Battery System (LXE suggests using this accessory specifically with a Low Temperature MX5X.)

Do not use the MX5 Belt Battery System with an MX5-IS in a hazardous location.

MX5X Features

New features affect user interaction and internal operation of the MX5X.

The appropriate wireless client utility for your device configuration has been pre-installed by LXE and the utility icon is displayed on the desktop.

	Windows CE .NET 4.2	Windows CE 5.0	Optional?
Summit® Client Utility	x	x	No
Aironet® Client Utility (Cisco)	x	-	No
Symbol® Client Utility	x	-	No
MX5X I-SAFE	x	x	Yes
SE1223 Integrated Laser Scanner	x	x	Yes
SE1224 Integrated Laser Scanner	x	x	Yes
SE2223 Integrated Laser Scanner	x	x	Yes
400MHz	x	x	No
64MB RAM	x	x	No
Type I/II Compact Flash slot	x	x	No
ATA Compact Flash slot	x	x	No
Charging/Communication Cradles	x	x	Yes
Wavelink® Avalanche® Enabler	-	x	Yes
RFTerm®	x	x	Yes
JAVA®	x	x	Yes
Single AppLock	x	-	Yes
Multi AppLock	x	x	Yes

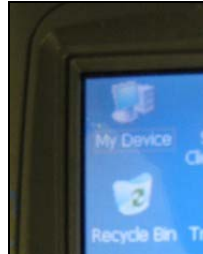
Figure 1-2 Features

Upgrading an MX5X to CE 5.0

Microsoft CE 5.0 Licenses must be purchased from LXE and applied to each upgraded device. The mobile device cannot be upgraded to CE 5.0 using the Wavelink / eXpress Config application.

Note: The MX5X operating system cannot be upgraded using Wavelink Avalanche.

If your (3.6 inch / 9.1 cm diagonal) MX5 touch screen border looks like this:



It can be upgraded to Windows CE 5.0.

If your (3.8 inch / 9.6 cm diagonal) MX5X touch screen border looks like this:



The device must be returned to LXE for upgrading to CE 5.0, or an LXE Field Service Engineer can be dispatched to upgrade the hardware and software. Contact your LXE representative for assistance.


MX5X Hazardous Location Device

Label : I-SAFE


Environmental Specifications







Operating Temperature	-6°F to 140°F (-21°C to 60°C) [non-condensing]
Storage Temperature	-60°F to 160°F (-51°C to 71°C) [non-condensing]
Rating	IEC IP67
Operating Humidity	5% to 90% non-condensing at 140°F (60°C)
Vibration	Based on MIL Std 810F

Read Before Use

 DO NOT USE THIS UNIT IN CLASSIFIED AREAS UNSUITABLE FOR ITS SAFETY RATINGS.	
CSA C22.2 No. 213-M1987 Non-Incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations	
US and Canadian Approval Per the Class / Division Classification System, this unit is rated for safe use in the following classified locations:	Class I Division 2 Groups A, B, C, D 300° C (T2) T_{amb} -21°C to +60° C (-6°F to 140°F)

The following symbol is used to identify and warn against specific hazards, and for accident prevention purposes:

Safety Alert Symbol with Keyword	Definition and Meaning
<i>Warning</i> 	Keyword that indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Warning 	To prevent ignition of a hazardous atmosphere, batteries must only be charged or changed in an area known to be non-hazardous.
Warning 	Explosion hazard – Do not disconnect while circuit is live unless area is known to be non-hazardous.
Warning 	Explosion hazard – Equipment not to be connected to a TNV source when used in a Class I Division 2 area.
Warning 	Explosion hazard – Substitution of components may impair suitability for Class I, Division 2, Groups A, B, C, D.
Caution 	Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.
Warning 	Inspect enclosure for signs of deterioration such as cracking, warping, swelling or softening. Do not use in Hazardous (Classified) Locations if there are any signs of deterioration.

Getting Started

Note: When your MX5X is pre-configured, the wireless client, flash card and scanner are programmed by LXE to your specifications. The sequence of steps in Getting Started must also be completed when the MX5X returns from a Cold Reset and when a new OS version is loaded. The wireless client, flash card, virtual keyboard and scanner parameters may also need to be reset after a cold reset.

This section's instructions are based on the assumption that your new 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, MX5X, and components from electrostatic discharge.


In general, the sequence of events is:

Windows CE .NET 4.2



MX5X Desktop CE Indication

1. Insert a fully charged battery. (Always put a fully charged battery in the MX5X 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. Press < N > when the message Update Micro/Boot? Y/N (*timer countdown*) is displayed, or, let the timer count down.
5. Calibrate the touchscreen.

After all files are loaded and the Desktop is displayed, adjust audio volume and other parameters if desired. If needed, change the Time and Date from it's default value by tapping the  | **Settings** | **Control Panel** | **Date/Time** icon.


Windows CE 5.0



MX5X Desktop CE Indication

1. Insert a fully charged battery. (Always put a fully charged battery in the MX5X at the beginning of the shift or workday.)
2. If the screen does not automatically display, tap the Power key.
3. Calibrate the touchscreen.

After all files are loaded and the Desktop is displayed, adjust audio volume and other parameters if desired.

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

Troubleshooting Start-up

Can't align the screen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts user access to the control panels. See <i>Chapter 6 - AppLock</i> for setup and processing information.
RFTerm® opens and runs upon each cold reset and warm reset.	This activity is the default setting for RFTerm. Tap File Exit to close the RFTerm application.
Touch screen won't accept stylus taps.	Touchscreen may have been disabled or the touchscreen may require recalibration. Hold down the Power key and the Orange key for 4+ seconds to warmboot the device. Force the Start menu to appear by pressing the right arrow key and the Blue key to access Start button options, then use the arrow keys to select menu options (e.g. Start Settings).
The MX5X seems to lockup as soon as it is warm booted.	There may be small delays while the wireless client connects to the network, Wavelink Avalanche management of the MX5X startup completes, and AppLock launch sequences finalize.

Setup the Client and Network

Prerequisites

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



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

Access Terminal Emulation Parameters




RFTerm icon on desktop.

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

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

to properly set up your host session.

Make sure the mobile client network settings are configured and functional. If you are connecting over wireless LAN (802.11b/g), make sure your mobile client is communicating with the Access Point.

1. From  | 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.

Saving Settings

When returning from a Cold Reset the previously saved (or original if this is the first Cold Reset) registry savings are reloaded.

When you want to save the registry without having to reset the MX5X, tap the My Computer icon then the System folder then double-tap the RegSave file.

The RegSave utility creates the RegTemp.reg registry backup file. The registry is reloaded from the RegTemp.reg file after a Cold Reset.

The registry save process takes 5 – 10 seconds. It is also saved after each Resume from Suspend and each time the OK button is tapped in Control Panel applets.

Components



Figure 1-3 Front of MX5X

- | | | | |
|---|-----------------|---|-----------|
| 1 | Scanner Housing | 4 | Keypad |
| 2 | Microphone | 5 | Power Key |
| 3 | Touchscreen | 6 | Speaker |

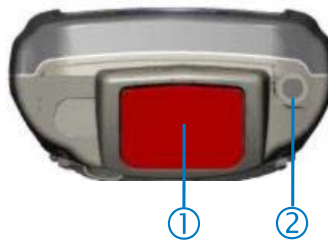


Figure 1-4 Scan Aperture and Audio Jack

- | | | | |
|---|---------------|---|------------|
| 1 | Scan Aperture | 2 | Audio Jack |
|---|---------------|---|------------|

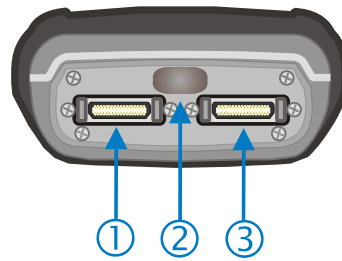


Figure 1-5 Ports

- | | | | |
|---|---|---|--|
| 1 | COM 1 – RS-232, Ethernet, USB and AC Power Connection | 3 | COM 4 – RS-232 and AC Power Connection |
| 2 | COM 3 – IR Port | | |



Figure 1-6 Back w/Optional Handle or Hand Strap

- | | | | |
|---|--------------------------|---|------------------|
| 1 | Scanner | 4 | Trigger |
| 2 | Stylus and Stylus Pocket | 5 | Battery Fastener |
| 3 | Trigger Handle | 6 | Main Battery |



Figure 1-7 Handle (Optional)

1 Scan Aperture
2 Trigger

3 Handle

Power Key

Note: Refer to the section titled *Power Modes* later in this guide for information relating to the power states of the MX5X.



Figure 1-8 Power Key Location

The Power key is located next to the < Z > key on the keypad. When a battery is inserted in the MX5X for the first time press the Power key.

Tapping the Power key places the MX5X immediately in Suspend mode. Tapping the Power key again, or connecting to AC power, immediately releases the MX5X from Suspend Mode.

Please refer to the section titled *Power Modes* later in this guide for a list of the kinds of activities that will return the MX5X from Suspend Mode.

Please refer to the section titled *Power Key* in Chapter 2 for Reboot options and instruction.

Assembly

Insert Main Battery

Press the Power key after the battery is inserted into the MX5X.

Note: On first use the MX5X batteries should be charged with an external power source (i.e. AC Adapter, powered MX5 cradle or MX5 Multi-Charger) – 3 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 MX5 Multi-Charger.

The MX5X battery compartment is located at the bottom of the back of the mobile device. The fasteners in the main battery pack are connected to the battery pack.

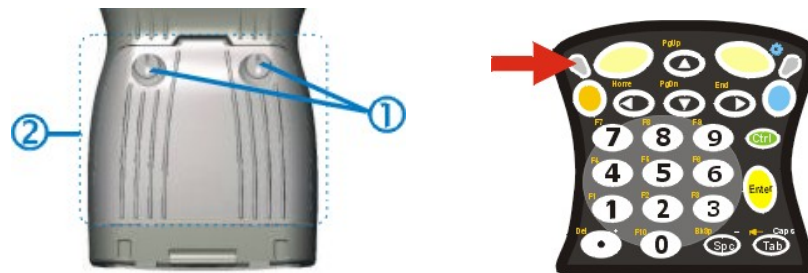



Figure 1-9 Main Battery Pack

- 1 Battery Pack Fasteners
- 2 Battery Pack

Note: Using the battery removal tool (or a coin) twist each fastener to the left to loosen the battery pack. Twist the fastener to the right to tighten the battery pack.

Place the battery in the battery well, making sure the tabs on the bottom of the battery pack fit into the slots at the bottom end of the battery well. Push the battery down into the battery well while fastening the screws. Fasten the screws tight enough to allow the rubber gasket to create a watertight seal. If the screws do not easily twist into the threaded opening, remove the battery pack and repeat the process. When the main battery pack is charging, the Battery Charge LED flashes green. The backup battery is trickle-charged by the main battery. There is no backup battery charging indicator. Whenever possible, use the AC power adapter with the MX5X to conserve the main battery and charge the backup battery.

About Lithium-Ion Batteries

Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the MX5X 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 will vary based on usage, ambient temperature and peripherals drawing power from the MX5:

100% capacity	2800 mAh minimum
80% capacity	2240 mAh minimum

Deciding when to put a fully charged main battery pack in the MX5X is difficult to quantify because it is very application specific. 1800 mAh may be the cutoff for one customer who uses the computer frequently, while 1000 mAh may be perfectly fine for a customer who occasionally uses the computer. 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.

Connect External Power Supply (Optional)

The MX5X receives AC/DC power from the AC/DC 12V Power Supply or a powered MX5 Cradle.

The MX5X DC power connection is located at the base of the MX5X. The cradle power jack is located on the back of the cradle.

The A/C power cable is not included with the Power Supply, please contact your LXE representative for replacement power cables. When the power cable is connected to a wall outlet and the Power Supply, the ON indicator on the Power Supply illuminates green.



Figure 1-10 AC/DC 12V External Power Supply

1. Squeeze the sides of the power connector and push the power cable connector into either MX5X port. The click means the connector is seated firmly.
2. The CHGR LED above the keypad illuminates when the MX5X is receiving external power through the power jack. The main battery recharges when the MX5X is connected to an external power source.

Note: When the MX5X is receiving power through a cradle connected to external power the MX5's CHGR LED is illuminated.

When the MX5X is connected to an external power supply, and the main battery pack is charging, the Battery Charge LED flashes green.



Figure 1-11 Battery Charging LED

Whenever possible, use the AC power adapter with the MX5X to conserve the main battery and charge the backup battery.

Install Pistol Grip Handle (Optional)

The MX5X can be purchased with a customer-installable pistol grip handle. The handle enables the user of the MX5X to hold the unit while pointing and activating the scanner with one hand. Pressing the trigger activates the scanner and functions the same as the Scan key on the keypad. With the handle installed the Scan key on the keypad remains active. The trigger duplicates the operation.

The handle is built of a durable and flexible plastic that will not detach from the MX5X if the unit is dropped.

The trigger handle is a mechanical device. Battery or external A/C power is not required for operation of the trigger handle. The trigger handle does not need to be removed when replacing the main battery pack.

Either the trigger handle is attached to the MX5X or the handstrap is attached, not both.

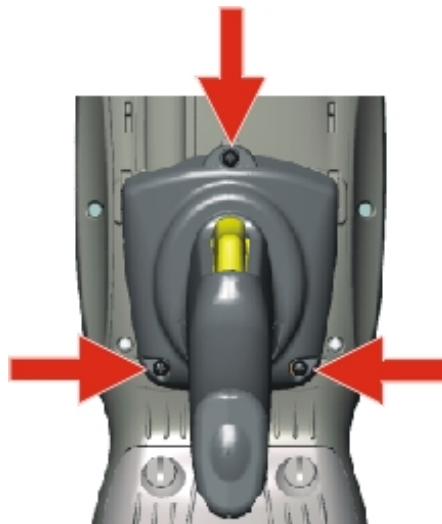


Figure 1-12 Trigger Handle Attach Points

Handle Installation

1. Place the MX5X, with the screen facing down, on a flat stable surface.
2. Slip the L-shaped plastic hooks, at the top of the handle, into the slots on each side of the back of the MX5X and slide the handle downward until the screw holes are visible.
3. Attach the pistol grip handle to the MX5X (as shown above) with the set of three screws and washers provided.
4. Test the handle's connection making sure the MX5X is securely connected.

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

Install Handstrap

Note: The handstrap cannot be used/installed when the MX5X has the trigger handle installed at the same time.

An elastic hand strap is available for the MX5X. 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 MX5X battery pack.

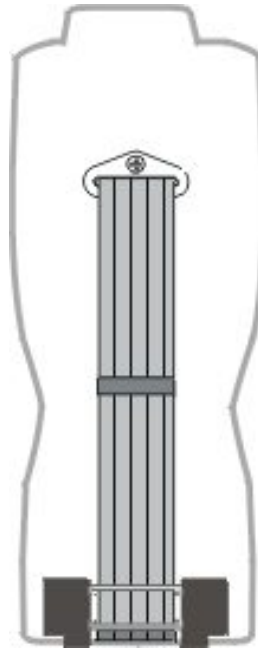


Figure 1-13 MX5X With Handstrap Installed

Installation

1. If a handle is installed, remove it at this time. See section *Install Pistol Grip Handle*.
2. Slip the strap through the upper bracket prior to securing the upper bracket to the unit.

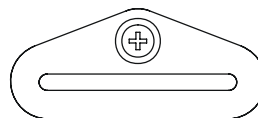


Figure 1-14 Upper Strap Bracket

3. When slipping the strap through the bracket make sure the closed loop fastener surface is up.
4. After slipping the strap through the bracket, fold the strap over so that the two closed loop fastener surfaces mate evenly.

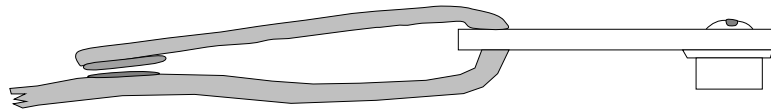


Figure 1-15 Strap Inserted in Upper Bracket

5. Prior to securing the upper bracket to the unit, slide the bottom assembly into the slots at the bottom of the MX5X. Insure that both ends of the bottom assembly are securely installed.
6. After securing the bottom of the strap to the MX5X, loosen the closed loop fastener strap and then secure the upper bracket to the unit with a screw.

Removal

1. Separate the closed loop fastener tabs and loosen the strap through the upper bracket.
2. Using a Phillips screwdriver, remove the upper bracket screw.
3. Pull the bottom assembly from the slots in the bottom back of the MX5X.

Slide the bottom bracket out and away from the MX5X when replacing the main battery pack.

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

How To

Tap 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, abrasive or sharp object to write on the touchscreen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. Firmly press the stylus into the stylus holder on the MX5X when the stylus is not in use.

Like using a mouse to left-click icons on a computer screen, using the stylus to tap icons on the MX5X 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 integrated barcode scanner or an input/output device connected to the serial port.
- A mouse right-click is performed by holding the stylus down on the touch screen. 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 constant stream of left mouse click messages. An application can choose to interpret this stream of messages as a right mouse click. LXE does not support non-LXE application programming.

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

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:.

- Press Tab and a Left or Right Arrow key to select a file.
- Press Shift and an Up or Down Arrow key to select several files. Press Shift+Arrow, then Shift+Arrow again for each additional file selected.
- Once you've selected a file, press Alt then press Enter to open its Properties dialog.
- Press Orange then press numeric dot to delete the currently highlighted file(name). Or, tap and hold the stylus on the filename and a menu box with a Delete option appears.

Calibrate the Touchscreen

Note: The first time it is used, the MX5X automatically runs the touchscreen calibration program. The calibration program is also run when Cold Reset is used.

If the MX5X is not responding properly to pen touch taps, the touchscreen may need to be recalibrated. Contact your System Administrator for assistance.

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

To start, select the Calibration tab then tap Recalibrate. Follow the instructions on the screen and press the Enter key to save the new calibration settings or press <Esc> to cancel or quit.

See Also: Chapter 3, section titled *Disable Touch and / or Calibration upon Cold Reset*.

Set Time Zone (Optional)

Note: The first time it is used, or the device returns from a Cold Reset, the MX5X sets 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)

Note: Upon initial startup, the MX5X automatically runs the touch screen calibration program and the Date/Time dialog.

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 and Keypad Backlight Timers

Note: Refer to the section titled Power Modes later in this manual for information relating to the power states of the MX5X.

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


The first option affects the MX5X when it is running on battery power only. The second option affects the MX5X when it is running on external power (e.g. AC adapter, powered vehicle or desktop cradle).

The default value for the battery power timer is 1 minute. The default value for the external power timer is 10 minutes. The backlight will remain on all the time when both checkboxes are blank.

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

Set the MX5X Power Schemes Timers

Note: Refer to the section titled *Power Modes* later in this guide for information relating to the power states of the MX5X.

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 MX5X will be running on battery power only.

Switch state to Suspend: Default is After 3 minutes

AC Power Scheme

Use this option when the MX5X will be running on external power (e.g. AC adapter, powered cradle).

Switch state to Suspend: Default is 5 minutes

Toggle the Display and Keypad Backlight On and Off

When the keypad backlight option is Enabled in  | Settings | Control Panel | Display | Backlight tab, both the display and the keypad backlights can be toggled on and off.

Locate the Blue key at the top of the keypad. Toggle the backlights on and off by pressing the Blue key, then the Right Scan key.

Increase or Decrease Keypad and Display Backlight Intensity

When the backlight is on, press the Orange key and the < 7 > key to decrease the intensity of the backlight. Repeating this keypress sequence continues to decrease the intensity of the backlight until the backlight is Off.

Once the backlight is off, use the Blue key and the Right Scan button keypress to toggle the backlight on. This process returns the backlight to its brightest intensity.

Connect Audio Jack (Optional)

The MX5X audio jack is located on the top of the unit next to the scan aperture. The internal speaker is disabled when the audio jack is connected.



Figure 1-16 Connect Audio Jack

Insert the barrel end of the connector into the MX5X audio jack and push in firmly.


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

Set The Audio Speaker Volume

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

The audio volume can be adjusted to a comfortable level for the user. The MX5X has an internal speaker and a jack for an external headset.

Using the Keypad

Note:  | Settings | Control Panel | Audio must have the options below Enable sounds for enabled before the following key sequences will adjust the volume.

To adjust speaker volume, locate the < V > key and the Blue key.

Adjust the speaker volume by pressing the:

Blue key, then the <V> 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.

As the arrow keys are tapped, the speaker beeps each time the volume increases or decreases in decibel range.

Using the Touch Screen

Tap the  | Settings | Control Panel | Audio icon.

Tabs	Actions
System	Moving the slider between Soft and Loud adjusts the speaker volume. Enable or disable sounds for each function by tapping the check boxes.
Routing	Use these options to determine where the audio output goes. Enable or disable the headset and speaker, and microphone gain.
Volume	As the volume scrollbar is moved between up and down for System volume, the computer beeps each time the volume increases or decreases in decibel range.
Extra	As the volume scrollbar is moved between up and down, the computer beeps each time the volume increases or decreases in decibel range for Bay Digital, CRMA Radio and Mixer volume.
Events	Choose sounds to play for Windows CE events or create your own sound scheme.

Troubleshooting Volume Adjust

Blue+V puts the MX5X in 'Volume Adjust' mode.

Shift+Blue+Shift puts the unit in 'Blue' Mode which, when followed by 'V', puts the unit in 'Volume Adjust' mode as well.

If the MX5X is responding to touch input, but does not respond to keypad (hard or soft) input, the MX5X may still be in Volume Adjust mode.

Press Enter to cancel (exit) Volume Adjust mode. After pressing enter, the MX5X should start responding to key input.

Enter the Multi AppLock Activation Key

Note: The touch screen must be enabled. See Chapter 6 - AppLock for AppLock instruction.

AppLock may be installed and running on the mobile device. AppLock restricts access to programs and the Windows CE Control Panel. Please contact your system administrator for instruction.

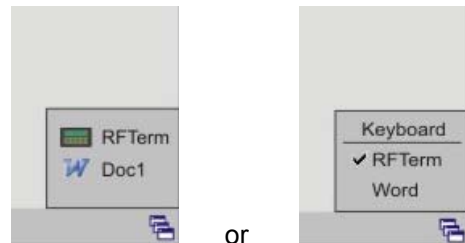


Figure 1-17 End-User Multi AppLock Touch Panel Segment

A checkmark indicates applications currently active or available for Launching by the user. Previous versions used the program icon to indicate the same function. When Keyboard is selected, the MX5X 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 visible at the far right in the taskbar. The taskbar is always visible on top of the application in focus. *Note: If only one application is configured and the Input Panel is not enabled, the Switchpad icon is not displayed.*

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the end-user. They can tap an application name in the popup menu and the selected application is brought to the foreground (in focus). 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 tap. The switchpad lists user applications as well as the Keyboard option.

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 (the default Global Key is Ctrl+Spc). When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground (in focus) 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.

Note that the system administrator may have assigned a different key sequence to use when switching applications.

Copy the MX5X LXEbook to the MX5X (Optional)

Note: The LXEbook user guides do not contain the illustrations and regulatory information contained in the full user guides on the LXE Manuals CD and on the LXE Website. See the full format user guide *MX5X User's Guide on the LXE Manuals CD*.

Mobile Device	Required Adobe Acrobat Reader Version
MX5X	Windows PDF Viewer (pre-installed by LXE)

First, using your desktop computer download *LXEbook – MX5X 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 MX5X to your PC.

When the MX5X and the desktop ActiveSync applications are synchronized, tap Explore on the ActiveSync menu on your PC to display the contents of the MX5X 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 MX5X.

When the file copy process is finished, disconnect the MX5X from the synchronization equipment and close ActiveSync.

To view the LXEbook on the MX5X, select  | Programs | PDF Viewer | File | Open. Locate the LXEbook on the MX5X and 'open' the file.

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

Enter Data

You can enter data into the MX5X through several different methods. The Scanner aperture provides barcode data entry, the RS-232 serial port or the IR port are used to input/output data, and the keypad provides manual entry.

Mobile devices with a touch screen and Microsoft CE software can use a stylus to input data, the COM ports and/or the keypad. An input panel (virtual keyboard) is available in applications that expect keyed input.

Keypad Entry

The keypad is used to manually input data that is not collected otherwise. Almost any function that a full sized computer keyboard can provide is duplicated on the MX5X keypad 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 2nd key function. For example, when you press a Blue or Orange key (the 2nd key), then press the key that has the desired second-function key, the second-function key is the ‘active’ key. The specific 2nd character is printed above the corresponding key in either Orange or Blue.

Stylus Data Entry

Note: This section is directed to the MX5X 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 MX5X 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 desk top 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 scanner and an input/output device connected to a 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, integrated scanner or a scanner connected to the serial port on the cradle, if the scanner applet is configured correctly.

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

See Also: Chapter 3, section titled Disable Touch and / or Calibration upon Cold Reset.

Scanner Entry

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

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



Figure 1-18 Scan Beam

Align the red beam so that the barcode is centered within the beam. The laser beam must cross the entire barcode. Move the MX5X towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.



Figure 1-19 Scanner LED Location

The Scanner Active LED turns red when the laser beam is on. Following a barcode scan and read the Scanner Active LED turns green for two seconds and the MX5X beeps, indicating a successful scan. If the scan was unsuccessful, the Scanner Active LED turns off and a different beep sequence is heard.

The laser engine and Scanner Active LED automatically turn off after a successful or unsuccessful read. The scanner is ready to scan again after the Scan key (or trigger on the handle if installed) is released, or after the green LED turns off following a successful scan.

Data Entry and Tethered Scanners

Please refer to the tethered scanner manufacturer's user guide for instruction.

Input Panel

The Input Panel is always available. Tap the virtual keyboard icon at the bottom of the screen to put the input panel 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 1-20 Input Panel

RS-232 Data Entry

The MX5X accepts input from an RS-232 device connected to either RS-232 port.

Note: ActiveSync (running on the desktop computer) will not transfer files over the RS-232 connector on the MX5 cradle IF the scanner port is configured for COM 1 External. Refer to ActiveSync Processes in Chapter 3 of this guide.

Getting Help

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

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

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

Manuals

This document is one in a series covering the MX5X family of computers:

For MX5X computers equipped with Microsoft Windows CE Operating Systems:

- MX5X User's Guide
- MX5X Reference Guide
- LXEbook – MX5X User's Guide (can be downloaded to the MX5X device from the LXE Manuals CD.)

For MX5X Intrinsically Safe (I-SAFE) computers equipped with Microsoft Windows CE Operating System:

- MX5X Intrinsically Safe User's Guide
- MX5X Reference Guide
- LXEbook – MX5X I-Safe User's Guide (can be downloaded to the I-SAFE device from the LXE Manuals CD.)

For both MX5X and MX5 Pocket PC computers, the following are interchangeable (except where noted):

- MX5 Cradle Reference Guide
- MX5 Multi-charger Reference Guide
- MX5 Belt Battery System (LXE suggests using this accessory specifically with a Low Temperature MX5X. **Do not use the MX5 Belt Battery System with an MX5-IS in a hazardous location.**)

Additional Manuals

- RFTerm Reference Guide
- LXE Security Primer
- CE API Programmer's Guide
- Integrated Scanner Programming Guide

Accessories

Note: Bluetooth access, Bluetooth modules and Bluetooth Manager are not supported by LXE.

MX5X Standard

Note: Items with a Green letter R in the first 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.

Holding Accessories		
R	Strap, Hand, Nylon	MX5A401HANDSTRAP
	Handle, w/wrist strap	MX5A406HANDLE
R	Handle, Neoprene slip-on cover	MX5A407HANDLECOVER
R	Case and strap, MX5X w/o handle	MX5A402CASE1
R	Case and strap, MX5X w/handle	MX5A403CASE2
R	Holster, MX5X w/o handle, w/o belt	MX5A404HOLSTER1
	Holster, MX5X w/handle, w/o belt	MX5A405HOLSTER2
R	Holster, MX5X w/handle, w/o belt	9000A407HOLSTERHAND
R	Belt, Use with Holsters	9200L67
	Belt, Heater Battery, MX5 (US only)	MX5A382HTRBATTBELT
	Charger, Heater Battery Belt, MX5 (US only)	MX5A383BATTBELTCHGR
	Cable, Heater Battery Belt to MX5, 12" US only (US only)	MX5A053CBLBATTBELT
R	Cable, Heater Battery Belt to MX5, 1.5M (Non-US)	MX5A054CBLBATTBELTWW
Miscellaneous		
R	Stylus, Tethered	9000A507STYLUS
R	Stylus, 6 Pack Replacement, MX5	MX5A501STYLUS
R	Software, CE .NET 4.2 SDK, MX5 CE	MX5XA505CENET42SDK
Battery Chargers and Battery		
	6 Unit Charger w/ US Power Cable	MX5A385CHGR6US
R	6 Unit Charger w/o US Power Cable	MX5A385CHGR6WW
R	Tool, Battery Removal 5 Pack, MX5	9000A508BATTERYTOOL
R	Battery, Li-Ion	MX5A379BATT
Cradles and Power Supplies		
R	Vehicle Mount Cradle (Power Adapter Required)	MX5A001VMCRADLE
R	Standard Desktop Cradle	MX5A002DESKCRADLE
R	Enhanced Desktop Cradle, MX5	MX5A003EDESKCRADLE
R	Enhanced Desktop Cradle, Ethernet, MX5X	MX5A004ETHDESKCRADLE
	Power Supply, AC/DC w/ US Power Cable	MX5A305PSACUS
R	Power Supply AC/DC w/o Power Cable	MX5A305PSACWW
R	Power Supply, 12V, Bare Wire Input, MX5X Output	MX5A306PS12V
	Power Supply, 12V Auto to VM Cradle	MX5A380PSAUTO12VUS
R	Power Supply, 12V Auto to VM Cradle (EU)	MX5A381PSAUTO12VWW
R	Power Supply, 24V-72V, Bare Wire Input, MX5X Output	9000A316PS24V72VMX5
Cables for Cradle and MX5/MX5X Serial Ports		
R	Cable, MX5 to PC RS-232, D26 to DA9F	MX5A051CBLD26DA9F
R	Cable, MX5 to PC USB, D26 to USB	MX5A052CBLD26USB
R	Cable, MX5 D26 to Ethernet RJ45, MX5X	MX5A057CBLETHD26RJ45
R	Cable, MX5 D26 to USB Host Receptacle, MX5X	MX5A058CBLD26USBHOST

Tethered Scanners (requires 3" D26 to DA9M cable)		
R	Cable, MX5X for Powerscan, 3", D26 to DA9M	MX5A055CBL3IND26D9M
R	Scanner, Powerscan, SR, 8' Cbl	8300A326SCNRPWRSR8DA9F
R	Strap with Scanner clip	9000A411SCNRSTRAP
	Scanner, Powerscan, SR, 12' Cbl	8300A327SCNRPWRSR12DA9F
R	Scanner, Powerscan, LR, 8' Cbl	8310A326SCNRPWRLR8DA9F
R	Scanner, Powerscan, LR, 12' Cbl	8310A327SCNRPWRLR12DA9F
R	Scanner, Powerscan, XLR, 8' Cbl	8320A326SCNRPWRXLR8DA9F
	Scanner, Powerscan, XLR, 12' Cbl	8320A327SCNRPWRXLR12DA9F

MX5X ISAFE Device

Note: US and Canada only.

Holding Accessories		
R	Strap, Hand, Nylon	MX5A401HANDSTRAP
R	Handle, w/wrist strap	MX5A406HANDLE
R	Handle, Neoprene slip-on cover	MX5A407HANDLECOVER
R	Case and strap, MX5X w/o handle	MX5A402CASE1
R	Case and strap, MX5X w/handle	MX5A403CASE2
R	Holster, MX5X w/o handle, w/o belt	MX5A404HOLSTER1
R	Holster, MX5X w/handle, w/o belt	9000A407HOLSTERHAND
R	Belt, Use with Holsters	9200L67
Miscellaneous		
R	Stylus, Tethered	9000A507STYLUS
R	Stylus, 6 Pack Replacement, MX5	MX5A501STYLUS
R	Software, CE .NET 4.2 SDK, MX5 CE	MX5XA505CENET42SDK
R	Rubber dust covers for external data ports. Two covers with tether.	I62-0465-001
Battery Chargers and Battery		
	6 Unit Charger w/ US Power Cable, 2 Battery Removal Tools	MX5A385CHGR6US
R	Tool, Battery Removal 5 Pack, MX5	9000A508BATTERYTOOL
R	Battery, Li-Ion	MX5A379BATT
Cradles and Power Supplies		
R	Standard Desktop Cradle	MX5A002DESKCRADLE
R	Enhanced Desktop Cradle, MX5X (Not ISAFE Approved)	MX5A003EDESKCRADLE
R	Enhanced Desktop Cradle, Ethernet, MX5X	MX5A004ETHDESKCRADLE
	Power Supply, AC/DC w/ US Power Cable (Not ISAFE Approved)	MX5A305PSACUS
Cables for Cradle and MX5/MX5X Serial Ports		
R	Cable, MX5X to PC RS-232, D26 to DA9F	MX5A051CBLD26DA9F
R	Cable, MX5X to PC USB, D26 to USB	MX5A052CBLD26USB
R	Cable, MX5X D26 to Ethernet RJ45, MX5X	MX5A057CBLETHD26RJ45
R	Cable, MX5 D26 to USB Host Receptacle, MX5X	MX5A058CBLD26USBHOST
	<i>Note: Use MX5A051CBLD26DA9F or MX5A052CBLD26USB cable for ActiveSync communication with MX5X cradles.</i>	

Chapter 2 Physical Description and Layout

Hardware Configuration

System Hardware

The MX5X hardware configuration is shown in the following figure.

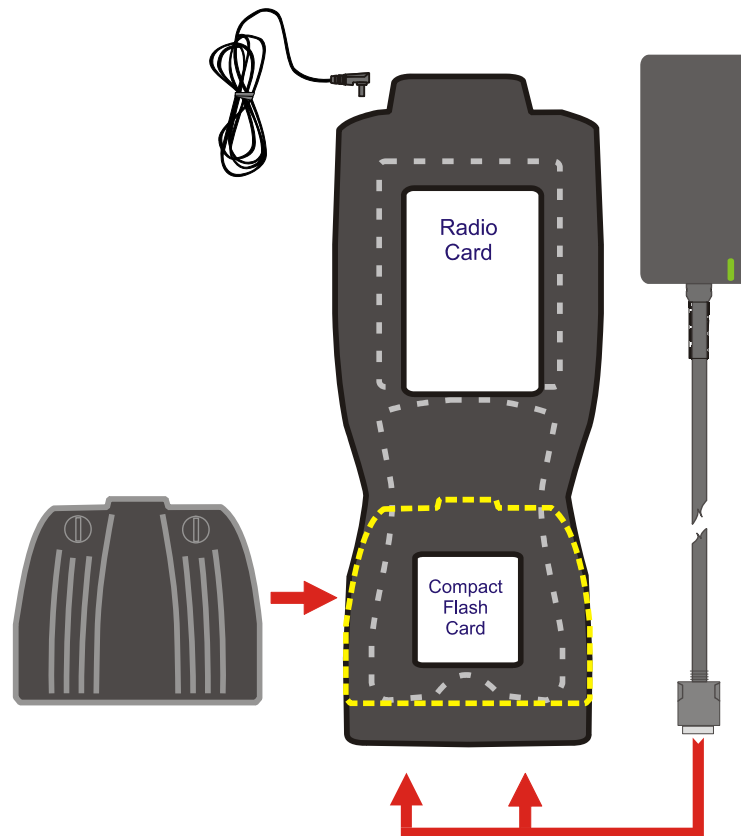


Figure 2-1 System Hardware

Note: LXE does not distribute nor support headsets connected to the MX5X.

Central Processing Unit

The LXE MX5X CPU is an Intel Xscale processor running at 400 MHz. The operating system is, either Microsoft CE .NET 4.2 or Microsoft CE 5.0, resident in flash memory.

Core Logic

The MX5X supports the following I/O components of the core logic:

- One PCMCIA slot (supports Type II PCMCIA cards).
- One compact Flash card slot (supports Type I and II cards) in the rear hatch.

- One ATA compact Flash card slot under the main battery pack.
- One InfraRed port.
- Two serial ports.
- One Digitizer Input port (Touchscreen).

Note: As the MX5X does not have PC Card Management software installed, LXE recommends purchasing pre-formatted cards.


System Memory

On-board 128MB low power DRAM, 64MB Compact Flash for operating system, 40MB available for application and data storage.

64MB Flash contains the CE operating system, hardware-specific OEM Adaptation Layer, device drivers, standard CE applications and utilities. The operating system supports MFC, ATL and Visual Basic programming languages, TCP/IP and PPP network protocols. The Flash is configured as the primary boot device.

The computer has one Type I/II CF slot and one ATA CF slot. The MX5X supports and auto detects up to 256MB of Type I compact flash memory.

Video Subsystem

The touchscreen is a 3/8" (9.65cm) ¼ VGA 240 by 320 pixel TFT Reflective Active Color LCD. Backlighting is available, 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 graphics modes.

A touch screen allows mouse functions (pointing and tapping on the display or Signature Capture) using an LXE approved stylus.

The color display is optimized for outdoor use but may also be used indoors. The color display has a CCFL (Cold-Cathode Fluorescent Lighting) front light.

The transfective display appears to have a greenish hue when the unit is in Suspend.

Power Supply

The LXE MX5X uses two batteries for operation.

A replaceable Lithium-Ion (Li-Ion) 2800mAh battery pack. The battery pack recharges while in the MX5X with the computer in a powered cradle or with the optional external power source attached. The main battery pack can be removed from the MX5X and inserted in the MX5 Multi-Charger which simultaneously charges up to six battery packs in four hours.

An internal 450 mAh Nickel Metal Hydride (NiMH) coin cell backup battery. The backup battery is recharged directly by an external power source. Full charging of the backup battery will take seven hours. The backup battery must be replaced by qualified service personnel.

Connecting the MX5X to an external power source, and a main battery in the MX5X, is necessary for backup battery charging.

COM Ports


The MX5X has two mini D serial ports that are configurable using the  | Settings | Handheld | Comms tab:



Figure 2-2 COM Ports – Left and Right

Port 1 (left) COM 1	Port 2 (right) COM 4
USB	RS-232
RS-232	AC Power
AC Power	
Ethernet	
COM 3 is always the IR port.	
ActiveSync	

Power to the COM ports may be turned on and off.

Note: *ActiveSync is not configurable to work on COM 4. IR ActiveSync application is available. Refer to ActiveSync Processes in Chapter 3 of this guide.*

Audio Interface

An interface is available for headset/microphone operation. When the headset is plugged into the audio port next to the scan aperture, the speaker at the bottom, front of the MX5X is disabled.

Power Key

Note: Refer to the section titled *Power Modes* for information relating to the power states of the MX5X.

The power key is located next to the < Z > key on the keypad. When a battery is inserted in the MX5X for the first time, the Power key must be pressed.

Quickly tapping the Power key places the MX5X immediately in Suspend mode. Quickly tapping the Power key again, or connecting the AC adapter, immediately returns the MX5X from Suspend.

Note: The unit will not suspend on AC power nor when connected through ActiveSync.

Reboot Sequence

When the desktop is displayed or an application begins, the power up (or reboot) sequence is complete. If you have previously saved your settings², they will be restored on reboot.


Warm Reset

Hold down the Power key and the Orange key for 4+ seconds. A warm reset does not affect the operating system and no data loss occurs.

Cold Reset

Hold down the Power key, the Blue key and the Orange keys for 4+ seconds. The MX5X will power off, release the keys and the device will power on again.

Calibrating the touchscreen will need to be performed when the MX5X powers on again. See Chapter 3, section titled *Disable Touch and / or Calibration upon Cold Reset*.

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

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 as necessary.

LXE recommends the RegSave file be run when configuration changes are made.

Note: When performing a Cold Reset on a device, the system will ask if you want to overwrite files – LXE recommends selecting No and continuing with the Cold Reset process.



If you need to set up the SE1223, SE1224 or SE2223 integrated scanner barcode reading parameters, please refer to the *Integrated Scanner Programming Guide* on the LXE Manuals CD or the LXE ServicePass website.

² Configuration settings are saved when a configuration applet is exited by tapping OK.

PCMCIA and Flash Cards

Note: When removing or installing PCMCIA and/or Compact Flash cards, protect the MX5X internal components from electrostatic discharge.

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

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

The compact flash card under the main battery pack is ATA only and is intended to store program CAB files, MX5X utilities, the registry and the registry backup information.

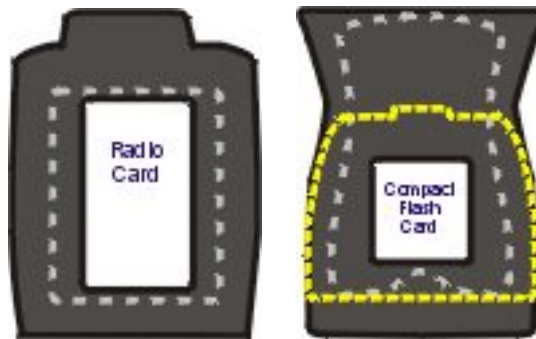


Figure 2-3 PCMCIA Wireless Client Card and Flash Card Location

Note: As there is no PC Card management software loaded on the MX5X, LXE recommends purchasing preformatted PC and Flash cards as well as preformatted Compact Flash disks.

Slot 1

The MX5X has one internal PCMCIA slot that conforms electrically to PCMCIA 2.1 specifications. The PC Slot supplies .75 of an amp at 3V, 5V and for dual 3.3V/5V cards. Battery voltage is supplied through unused pin 35 to support a WAN wireless client in the slot, if installed.

The PC slot is accessible by the use of a Phillips screwdriver to remove the back hatch of the unit. It accepts Type II cards only. Slot 0 accepts PCMCIA 2.4GHz wireless client cards.

Note: Care must be taken, when reattaching the back hatch to the device, to preserve the water tight seal.

Slot 0

The MX5X has one internal compact Flash card port that supports Type I and II CF cards.

The wireless client drivers are stored on the compact flash card in the ATA CF slot (under the main battery pack). During the cold boot process, the `JmpStart` program accesses the compact flash card and loads the wireless client drivers and any saved parameters.

Installation / Removal

Equipment required: A screwdriver (not supplied by LXE)

- 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 MX5X 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.

PCMCIA Cards

Installation

1. Using a screwdriver, loosen the back hatch of the MX5X and carefully remove or loosen all cables. Disconnect the antenna from the network card.
2. Set both the back and the screws aside.
3. Slide the PC Card, connector side first, into the slot until it seats. Use caution not to pull or snag the antenna connector.
4. If the PC Card is difficult to seat in the slot, remove the card, turn it around and re-install.

Removal

Grasp the top of the PC Card and pull it straight upward to remove.

Use caution not to pull or snag the antenna connector on a network card, if installed.

Flash Cards

Installation

Place the MX5X into Suspend. Disconnect the AC adapter from the MX5X.

- ATA CF Card – Loosen then remove the main battery pack.
- Hatch CF Card – Loosen then remove the back cover of the MX5X taking care not to pinch or twist any cables. Follow the instructions for removing the PCMCIA card, if installed.

Insert the CF card in the recessed slot, label side uppermost.

Replace the main battery pack (or the PC card and back cover of the MX5) and perform a warm reset. *Always perform a warm reset when exchanging one Flash card for another.*

Removal


Place the MX5X into Suspend. Disconnect the AC adapter from the MX5X.

- ATA CF Card – Loosen then remove the main battery pack.
- Hatch CF Card – Loosen then remove the back cover of the MX5X taking care not to pinch or twist any cables. Follow the instructions for removing the PCMCIA card, if necessary.


Carefully lift the CF card up and away from the recessed slot.

Accessing the Data on CF and PCMCIA Cards


ATA CF Card

Tap the  | Programs | Windows Explorer | System folder.

Hatch CF Card

Tap the  | Programs | Windows Explorer | Storage Card (Storage Card 2 when the PCMCIA slot is not empty).

Hatch PCMCIA Card

Tap the  | Programs | Windows Explorer | Storage Card.

COM Ports

The MX5X supports three COM port options.





Scanner Port	
RS-232 Port, Ethernet, USB and AC Power (COM 1, left)	
RS-232 Port, AC Power (COM 4, right)	
IR Port (COM 3)	

Figure 2-4 COM Ports

COM 1 port is always the left (with screen facing up) RS-232 port on the base of the MX5X. COM 1 port accepts RS-232, USB, USB Host, Ethernet and AC power connectors.

The RS-232 port on the docking cradle is ‘connected’ to the MX5X when a tethered scanner is connected to the RS-232 port on the MX5 cradle, and the MX5X is in the cradle. The cradle must be powered by an alternate AC or DC power source to enable tethered scanner use.

The COM 3 port is always the IR port on the base of the MX5X.

COM 4 is always the right (with screen facing up) RS-232 port on the base of the MX5X. COM 4 port accepts RS-232 and AC power connectors.

To edit Scanner Com Port parameters, tap the  | Settings | Control Panel | Scanner. Change the parameter values and tap OK to save the changes.

An RJ45 Ethernet port is on the Enhanced Desktop Cradle with Ethernet Port.

USB Port

The USB port requires a DB26 to USB cable (available from LXE). The serial port/USB port also supports serial data transfer (using a null modem cable) and USB I/O at 1.5 Mbps. The MX5X automatically detects the cable configuration. Host and client is automatically configured based on the type of cable used.

Refer to section titled *Accessories* in this guide for part numbers for the DB26-USB cable and the null modem cable.

Integrated Scanner Port (Optional)

The MX5X integrated barcode scanner is used to collect barcode data from any nearby compatible barcode label. Depending on the size of the barcode, size of bars and spacing and quality of the barcode, the scanner is used to read barcodes between 3 in (7.6 cm) and 30 in (76 cm). The barcode scanner reads UPC/EAN, Code 39, Code 93, I 2 of 5, Discrete 2 of 5, Code 128, Codabar and MSI symbologies.

The internal barcode scanner scans only when either Scan button is pressed or the scan trigger is pressed, if installed. Scan buttons have no effect on tethered barcode scanners connected to the RS-232 port. The Scanner LED illuminates during any integrated scanner activation.

Look on the label on the back of the MX5X. The type of installed scan engine should be clearly labeled and may be one of the following:


- Symbol SE 1224 HP
- Symbol SE 1223 LR
- Symbol SE 1223 ALR
- Symbol SE 2223 2D

Use the scanner label information if you need to program the *Symbol* scanner engine using the barcodes in the *Integrated Scanner Programming Guide* (available on the LXE Manuals CD or the LXE ServicePass website).

Note: Use the scanner control panel to set up using both the integrated scanner and a tethered scanner.

To switch active scanner Com ports tap the  | Settings | Control Panel | Scanner | Main tab.

Note: If there is no internal scanner, Internal is greyed out. On units without an internal scanner, controls on Port 1 and Port 2 are greyed out – the COM1 external control can be selected.


To assign baud rate, parity, stop bits and data bits to Com 1, tap the  | Settings | Control Panel | Scanner | COM1 tab.

If the scanner needs to be configured, refer to the *Integrated Scanner Programming Guide* on the LXE Manuals CD.


Tethered Scanners (Optional)

Note: LXE cable number MX5A055CBL3IND26D9M must be used with PowerScan® SR, LR and XLR tethered scanners connected directly to the MX5X device. Do not connect Symbol® tethered scanners to the MX5X device or to this cable.

The MX5X Scan buttons have no effect on tethered barcode scanners connected to a serial port on the MX5X or vehicle cradle. Tethered scanners read barcode scans only when the trigger on the tethered scanner is pressed.

To set the MX5X to use a tethered scanner, tap the  | Settings | Control Panel | Scanner | Main tab.

Tap the Send Key Messages (WEDGE) checkbox. The COM port that accepts the scanner data can be configured for data rate, parity, stop bits and data bits using the COM1 tab.

If the tethered scanner is powered by the mobile device, enable Power Output in  | Settings | Control Panel | Handheld | Comms tab.

See Also: Tethered Barcode Scanner Data Entry Using the MX5 Cradle.

Data Entry and Tethered Scanners

Please refer to the tethered scanner manufacturer's user guide for instruction.

RS-232 Serial Ports

RS-232 connection is made through an RS-232 serial port. The connector is an industry-standard RS-232 DB26 female connector. The MX5X automatically detects the cable configuration type.



Figure 2-5 RS-232 Ports

COM1

Cable connections: RS-232, Ethernet, USB and AC Power.

PIN	SIGNAL	PIN	SIGNAL
1	CHG +	14	CHG GND
2	CHG +	15	CHG GND
3	CHG +	16	CHG GND
4	DCD1	17	TPO +
5	RX1	18	TPO -
6	TX1	19	GND
7	DTR1	20	TPI +
8	DSR1	21	VCCOUT2
9	RTS1	22	TPI -
10	CTS1	23	RI VCCOUT1
11	SHIELD	24	SHIELD
12	USB +5V	25	USB COM
13	USB +	26	USB -

COM4

Cable connections: RS-232 and AC Power.

PIN	SIGNAL	PIN	SIGNAL
1	CHG +	14	CHG GND
2	CHG +	15	CHG GND
3	CHG +	16	CHG GND
4	DCD2	17	NC
5	RX2	18	NC
6	TX2	19	GND
7	DTR2	20	NC
8	DSR2	21	NC
9	RTS2	22	NC
10	CTS2	23	RI VCCOUT2
11	NC	24	NC
12	NC	25	NC
13	NC	26	NC

Figure 2-6 DB26 RS-232 Pinouts

USB Port

The USB port (the left port when the MX5X is face up) requires a DB26 to USB cable (available from LXE). The connector is an industry-standard RS-232 DB26 female connector.



Figure 2-7 MX5X USB Port

The serial port/USB port also supports serial data transfer (using a null modem cable) and USB I/O at 1.5 Mbps. The MX5X automatically detects the cable configuration. Refer to section titled *Accessories* in this guide for part numbers for the DB26-USB cable and the null modem cable.

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

MX5X Cable End	Cable Signal	USB Cable End
1 Not Used		1 Not Used
2 Not Used		2 From 7
3 To 3	D + (Green Wire)	3 From 3
4 Not Used		4 From 5
5 To 4	Ground (Black Wire)	5 Not Used
6 Not Used		6 Not Used
7 To 2	D - (White Wire)	7 Not Used
8 Not Used		8 Not Used
9 Not Used		9 Not Used

Figure 2-8 USB-Serial Cable Pinouts

IR Port

The InfraRed (IR) port provides a means of transferring information to a device with a similar port and the proper software. The IR port can be used to communicate with printers or a host computer with the use of an adapter.

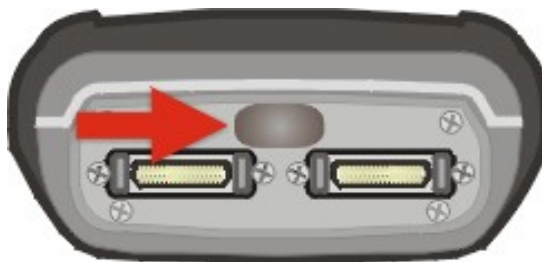


Figure 2-9 IR Port on MX5X

The IR Port is specified as COM 3 and is a bi-directional half-duplex infrared port. It supports the Slow IrDA (Infrared Data Access) PHY Layer standard that allows communication speeds up to 115k baud.

When sending data through the IR port to another MX5X IR port, make sure both units are in close proximity to each other. The IR operating envelope has a distance range of 2 cm (0.79 inches) to 15 centimeters (6 inches) with a viewing angle of 30 degrees.

Programmable Buttons



Figure 2-10 Scan Buttons

The Scan buttons can be programmed by the System Administrator to perform the following functions:

Disabled	Key press has no effect.
Scan	Pressing this key activates the laser scanner.
Enter	Pressing this key confirms a forms entry or transmits information. See the following section titled <i>Enter Key Function</i> in <i>The Keypad</i> section.
Tab	Pressing this key moves the cursor to the next input field.
Field Exit	IBM5250/TN5250 units only. Pressing this key exits an input field. See the following section titled <i>Field Exit Key Function</i> in <i>The Keypad</i> section.
Esc	Pressing this key cancels the current operation.

The default setting for the right button is Enter. The default setting for the left button is Enter.

When the MX5X does *not* have an integrated scanner, both buttons default to Enter keys and the Scan selection is greyed out. The buttons can be programmed to perform other functions when there is no internal scanner.

How To: Program the Scan Buttons

Access: the  | Settings | Control Panel | Scanner | Keys tab

Tap the desired control option. Tap OK to close this menu option. Tap X to cancel changes. Any changes made are in effect immediately.

Power Modes

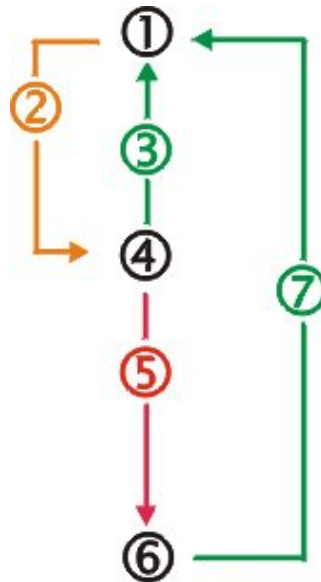


Figure 2-11 Power Modes – On, Suspend and Off

1. On
2. Tap Power key or the power has failed
3. Power key or connect to AC power supply
4. Suspend
5. Backup battery and main battery depleted
6. Off
7. Power On

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 MX5X

After a new MX5X has been received, a charged main battery inserted, and the Power key tapped, the MX5X 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.

LED Indicators

LED	When On ...
Scanner Active	Integrated barcode scanner function. Red – scanning. Green – good scan.
Main Battery Charging	Left Green LED flashes. When the battery is fully charged, the green LED remains lit.

Suspend Mode

The MX5X

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

MX5X Suspend timers are set using  | Settings | Control Panel | Power | Schemes tab.

A Power key tap wakes the unit and resets the display backlight timers.

Connecting the MX5X to AC power wakes the unit and resets the display backlight timers.

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 MX5X must be placed in Suspend mode before hot-swapping the main battery.

Off Mode

The unit is in Off Mode when the main battery and the backup battery are depleted. Insert a fully charged main battery and press the Power key to turn the MX5X On.

The Keypad

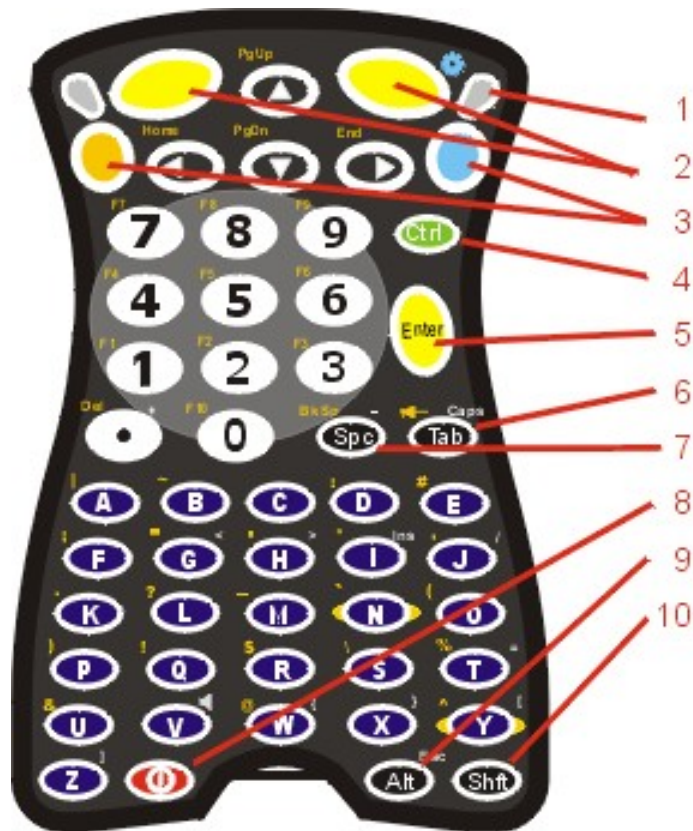


Figure 2-12 The ANSI / Batch Keypad

1	Scanner Active LED	6	Tab
2	Left and Right Scan	7	Spc
3	Blue and Orange 2 nd Function Key	8	Power On/Off
4	Ctrl	9	Alt
5	Enter	10	Shift

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

Scan Key Function



When programmed as Scan keys, either the left or right Scan key activates the scanner. The internal scanner scans only when the Scan button is pressed (or when the scan trigger is pressed on the optional trigger handle, if installed).

Enter Key Function



The Enter key is used to confirm a forms entry or to transmit information. How it is used is determined by the application running on the computer.

2nd Key Function



The Orange (top left) and Blue (top right) keys are 2nd keys used to activate the 2nd 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 2nd function of that key. Using the 2nd key activates the second key function. Note that the 2nd key only stays active for one keystroke. Each time you need to use the 2nd function you must press the Orange or Blue 2nd key. To cancel a 2nd function before pressing another key, press the 2nd key again.

Ctrl Key Function



The Ctrl key enables the control functions of the keypad. This function is similar to a regular keyboard's Control key. Note that the Ctrl key only stays active for one keystroke. Each time you need to use a Ctrl function, you need to press the Ctrl key before pressing the desired key.

Alt Key Function



The Alt key enables the alternate functions of the keypad. This function is similar to a regular keyboard's Alt key. Note that the Alt key only stays active for one keystroke. Each time you need to use an alternate function, you need to press the Alt key before pressing the desired key.

Shft 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.

Spc Key Function



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.

Field Exit Function



IBM TN5250 specific keypad only. The left Scan 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 *Programmable Buttons* section for instruction.

Mode Key Functions

Caps Key and CapsLock Mode



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

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

- 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.

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.

Keypress Sequences

See Appendix A for key maps for all keypads.

Input Panel

The Input Panel is always available. Tap the keyboard icon at the bottom of the screen to put the input panel on the display. See *Input Panel* in Chapter 1. If the touch screen has been disabled, the input panel is not available.

Accessing Files on the Compact Flash Card

Double tap My Computer then select System. Files stored on the Compact Flash (CF) card are listed.

Touchscreen



Figure 2-13 Touchscreen

The MX5X Touchscreen is an Active Color LCD unit capable of supporting QVGA 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 has a CCFL (Cold-Cathode Fluorescent Lighting) front light. When the device is in Suspend mode, the reflective 256 color display appears to have a greenish hue.

The display is automatically turned off when the MX5X enters the Suspend state.

See Also: Chapter 3, section titled *Disable Touch and / or Calibration upon Cold Reset*.

Display and Keypad Backlight Timer

When the Backlight timer expires the display and keypad backlight is turned off.

The default value for the battery power timer is 1 minute. The default value for the external power timer is 10 minutes.

The backlight timer *dims the backlight* on the touchscreen at the end of the specified time and turns the keypad backlight off. When the display wakes up, the Backlight timers begin the countdown again.

See the section titled *Set the Display Backlight Timer* in *Chapter 1 Introduction*, section titled *Quick Start*.

Cleaning the Glass Display/Scanner Aperture

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

As the MX5X screen is the same size as commercially available Palm® handheld devices, static screen protectors that fit the Palm device will also fit the MX5X. Static screen protectors for the MX5X are not available from or supported by LXE.

Speaker



Figure 2-14 Speaker Location

The MX5X Speaker has a loudness of at least 87 dB (1500 Hz) at 10 cm measured from the front of the unit. The Speaker volume is adjustable via the keypad or the Settings or by an application through the use of an API call. There are 5 distinct volume levels. The minimum volume level is 0 (no sound) with a default setting of 3. The volume sticks at maximum and minimum levels.

The speaker is disabled when a headset is plugged into the Audio Jack on the endcap. The audio volume can be adjusted to a comfortable level for the user. The volume is increased or decreased one step each time the volume key sequence is pressed.


Speaker volume is first enabled and adjusted using the 'Audio' icon. The default value for Audio is midrange Volume and all sounds enabled. When volume and sounds are enabled, speaker volume can be adjusted using the volume key sequence, if desired.

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

Set The Audio / Speaker Volume

The audio volume can be adjusted to a comfortable level for the user. The MX5X has an internal speaker and a jack for an external headset.

Using the Keypad

Note:  | Settings | Control Panel | Audio must have the options in the Enable sounds for checked before the following key sequences will adjust the volume.

To adjust speaker volume, locate the <V> key and the Blue key.

Adjust the speaker volume by pressing the:

- Blue key, then the <V> 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.

As the arrow keys are tapped, the computer beeps each time the volume increases or decreases in decibel range.

Using the Touch Screen

Tap the  | Settings | Control Panel | Audio icon.

Tabs	Actions
System	Moving the slider between Soft and Loud adjusts the speaker volume. Enable or disable sounds for each function by tapping the check boxes.
Routing	Use these options to determine where the audio output goes. Enable or disable the headset and speaker, and microphone gain.
Volume	As the volume scrollbar is moved between up and down for System volume, the computer beeps each time the volume increases or decreases in decibel range.
Extra	As the volume scrollbar is moved between up and down, the computer beeps each time the volume increases or decreases in decibel range for Bay Digital, CRMA Radio and Mixer volume.
Events	Choose sounds to play for Windows CE events or create your own sound scheme.

Troubleshooting

Blue+V puts the MX5X in *Volume Adjust mode*.

Shift+Blue+Shift puts the unit in *Blue Mode* which, when followed by <V>, puts the unit in Volume Adjust mode as well.

If the MX5X is responding to touch input, but does not respond to keypad (hard or soft) input, the MX5X may still be in Volume Adjust mode.

Press Enter to cancel (exit) Volume Adjust mode. After pressing enter, the MX5X should start responding to key input.


Power Supply

The MX5X 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 MX5X 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 MX5X 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 three hours when the MX5X is connected to external power through it's power jack.

Checking Battery Status

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

Important Battery Information

Important: If the main battery has been out of the MX5X for an extended period of time or becomes fully discharged or dead, a fully charged backup battery will last for up to 24 hours. If this happens, the device will cold reset the next time power is applied from either AC power or a charged main battery. A cold reset will cause loss of data and custom programs. Always store unused MX5's with a fully charged main battery pack installed.

Until the main battery and backup battery are completely depleted, the MX5X 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 MX5X to conserve the main battery and charge the backup battery..

When a new battery is installed in the MX5X for the first time (or when the backup battery is completely depleted), the Time and Date must be re-set.

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.

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 MX5X 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 Hot-Swapping

When the main battery power level is low, the MX5X will signal the user with a warning dialog box on the display and a warning tone. The low battery warning notice and tones continue until the main battery is replaced, the battery completely depletes, external power is applied to the MX5X using an AC Adapter, or the MX5X is placed in a powered cradle.

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

When the main battery is removed, the MX5X 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 MX5X cannot be used until a charged main battery pack is installed. After installing the new battery, the MX5X automatically transitions to the On state. Full operational recovery from Suspend can take several seconds while the wireless client (if installed) is reestablishing an RF link.

If the backup battery depletes before a fully charged main battery can be inserted, the MX5X will turn OFF and the Power key must be tapped after a main battery pack is installed.

Low Battery Warning

It is recommended that the main battery pack be removed (with the battery removal tool) and replaced when it's energy depletes. When the Low Battery Warning appears perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be.

When the unit is in an ON state, a low battery warning dialog box appears on the display and a warning tone is emitted.

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

Battery Status LEDs

Main Battery Charging	Left GREEN LED slow flashing.
Main Battery Fully Charged	Left GREEN LED stops flashing; is solid ON.
Charge / battery fault	Left GREEN LED has quick double flashes.

Backup Battery

The MX5X has a backup battery that is designed to provide limited-duration electrical power in the event of main battery pack failure. The backup battery is a 450 mAh Nickel Metal Hydride (NiMH) battery that is factory installed in the unit. The energy needed to charge the backup battery comes from an AC adapter.

It takes several hours of operation before the backup battery is capable of supporting the operation of the computer. The duration of backup battery life is dependent upon operation of the MX5X, it's features and any operating applications.

The backup battery is replaced by LXE.

Note: This mobile device's backup battery maintains it's 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 setup defaults when a fully charged main battery pack is installed and the device is powered On again.

Battery Maintenance Publication

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

Battery Chargers

MX5 Multi-Charger (Optional)



Figure 2-15 LXE Multi-Charger

The MX5X main battery pack can be charged in the LXE Multi-Charger.

The main battery pack can be charged in the LXE Multi-Charger. Please refer to the *MX5 Multi-Charger User's Guide* for instruction.

The multi-charger requires an external power source before battery pack charging can commence.

The external Power Supply for the Multi-charger is shipped with the multi-charger.

MX5 Multi-Chargers are not approved for use in Hazardous Locations.

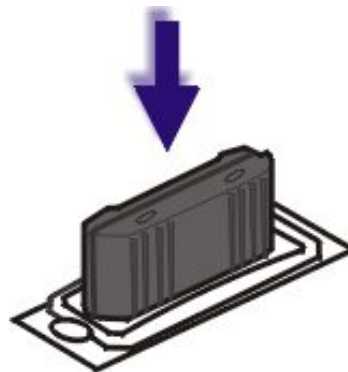


Figure 2-16 Insert Battery Pack in Charging Pocket

Lower the battery pack straight into the battery charger pocket and push it down firmly. Do not 'slam' the battery into the charging cup or drop it into the cup.

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



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

External Power Supply for MX5X and Cradle

The MX5X DC adapter can be plugged into either of the D26 pin connectors on the bottom of the MX5X.

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



Figure 2-17 AC/DC 12V Power Supply

Note: When the MX5X is receiving power through a cradle connected to external power the Battery Charge LED on the MX5X is green.

Cradles

MX5 cradles are not approved for use in Hazardous Locations.

Important: The cradles are not designed to secure an MX5X with a protective padded case. The vehicle cradle is not designed to secure an MX5X with a trigger handle. The desktop cradles will secure mobile device's with handstraps or trigger handles.

MX5 docking cradles give the MX5X the ability to communicate with a host computer and other devices. In addition, using wall AC adapters or DC/DC converters, the cradle charges the main battery. The MX5X can be either On or in Suspend mode while in the cradles.

LXE offers three desktop cradles and one vehicle cradle:

<p>Standard Desktop Cradle requires AC power before main battery charging can commence. This cradle does not have an active LED on the front housing. MX5A002DESKCRADLE</p>
--

<p>Enhanced Desktop Cradle requires AC power before main battery charging can commence. It will charge both the main battery in the MX5X and another MX5X Battery Pack at the same time. MX5A003EDESKCRADLE</p>
--

<p>Enhanced Desktop Cradle with Ethernet Port requires AC power before main battery charging and host/client communications can commence. It will charge both the main battery in the MX5X device and another main battery pack at the same time. MX5A004ETHDESKCRADLE</p>

<p>Vehicle Mount Cradle requires AC/DC power before main battery charging can commence. MX5A001VMCRADLE</p>
--

Note: LXE offers a device similar in appearance to the MX5CE device – the LXE MX5 Pocket PC 2002 device. All MX5 cradles can be used by the MX5s. The Enhanced Desktop Cradle, developed specifically for the MX5X device, cannot be used by the MX5 Pocket PC device.

Cradle COM port and power cables are available from LXE. The RS-232 connector is located on the back of the cradle. When the MX5X is properly docked, the COM 1 RS-232 interface connects with the DA9 RS-232 port in the cup at the front of the cradle. The cup at the back of the desktop cradles accept a single Battery Pack for charging.


The Ethernet port is on the Enhanced Desktop Cradle with Ethernet Port.

Tethered Barcode Scanner Data Entry Using the MX5 Cradle

The MX5X supports an accessory barcode label reading device (a tethered scanner) connected to the serial port on a vehicle cradle. Keypad data entries can be mixed with barcode data entries. Any tethered scanner that decodes the barcode internally and outputs an RS-232 data stream may be used. It sends the data to the MX5X in ASCII format.

The serial port parameters may need to be changed to match the parameters of the tethered scanner.

When a tethered scanner is connected to the serial port on a vehicle cradle, the MX5X scanner must be configured as follows:

1. Start | Settings | Control Panel | Scanner | Main | either Port 1 or Port 2
2. Select COM1 External on one of the ports. The tethered scanner must be connected to the DB9 port on the vehicle cradle. The cradle must be powered by an alternate AC or DC power source to enable tethered scanner use.
3. If the tethered scanner is powered by the mobile device, enable Power Output in  | Settings | Control Panel | Handheld | Comms tab.

See Also: Tethered Scanners (Optional).

The *MX5 Cradle Reference Guide* contains cradle installation and technical information.



Chapter 3 System Configuration

Introduction

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

Your MX5X operating system may be Windows CE .NET 4.2 or Windows CE 5.0. The MX5X operating system is displayed on the Desktop as Windows CE .NET or Windows CE. This is the factory default value for the Desktop Display Background.

This chapter presents information and procedures that are common to both CE versions unless otherwise noted.

Windows Operating System



For general use instruction, please refer to commercially available Windows CE .NET 4.2 user's guides or Windows CE 5.0 user's guides or the Windows on-line Help application installed in the mobile device.

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

Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX5X and its Windows CE environment.

2.4 GHz Network Configuration

All 2.4GHz network configuration is included in *Chapter 5 – Wireless Network Configuration*.

Installed Software

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

When you order a mobile device you receive the software files required by the separate programs needed for operation and wireless communication. The files are loaded by LXE and stored in folders in the mobile device. This section lists the contents of the folders and the general function of the files. Files installed in the mobile device are specific to the intended function of the mobile device.

Files installed in each mobile device configured for a wireless network environment contain wireless client specific drivers – the drivers for each type of client are specific to the manufacturer (e.g. Cisco, Symbol, Summit) for the clients installed in the RF environment and are not interchangeable.

Software Load

The software loaded on the MX5X computer consists of Windows CE .NET 4.2 or Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Operating System -- Full Operating System License: Includes all operating system components, including Windows CE 5.0 or CE .NET 4.2 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
- Wavelink Avalanche (Option)
- LXE AppLock (Option)
- Java (Option) -- Java executables and browser components are handled by the Java option (when installed).
- Terminal Emulation (Option)
- RFTerm (VT220, TN5250, TN3270). Runs automatically at the conclusion of each reboot (if installed).
- LXE API Routines (see *Accessories* for the LXE SDK Kit part number)

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

Software Applications

The following applications are included:

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

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

Optional

AppLock (Option)

Installed by LXE. 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.

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. Requires Windows CE 5 operating system.

The mobile device cannot be upgraded to CE 5.0 using the Wavelink / eXpress Config application. The device must be returned to LXE for upgrading or an LXE Field Service Engineer can be dispatched to upgrade the device. Contact your LXE representative for assistance.

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 MX5X has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. The designation of the mobile device to the Avalanche Manager is LXE_MX5X.

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.

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

Terminology may appear different, based on your installed version:

Avalanche Manager may be shown as the Avalanche Mobility Center Console

Desktop



For general use instruction, please refer to commercially available Windows CE .NET 4.2 or Windows CE 5.0 user's guides or the Windows on-line Help application installed in the mobile device.

Note: Whenever possible, use the AC power adapter with the MX5X to conserve the main battery and to ensure the backup battery is charged.

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

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

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

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

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








Desktop Option	Icon	Function
My Computer (CE .NET 4.2) My Device (CE 5.0)		Access files and programs.
Recycle Bin		Storage for files that are to be deleted.
Internet Explorer		Connect to the Internet/intranet (requires a wireless transmitter and Internet Service Provider – ISP enrollment is not available from LXE).
Transcriber		Enter text using the stylus on the touch screen.
Wireless Client Setup Icon (Summit, Cisco, Symbol)		Used for configuring wireless client for network security settings. Note that only one client can be used at a time, e.g. if the Summit client icon is present, the Cisco client icon is not present.
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.

Figure 3-1 Desktop Icons

My Computer Folders (CE .NET 4.2)

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
Profiles	Network user profiles	Yes
Program Files	Applications	No
System	Internal ATA Card (64Meg total, 28 Meg free for User Applications)	Yes
Temp	Location for temporary files	No
Windows	Operating System in ROM	Yes

Folders Copied at Startup

The following folders are copied on startup:

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

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

The following folders are ***NOT*** copied on startup:

- Windows\AppMgr
- Windows\Recent
- Windows\Startup

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

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

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

My Device Folders (CE 5.0)

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 (CAB file storage)	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. Note that there can be only one wireless client installed at a time. The client driver configuration utility chosen is based on the type of installed wireless client card (Cisco, Summit, Symbol).

Access:  | Programs

Cisco Requires Windows CE .NET 4.2 operating system.	Set Cisco client / network parameters. (See <i>Chapter 5 Wireless Network Configuration</i> for instruction.)
Symbol Requires Windows CE .NET 4.2 operating system.	Tap the Network icon in the toolbar to set up the Symbol client (See <i>Chapter 5 Wireless Network Configuration</i> for instruction.)
Summit	Set Summit Client / network parameters. (See <i>Chapter 5 Wireless Network Configuration</i> for instruction.)
Communication	Stores Network communication options
Get Connected	Run this command after setting up a connection
Remote Desktop	Displays MX5X file structure on a remote desktop monitor
Terminal	Log on to a Windows Terminal Server
Microsoft File Viewers	View downloaded files (see Note)
Excel Viewer	View Excel 97 (and later) documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
PowerPoint Viewer	View PowerPoint files
Word Viewer	View Word 97 (and later) 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
iRescue	Data backup and recovery utility
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Windows Explorer	File management program
Transcriber	Enter data using the stylus on the touch screen.

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

Communication

Access:  | Programs | Communication

Note: Some communication menu options require an external modem connection to the MX5X. Modems are not available from LXE nor supported by LXE.

ActiveSync

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, USB or the infrared port on the MX5X. Refer to *ActiveSync Processes* later in this guide.

Note: ActiveSync does not transmit through the IR port in vehicle cradles. It will transport through the IR port of the MX5 desktop cradles.

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

Synchronizing from the MX5X

You must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device. Refer to *ActiveSync Processes* later in this guide.


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

Note: If you have a wireless LAN card, you can synchronize remotely from your device.

Tap Sync to connect and synchronize. View synchronization status.

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


Tap Stop to stop synchronization.


Tap  | Help for context-sensitive help.

Get Connected

Get Connected is used to initiate a hardwired connection to a host.

The default connect setup is USB direct connect.


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

The wireless link is made using  | Run. Tap the Browse button and browse to the Windows folder. Select `repllog.exe` and tap the OK button. The Run text box reappears with `\windows\repllog` in the text box.

Before pressing Enter, type a backslash (/) and `remote` in the Run text box. For example: `\windows\repllog / remote`

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

Remote Desktop Connection

Access:  | Programs | Communication | Remote Desktop Connection

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

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

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

Command Prompt


Access:  | Programs | Command Prompt



Figure 3-2 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 MX5X inbox and a desktop inbox. Refer to *ActiveSync Processes* in Chapter 3 of this guide.

Internet Explorer

Access:  | Programs | Internet Explorer


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

Media Player

Access:  | 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. Tap the <?> button to access Media Player 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.

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

Taskbar

Access:  | Settings | Taskbar and Start Menu

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 to make the Start button appear.

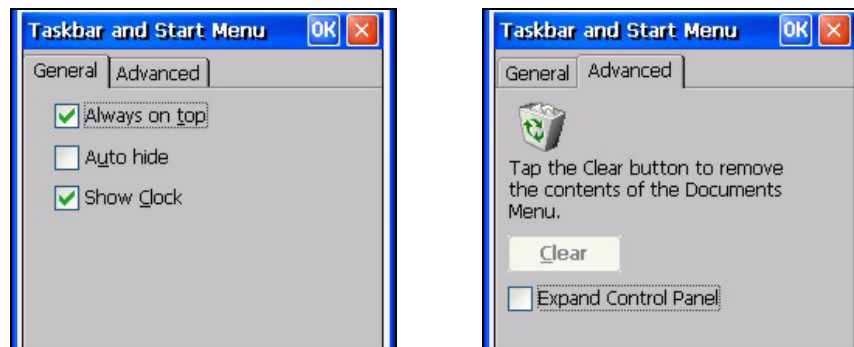


Figure 3-3 Taskbar and Start Menu Properties

Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the Settings | Control Panel menu option.

Clear Contents of Document Folder

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

Control Panel Options

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

Getting Help

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

Option	Function
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility. See <i>Chapter 6 – AppLock</i> for details.
Audio	Set volume parameters and assign sound wav files to CE events. Adjust the volume, record gain, and sidetone for headphone, software and microphone. Set volume for Bay Digital, CRMA Radio and Mixer.
Aironet Client Utility	Set the parameters for a Cisco client. (See <i>Chapter 5 Wireless Network Configuration</i> for instruction.) Requires Windows CE .NET 4.2 operating system.
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, window/menu appearance parameters and set backlight properties and timers.
Handheld	Displays hardware and software details. Tabs are Versions, Comms, Radios, Misc. Enable or disable the touch panel (see Handheld Properties Misc).
Input Panel	Select the current key / data input method.
Internet Options	Set General, Connection, Security and Advanced options for Internet connectivity. CE 5 version added Privacy and Popups options.
Keyboard	Set key repeat delay and key repeat rate.
Mouse	Set the double-click sensitivity for stylus taps on the touch screen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set MX5X owner details (name, phone, etc) and Notes. Enter Network ID for the device – user name, password, domain. Includes option to display owner identification at power-on.
Password	Set MX5X user access password properties.

Option	Function
PC Connection	Control the connection between the MX5X and a local desktop or laptop computer.
Power	Set Power scheme properties. Review battery status and properties..
Regional Settings	Set appearance of numbers, currency, time and date based on regional and language settings.
Remove Programs	Remove user installed programs in their entirety.
Scanner	Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. See section titled <i>Determine Your Scanner Software Version</i> .
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel. Enable or disable the touch panel (see Handheld Properties Misc).
Symbol	Set the parameters for a Symbol client. (See <i>Chapter 5 Wireless Network Configuration</i> for instruction.)
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description.
Terminal Server Client Licenses	Assign a stored Terminal Server Client license to the device.

Accessibility

Access:  | Settings | Control Panel | Accessibility



Figure 3-4 Accessibility Options

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.

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 computers intended to be used as dedicated, single or multiple application devices. In other words, only the application or feature(s) specified in the AppLock configuration by the Administrator are available to the 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 also 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.

Audio

Access:  | Settings | Control Panel | Audio

Set volume parameters and assign sound wav files for operating system events. Adjust the volume, record gain, and sidetone for headphone, software and microphone. Set volume for Bay Digital, CRMA Radio and Mixer.

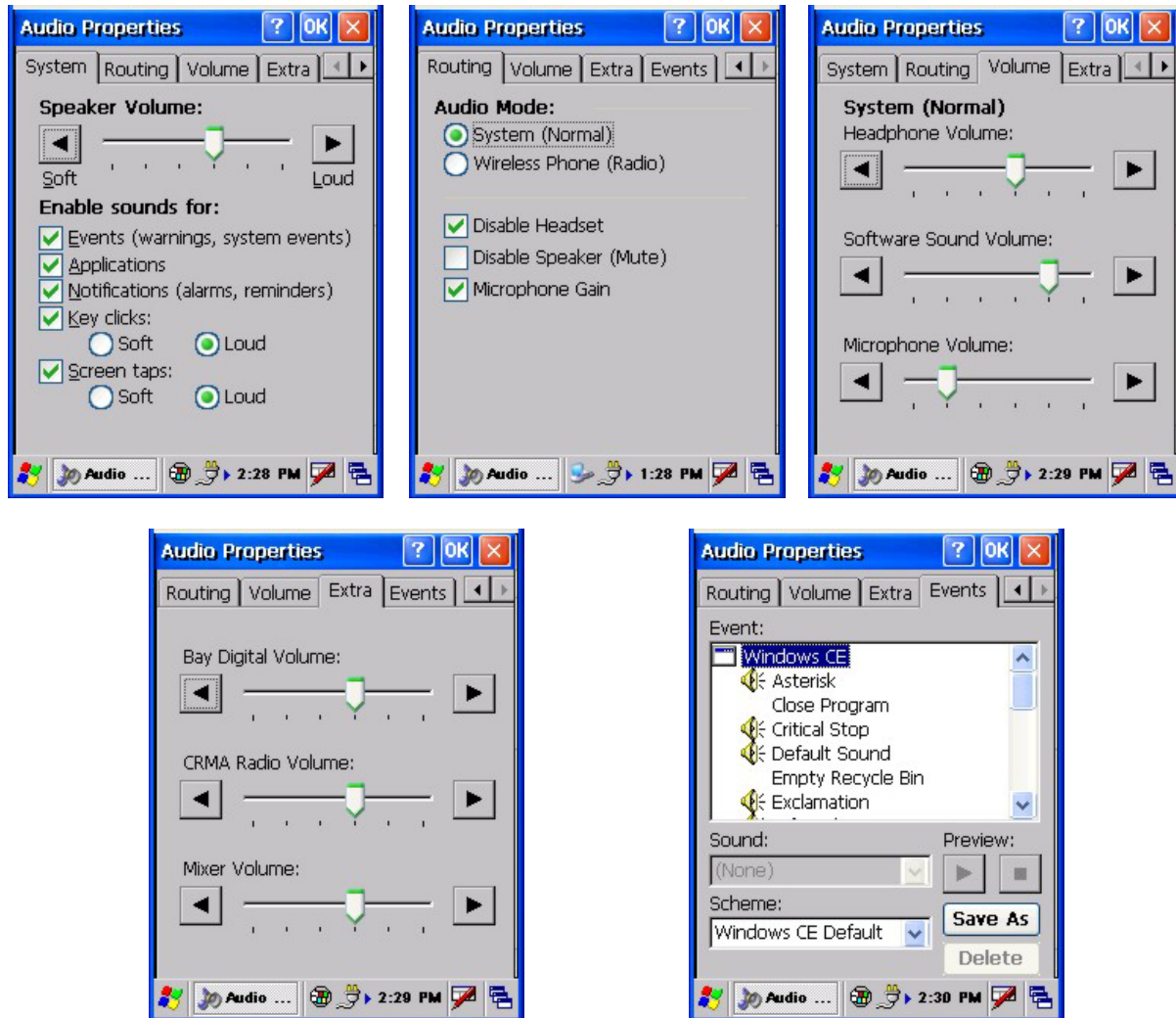


Figure 3-5 Audio Properties

Factory Default Settings	Bootloader	
	Version 1.01	Version 1.02
System		
Speaker Volume	Loud	Loud
Events	Enabled	Enabled
Applications	Enabled	Enabled
Notifications	Enabled	Enabled
Key Clicks	Loud	Loud
Screen taps	Loud	Loud
Routing		
System (Normal)	Enabled	Enabled
Wireless Phone (Network card)	Disabled	Disabled

Factory Default Settings	Bootloader	
	Version 1.01	Version 1.02
Headset	Disabled	N/A
CRMA Radio	Disabled	N/A
Exp. Bay	Unhighlighted Enabled	N/A
Disable Headset	Enabled	1
Disable Speaker (Mute)	Disabled	Enabled
Microphone Gain	Disabled	Enabled
Volume		
Headphone	60%	60%
Software	80%	80%
Microphone	60%	60%
Extra Volume		
Bay Digital	60%	60%
CRMA Radio	60%	60%
Mixer	60%	60%
Events		
Scheme	Windows CE Default	Windows CE Default

Note: Bluetooth access, Bluetooth modules and Bluetooth Manager are not supported by LXE.

Certificates

Access:  | Settings | Control Panel | Certificates

Manage digital certificates used for secure communication.


Note: It is important that all dates are correct on the mobile devices when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.



Figure 3-6 Digital Certificates

Lists the Stored certificates trusted by the MX5X user. These values may change based on the type of wireless security resident in the client, access point or the host system.

Date/Time

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

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

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

Note: Date and time is reset to the default value each time the MX5X is rebooted.

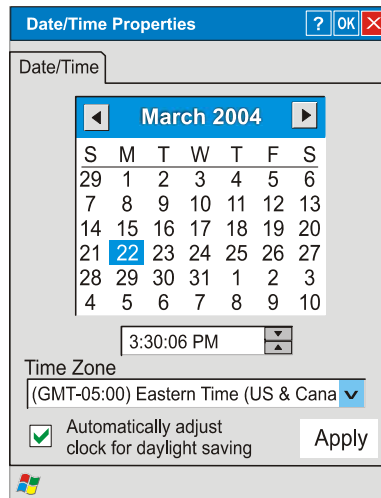


Figure 3-7 Date/Time Properties

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

Dialing

Access:  | Settings | Control Panel | Dialing

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



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

Figure 3-8 Dialing Properties

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
Backlight	
Battery Auto Turn Off	Enabled
Idle Timer	1 minute
External Auto Turn Off	Enabled
Idle Timer	10 minutes

Display Properties

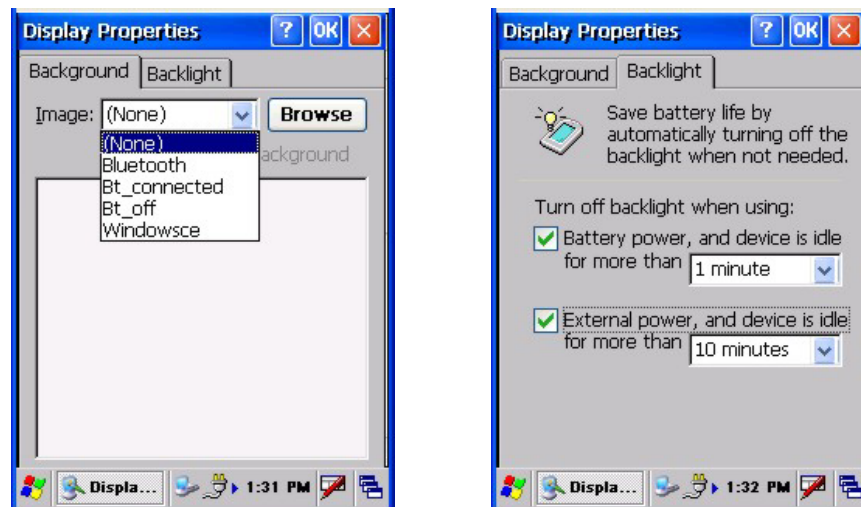


Figure 3-9 Display Properties

Background

There is no 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.

Backlight


Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. When the backlight timer expires, the screen backlight is dimmed not turned off and the keypad backlight is turned off. Default values are 1 minute for Battery power and 10 minutes for External power.

Handheld

Access:  | Settings | Control Panel | Handheld

Displays hardware, communications, versions and WLAN client details.

How to Disable Touch and / or Calibration upon Cold Reset

Access:  | Settings | Control Panel | Handheld | Misc tab


Use this option to disable the touch panel. It can also be used to disable the touch screen calibration configuration during a Cold Reset. When touch is disabled, the keypad must be used for input. The Input Panel cannot be used.

Disable Touch Panel and Calibration

Access: My Computer | System

Create a file on the CF card (My Computer\System folder) named DisableTouchScreen.dat. If this file is present on the CF card, the touch screen will be disabled, and calibration will NOT be requested upon a cold reset.

Disable Touch Panel Only

Access:  | Settings | Control Panel | Handheld | Misc tab

To just disable the touch panel (calibration still required upon cold reset), enable (tap) the Touch Panel Disabled checkbox on the Misc tab in the Handheld Properties Control Panel.

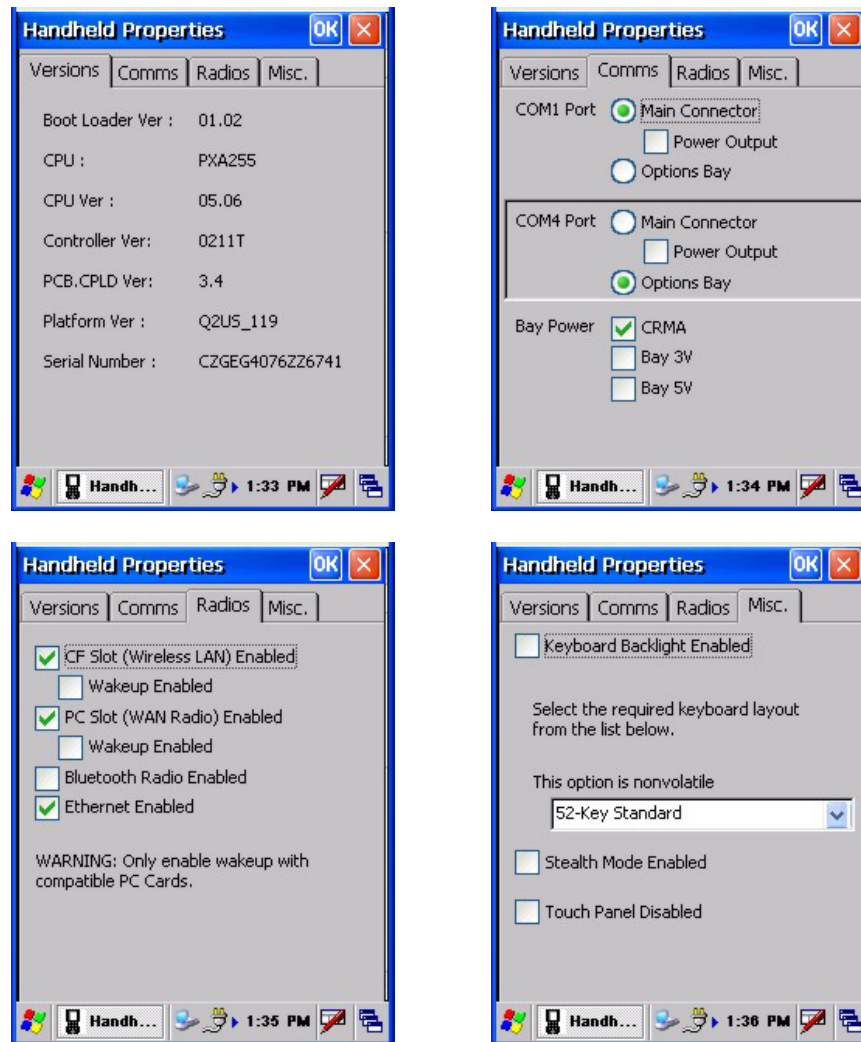
When checked, the touch panel is disabled. When touch is disabled, the keypad must be used for input. The Input Panel cannot be used.

How to Re-enable Touch and / or Calibration upon Cold Reset

Access: My Computer | System

To enable Touch Panel and Calibration, delete the file named DisableTouchScreen.dat on the CF card (My Computer\System folder). When this file is present on the CF card, the touch screen is disabled, and calibration does not occur after a cold reset.

To enable the Touch Panel only, uncheck the Touch Panel Disabled checkbox on the Misc tab in the Handheld Properties Control Panel (Start/Settings/Control Panel/Handheld/Misc tab).

Bootloader Version 1.02**Figure 3-10 Handheld Properties – Version 1.02****Versions tab**

Bootloader, CPU type, CPU, Controller, PCB.CPLD, Platform versions. Mobile device serial number.

Comms tab

Comms	Default
COM 1 Port	Main Connector enabled Disabled: Power Output for Main Connector, Options Bay
COM 4 Port	Main Connector enabled Disabled: Power Output for Main Connector, Options Bay
Bay Power	Disabled: CRMA, Bay 3V, Bay 5V

Radios tab

Parameter	Default
CF Slot Enabled	Enabled (checkmark)
CF Slot Wakeup Enabled	Disabled (blank)
PC Slot Enabled	Enabled (checkmark)
PC Slot Wakeup Enabled	Disabled (blank)
Bluetooth Radio Enabled	Disabled (blank) [see Note]
Ethernet Enabled	Enabled (checkmark)

Note: Bluetooth access, modules and Bluetooth Manager are not supported by LXE.

Misc tab

Parameter	Defaults
Keyboard Backlight Enabled	Enabled (checkmark)
Nonvolatile option	52-key Standard Options: 52-key Phone, 52-key MultiKey
Stealth Mode Enabled	Disabled (blank) [see Note]
Touch Panel Disabled	Disabled (blank) [see Note]

Note: See previous section titled How To Disable Touch and / or Calibration upon Cold Reset and How To Enable Touch and / or Calibration upon Cold Reset.

Bootloader Version 1.01
Versions tab

Bootloader, CPU type, CPU, Controller, PCB.CPLD, Platform versions. Mobile device serial number.

Comms tab

Comms	Defaults
COM 1 Port	Main Connector enabled Disabled: Power Output for Main Connector, Options Bay
COM 4 Port	Options Bay enabled Disabled: Main Connector, Power Output for Main Connector,
Bay Power	CRMA Disabled: Bay 3V, Bay 5V

Radios tab

Parameter	Defaults
CF Slot Enabled	Enabled (checkmark)
CF Slot Wakeup Enabled	Disabled (blank)
PC Slot Enabled	Enabled (checkmark)
PC Slot Wakeup Enabled	Disabled (blank)
Bluetooth Radio Enabled	Disabled (blank) [see Note]
Ethernet Enabled	Enabled (checkmark)

Note: Bluetooth access, modules and Bluetooth Manager are not supported by LXE.

Misc tab

Parameter	Defaults
Keyboard Backlight Enabled	Disabled
Nonvolatile option	52-key Standard Options: 52-key Phone, 52-key MultiKey
Stealth Mode Enabled	Disabled (blank) [see Note]
Touch Panel Disabled	Disabled (blank) [see Note]

Note: See previous section titled *How To Disable Touch and / or Calibration upon Cold Reset and How To Enable Touch and / or Calibration upon Cold Reset.*

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

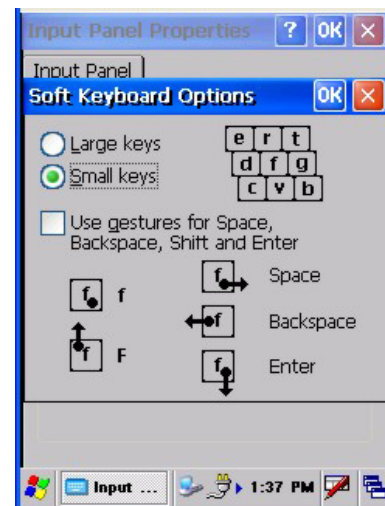
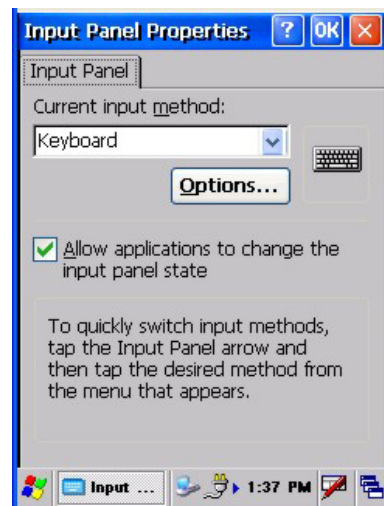



Figure 3-11 Input Panel

Use this option to make the Input Panel or the physical keypad primarily available when entering data. When new key maps are added to the registry, they will appear in the Input Method dropdown list.

Tap the Input Panel icon in the taskbar to toggle the on-screen Keyboard on and off.

Internet Options

Access:  | Settings | Control Panel | Internet Options

Set MX5X user options for internet connectivity.

Windows CE .NET 4.2 Defaults

Factory Default Settings	
General	
Start Page	http://www.msn.com/
Search Page	search.msn.com
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
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
Advanced	
Display web images	Enabled
Play web sounds	Enabled
Enable web scripting	Enabled
Display script error note	Disabled
Underline links	Never

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

Windows CE 5.0 Defaults

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

Factory Default Settings	
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

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

Keyboard

Access:  | Settings | Control Panel | Keyboard Icon

Set key repeat delay and key repeat rate.

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow

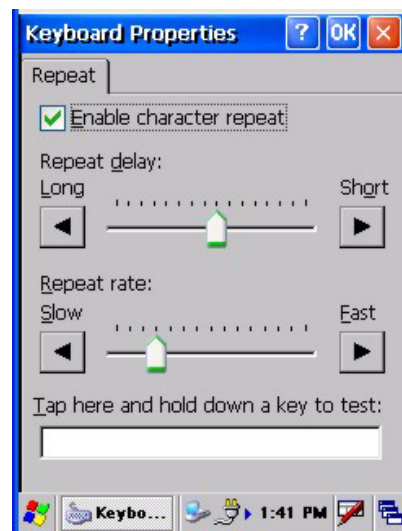


Figure 3-12 Keyboard Properties

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


These values do not affect virtual keyboard (Input Panel) taps.

Mouse

Access:  | Settings | Control Panel | Mouse



Set the double-click sensitivity for stylus taps on the touch screen.

Network and Dialup Connections

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

Create a dialup, direct, Ethernet or VPN connection on the MX5X.

Create a Communication Option

1. On the MX5X, 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, tap Connection. Then tap New...
3. Give the new connection an appropriate name (IR @ 9600, etc.). Tap the Direct Connection control. 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 disable Wait for dial tone, since a direct connection will not have a dial tone. Set the Cancel parameter (default is 2 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 button.
11. Select the new connection. Tap OK twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the MX5X with the appropriate cable.
14. Tap 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 MX5X 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

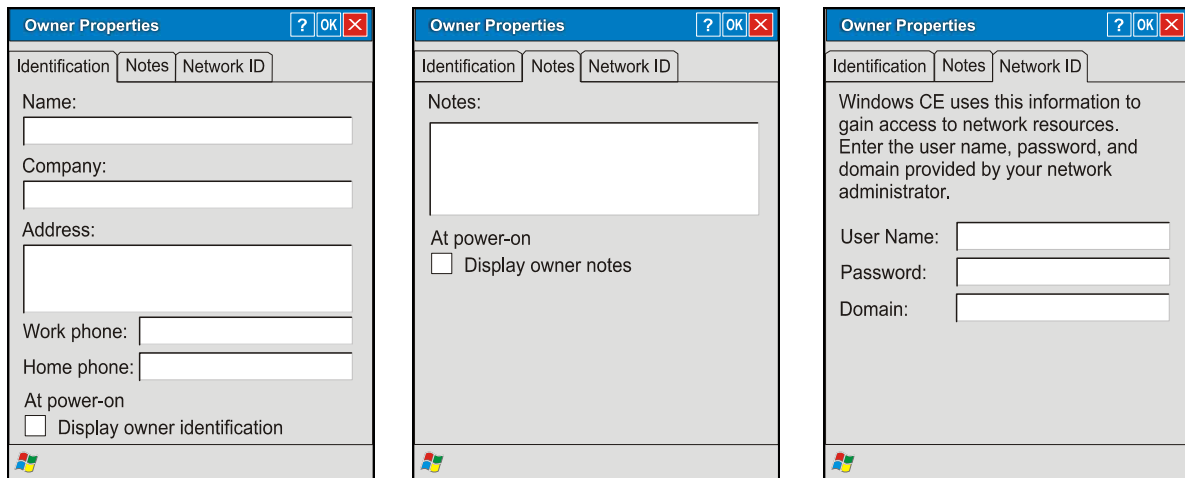


Figure 3-13 Owner Properties

There is little change from general desktop PC Owner Properties display. Enter the information and tap the OK box to save the changes. The changes take effect immediately.

Password

Access:  | Settings | Control Panel | Password Icon

Set MX5X access/power up password properties.

Factory Default Settings	
Password	Blank
At Power On	Disabled
Screensaver	Disabled

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

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

Tap the Enable password protection at power-on checkbox to set whether the user types a password at Power On.

New in Windows CE 5:

Tap the Enable password protection for screen saver checkbox to set whether the user types a password at Power On.

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.

PC Connection

Access:  | Settings | Control Panel | PC Connection

Control the connection between the MX5X and a nearby desktop/laptop computer.

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

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

Tapping Change Connection displays a list of configured ActiveSync connections.

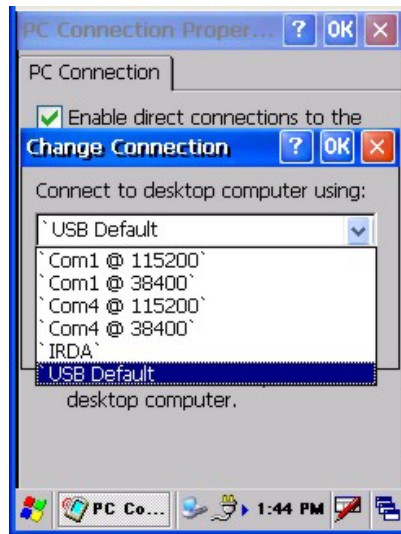


Figure 3-14 PC Connection / Change Connection

Please refer to the Backup MX5X Files section later in this chapter for parameter setting recommendations.

Power

Access:  | Settings | Control Panel | Power

Set Power Off, Backlight properties. Review battery status and details. Please refer to *Chapter 2 Physical Description and Layout* section titled *Power Modes*.

Factory Default Settings		
Status	Main Battery Power Gauge	
Power Schemes		
Battery	Suspend	3 minutes
AC Power	Suspend	5 minutes

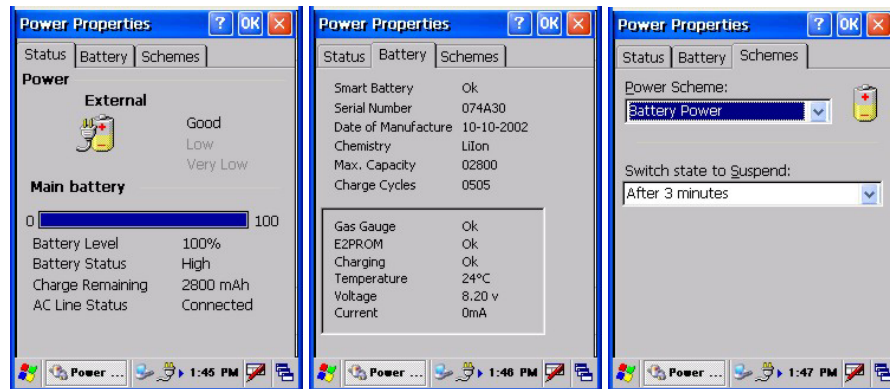


Figure 3-15 Power Properties

Status

The Status tab shows the status and the percentage of power left in the main battery (removable). The listed values cannot be changed by the user. Backup battery information is not available.

Battery

The Battery tab displays technical information (serial number, charge cycles remaining, etc.) about the main battery pack. Backup battery information is not available.

Schemes

The Schemes tabs allows the user to set the Suspend timers when the mobile device is running on Battery power or AC power. Adjust the settings and tap the OK box to save the changes. 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.

Factory Default Settings	
Regional Setting	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	\$123,456,789.00 pos / (\$123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long


New in Windows CE 5:

In addition to the above settings, the user can set the user interface language and the default input language.

Factory Default Settings	
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US

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

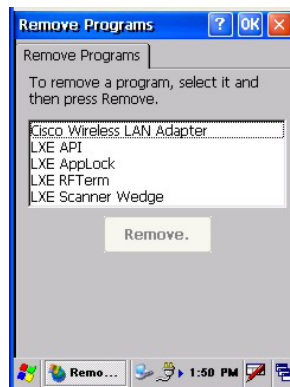


Figure 3-16 Remove/Delete User Installed Programs

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.

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 MX5X 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 MX5X 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, go to Settings | Control Panel | Handheld | Versions tab.

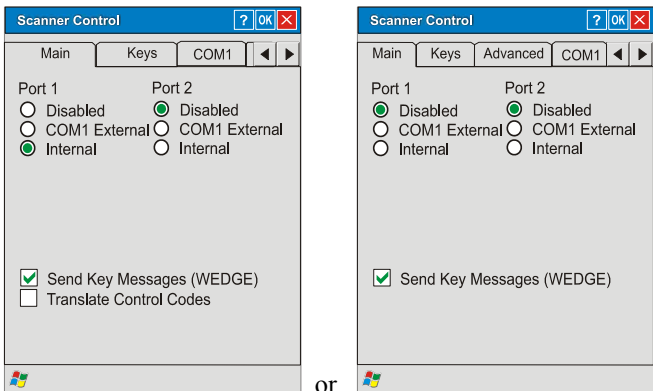
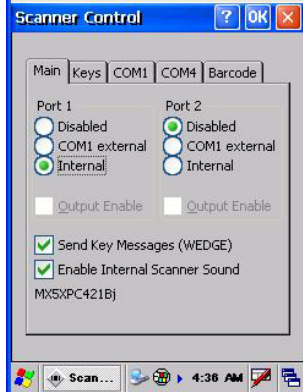
If the Scanner Control panel looks like this	Go to
	<p>This chapter, this section titled Scanner</p>
	<p>Chapter 4 Scanner</p>

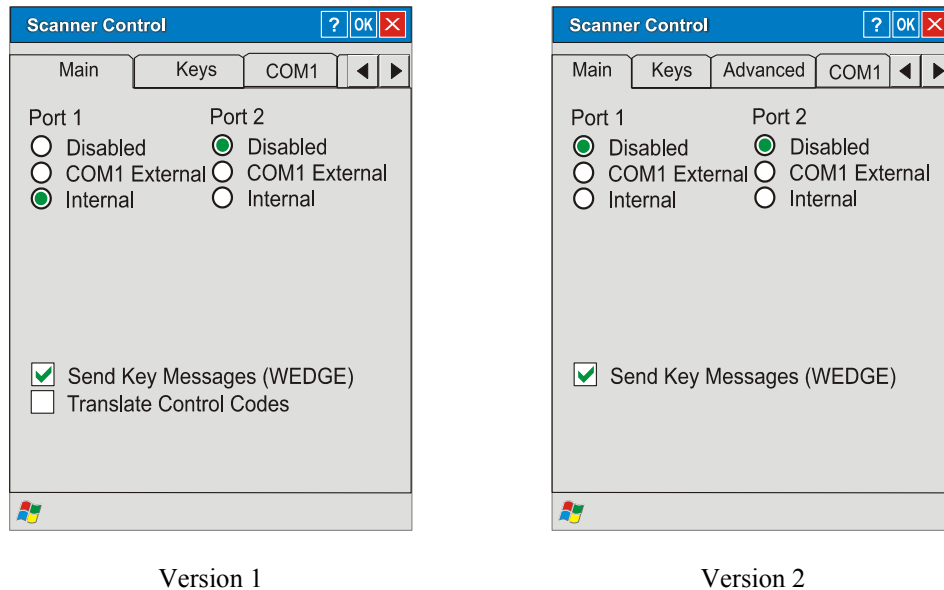
Figure 3-17 Determine Your Scanner Software Version

Factory Default Settings

Factory Default Settings	
Main	
Port 1	Disabled
Port 2	Disabled
Send key messages WEDGE	Enabled
Translate Control Codes	Disabled
Keys	
Left	Enter
Right	Enter
Advanced (Version 2)	
Translate	Disabled
Strip Leading	0 characters
Strip Trailing	0 characters
Prefix	Disabled
Suffix	Disabled
COM Ports (COM1, COM4)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	COM1 : 8 COM4 : greyed out

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

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

Main

Version 1

Version 2

Figure 3-18 Scanner Properties / Main Tab

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

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.

Version 1

If Translate Control Codes 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 Control Codes is not checked and Send Key Messages is checked, CTRL codes are passed through in Block mode.

See Also: Appendix C Reference Material section titled ASCII Control Codes.

Keys

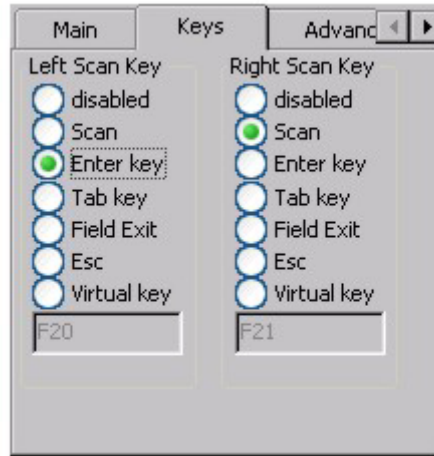


Figure 3-19 Scanner Properties / Keys Tab

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

Disabled	When either scan key is set to Disabled, it does nothing when pressed.
Scan	When set to Scan the integrated scanner is activated. If no integrated scanner is present, the Scan selection is greyed out.
Enter	When set to Enter, both the Enter key and the (Scan button) / Enter key perform the same function.
Tab	When set to Tab, both the Tab key and the (Scan button) / Tab key perform the same function.
Field Exit	<i>IBM TN5250 specific keypad only.</i> The left Scan key can be programmed as a Field Exit key.
Esc	When set to Esc the Scan key press halts the current function.

Change a Virtual Key (F20 or F21) Value

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

Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

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

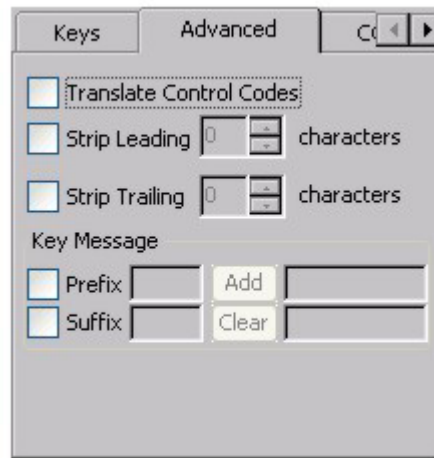
Advanced


Figure 3-20 Scanner Properties / Advanced tab

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

The title in the group box reflects the current mode. If you are in Block mode, the title of the group box is Block. If you are in Key Message mode, the title of the group box is Key Message.

Translate Control Codes

If Translate Control Codes 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 Control Codes is not checked and Send Key Messages is checked, CTRL codes are passed through in Block mode.

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*.

See Hat Encoding and Decimal-Hexadecimal Chart in Appendix C Reference Material.

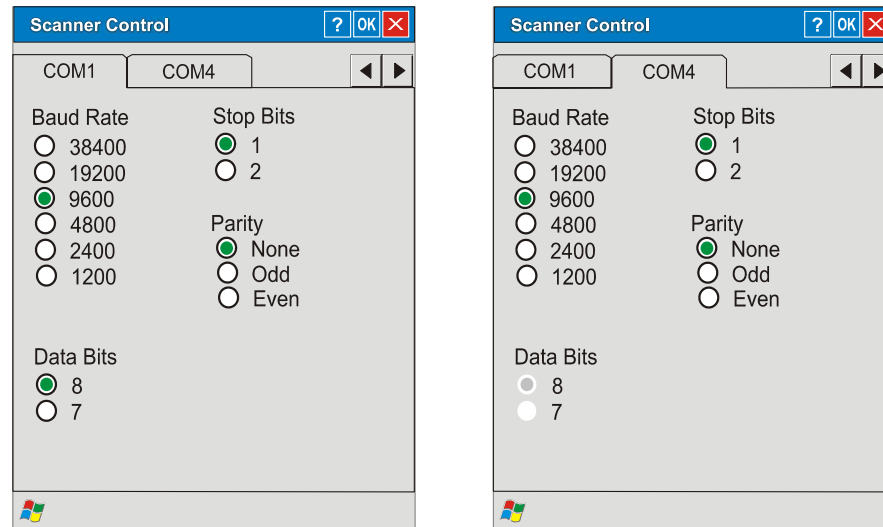
COM Ports


Figure 3-21 Scanner Properties / COM Port Settings

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


The COM 1 display contains the same parameters as the COM 2 and COM 3 Tab. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Note: Neither COM1 nor COM4 support 5V switchable power on Pin 9 for tethered scanners.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows folder, 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 MX5X is a single 2700 Hz beep, and a bad scan sound is a double beep.

Storage Manager

Access:  | Settings | Control Panel | Storage Manager

Note: *Storage Manager is not available until a storage device is installed in the MX5X.*

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

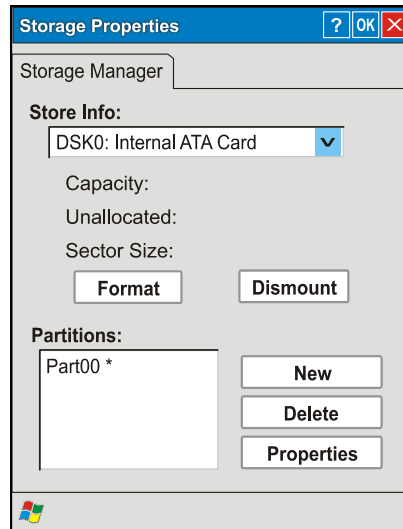


Figure 3-22 Storage Properties

On-line help is available for this option.

Topics available are:

- [Manage storage devices](#)
- [Manage disk partitions](#)
- [Creating a new partition](#)
- [Advanced partition features](#)

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

This menu option is not available in all versions.

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

Stylus

Access:  | Settings | Control Panel | Stylus

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

Double Tap

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

Calibration

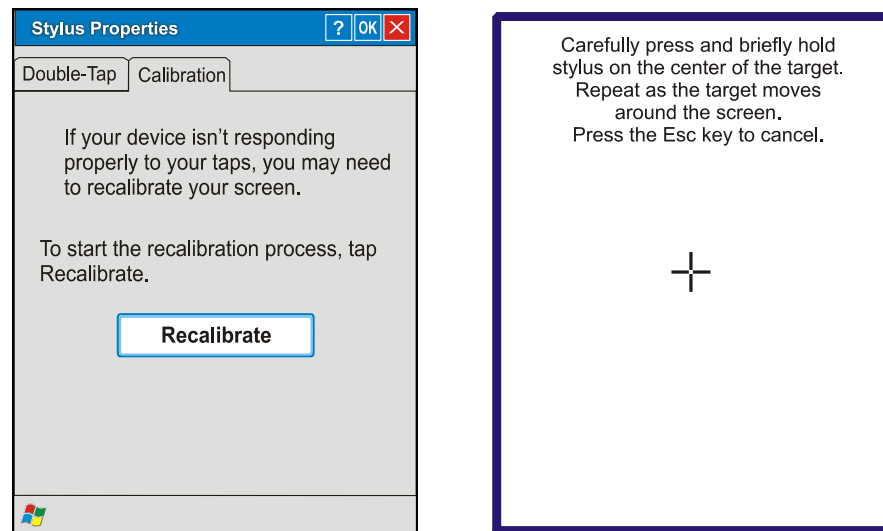


Figure 3-23 Stylus Properties / Calibration Start / Calibration Begin

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

Factory Default Settings	
General	N/A
Memory	Middle of Memory Bar
Device Name	Windows CE
Device Description	Windows CE Device
Copyrights	N/A

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. The name of the installed wireless card is listed in the dropdown list. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. Hence, a system with 64 MB may only report 35 MB memory, since 29 MB is used up by the Windows CE operating system. This is actual DRAM memory, and does not include internal flash or the internal ATA card used for storage.

Memory

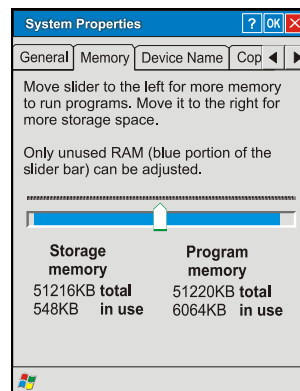


Figure 3-24 System / Memory

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 MX5X 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.

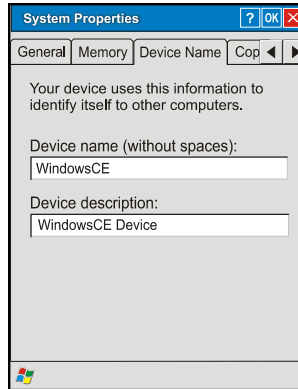
Device Name

Figure 3-25 System / Device Name

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

Copyrights

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

Compact Flash Cards, CAB Files and Programs

CF Compact Flash Card | Flash Card

The CF 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 a cold boot, the contents of any CAB files (for API, drivers, etc.) are automatically unpacked and then restarted after the subsequent warm boot.

Access Files on the CF Card

Tap the My Computer or My Device icon then the System folder.

Note: Perform a warm reset when exchanging one CF card for another.

CF Files

Persistent Storage Memory is not available on the MX5X. Instead, a Flash card is used for permanent storage of the LXE drivers and utilities. It is also used for registry content back up. The CF card is located in the socket under the main battery pack.

It is important that all CAB files on the card be given Read-Only attributes. On the MX5X, when a read-only CAB file is unpacked, it is not deleted.

The following files are included on every MX5X CF card:

WEDGE.CAB	Cab file containing the LXE scanner driver and control panel for the MX5X.
API.CAB	CAB file containing the LXE API for the MX5X device.

The following CAB files are optional and may or may not be present:

SUMMIT.CAB	Summit client driver and utilities.
SYMBOL.CAB	Symbol client driver and utilities.
CISCO.CAB	Cisco client driver and utilities.
RFTERM.CAB	LXE RFTerm terminal emulation application.
JAVA.CAB	Java application.
APLOCK.CAB	LXE AppLock program.
LXE_MX5X_ENABLER.CAB	Wavelink Avalanche Enabler
BT.CAB (See Note)	Bluetooth Manager program (CE .NET 4.2 only)

Note: Bluetooth Manager, Bluetooth service or options are not available for all MX5X devices or in all MX5X software releases. Bluetooth access, modules and Bluetooth Manager on the MX5X are not supported by LXE.

Bluetooth Manager (CE .NET 4.2 only)

Note: Bluetooth Manager, Bluetooth service or options are not available for all MX5X devices or in all MX5X software releases. Bluetooth access, modules and Bluetooth Manager on the MX5X are not supported by LXE.

Access: Taskbar icon

Set the parameters for a Bluetooth radio. The Bluetooth Manager must be installed by doubletapping the Bluetooth CAB file and then warm resetting the device. The Bluetooth icon is placed in the taskbar.

Factory Default Settings	
All Found Devices	Untrusted

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

API Calls

Refer to *Accessories* for the LXE MX5 SDK part number.

The LXE specific API calls for the MX5X are included in the LXE *CE API Programming Guide*.

The guide lists only the LXE-specific API calls and details which calls from the standard LXE API are and are not supported on the MX5X. It is intended as an appendix to the standard Microsoft Windows CE API documentation. The APIs detailed in the Programming Guide are included in the file LXEAPI.DLL..

LXE-specific API calls and registry settings, for LXE devices running Windows CE .NET 4.2 and CE 5.0, cover the following:

- Battery
- PCMCIA
- Power Management
- Scanner
- Serial Ports
- Version Control
- Miscellaneous

ActiveSync / Get Connected Process

Introduction

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

See Also: Section titled *ActiveSync*.

A partnership between a PC and the MX5X must be established using serial RS-232 or USB connection between the PC and the MX5X. When more than one PC will be synchronizing with the MX5X, each PC will need it's own partnership established. See section titled *Initial Install* for the procedure.

After the partnership has been established with the MX5X and the host computer, ActiveSync can be performed over serial, USB, wireless, InfraRed, or ethernet.

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your PC with the MX5X and vice versa. Synchronization compares the data on your MX5X with your 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.
- 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 MX5X, the data appears to transfer, but it is ignored by the MX5X 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 MX5X and the desktop/laptop (PC). Once a relationship has been established, tap Start | 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 Start | 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 cable your mobile device to the PC.

Serial Connection

Tap the  | Settings | Control Panel | PC Connection on the MX5X. Tap the Change Connection button. From the popup list, choose

COM 1 @ 115200


Note: The default is USB Default.

This will set up the MX5X to use COM 1. Tap OK and ensure the check box for Enable direct connections to the desktop computer is checked.

Select Start | Settings | Control Panel | Scanner and ensure the integrated laser scanner is set to a port that is NOT the same as the Get Connected port (COM 1).

Tap OK to return to the Control Panel.

USB Connection


Tap the  | Settings | Control Panel | PC Connection on the MX5X. Tap the Change Connection button. From the popup list, choose

USB Default


This will set up the MX5X to use the USB port. 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.

Connect – Initial Install Process

Connect the correct** cable to the PC (the host) and the MX5X (the client). Tap the  | Programs | Communication | Get Connected on the MX5X.

Note: ActiveSync connection between the MX5X and the desktop/laptop computer must be established using cabled USB or Serial connection for the initial setup only. The other connection options can be used thereafter. See Change Connection Parameters for a list of connection options.

The initial MX5X connection is made using  | Run. Tap the Browse button and browse to the Windows folder. Select repllog.exe and tap the OK button. The Run text box reappears with \windows\repllog in the text box.

Before pressing Enter, type a backslash (/) and remote in the Run text box. For example: \windows\repllog /remote

** Cables for initial ActiveSync Configuration:

USB Client to PC/Laptop	D26 to USB	MX5A052CBLD26USB
Serial Client to PC/Laptop	D26 to DA9F	MX5A051CBLD26DA9F

When the desktop/laptop computer and the MX5X successfully connect, the initial ActiveSync process is complete.

Change Connection Parameters

Tap the  | Settings | Control Panel | PC Connection. Tap the Change Connection button.

1. From the popup list, choose

Option	Description
IRDA	This will set up the MX5X to use the Infrared port at 57600 or 115200 baud
USB (Default)	This will set up the MX5X to use the USB port direct.
COM1 @ 115200	This will set up the MX5X to use: COM 1 direct at 38400 baud, COM4 direct at 38400 baud, or COM4 direct at 115200 baud

2. Tap OK and ensure the check box for Enable direct connections to the desktop computer is checked.
3. Tap OK to return to the Control Panel.
4. Select Scanner and ensure the integrated scanner is set to a port that is different than the Get Connected port (COM 1).

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

Backup MX5X Files Using ActiveSync

Use the following to backup data files from the MX5X to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

Initial ActiveSync partnership between the MX5X 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, wireless, InfraRed, or Ethernet.

MX5X and PC Partnership

An ActiveSync partnership between the PC and MX5X has been established. See section *Initial Setup*.

Serial Port Transfer

A PC with an available serial port and an MX5X with a serial port. The desktop or laptop PC must be running Windows 95, 98, NT or 2000.

Null modem cable with all control lines connected. LXE recommends using the RS-232 cable listed in the following section *Connect*.

Infrared Port Transfer

A PC with an infrared port and an MX5X with an infrared port. The desktop or laptop PC must be running Windows 98 SR2, Windows 2000 or Windows XP.

USB Transfer

A PC with an available USB port and an MX5X with a USB port. The desktop or laptop PC must be running Windows 98 SR2 or Windows 2000.

LXE-specific USB cable as listed in the following section *Connect*.

Ethernet Transfer

A PC with an available Ethernet port and an MX5X. The desktop or laptop PC must be running Windows 98 SR2 or Windows 2000.

LXE-specific Ethernet RJ45 cable as listed in the following section *Connect*.

Connect

Connect the correct cable to the PC (the host) and the MX5X (the client).

Select Get Connected from  | Programs | Communications | Connect.

Cable, MX5X to PC RS-232, D26 to DA9F	MX5A051CBLD26DA9F
Cable, MX5X to PC USB, D26 to USB	MX5A052CBLD26USB
Cable, MX5X D26 to Ethernet RJ45, MX5X	MX5A057CBLETHD26RJ45
Cable, MX5X D26 to USB Host Receptacle, MX5X	MX5A058CBLD26USBHOST

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

Ethernet or Wireless Connection

After establishing an Ethernet connection run \Windows\REPLLOG.EXE /remote. Select Network Connection in the ActiveSync dropdown box and your computer name in the second drop down box. Tap Connect on the MX5X.

If a partnership has previously been established, the Connection Status dialog box is displayed. Tap Sync Now to continue the synchronization or Disconnect to close the Ethernet connection.

The process is the same when using the Enhanced Ethernet Desktop cradle or the mobile device's Ethernet cable.

Explore

From the ActiveSync Dialog on the Desktop PC, tap on the Explore button, which allows you to explore the MX5X from the PC side, with some limitations. You can copy files to or from the MX5X using drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows directory on the MX5X. (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 – MX5X User's Guide* from your desktop computer to the My Documents folder on the MX5X.

Disconnect

Serial Connection

Disconnect the cable from the MX5X. Put the MX5X into Suspend by tapping the red Suspend button. Tap the status bar icon in the lower right hand corner of the status bar.

Then tap the Disconnect button.

IRDA Connection

Move the MX5X so the infrared beam is broken. Tap the status bar icon in the lower right hand corner of the status bar.

Then tap the Disconnect button.

USB Connection

Disconnect the cable from the MX5X. Tap the status bar icon in the lower right hand corner of the status bar.

Then tap the Disconnect button.

IMPORTANT – Do not put the MX5X into suspend while connected via USB. The MX5X will be unable to connect to the host PC when it resumes operation.

Wireless Device Connection

Put the MX5X into suspend by tapping the red Suspend button. Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Ethernet Connection

Tap Disconnect in the Connection Status dialog box. Disconnect the Ethernet cable..

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 MX5X is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (Windows | Settings | Control Panel | System | Device Name)

If the cold booted MX5X tries to reestablish the partnership with the same host PC, a new random number is generated for the MX5X and ActiveSync will insist the unique name of the MX5X be changed. If the MX5X 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.

Troubleshooting ActiveSync

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

If the MX5X is already in a powered docking cradle cabled to a PC, remove and reinsert the MX5X into the powered cradle.

If the MX5X is connected to a PC by a cable, disconnect the cable from the MX5X 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.

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

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

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 MX5X

- Tap Start | Programs | Communication | Get Connected to establish an ActiveSync connection to the host.

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 double-tapping REPLLOG.EXE on the CE device, the word CLIENT appears on the display in ASCII format. When using a serial port monitor, you see the host echo CLIENT, followed by SERVER. After this point, the data stream becomes straight (binary) PPP.

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.

iRescue


Note: iRescue material is copied from copyrighted iRescue material with permission from Itronix.

You can use the iRescue program to backup and restore the contents of the MX5X files and registry. There are four basic reasons to use iRescue:

- To clone program settings and files from one device onto other devices.
- To restore data if the battery is drained completely before a recharge.
- To restore data following a cold reset.
- To restore data if files or settings were unintentionally modified or deleted, causing a device malfunction or data loss.

The backup data is saved onto the mobile device's removable storage media, e.g. flash card.

Start iRescue

Select the iRescue icon in the taskbar. If you do not have this icon, select  | Run. Then type irescue and select OK. You can view version information by tapping the About button on the Backup tab.

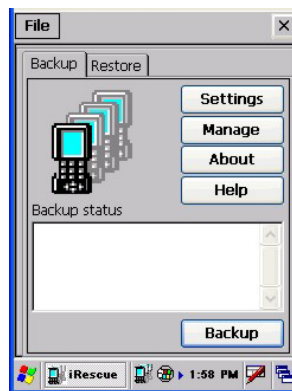


Figure 3-26 iRescue Backup

Backup Your Mobile Device using iRescue

Note: In order to perform a full backup, all other programs must be closed. If any programs are running, iRescue will prompt you to close them.

1. Open iRescue and select the Backup tab.
2. Select the Settings button and choose a backup destination from the Location drop-down list. This list shows all removable storage media on the device.
3. Tap OK.
4. Select the Backup button to begin the backup.

Note: Information about each completed task or error status will appear in the Backup status box and the Custom Status LED will flash red and green alternately during this operation.

Change Backup Settings

Open iRescue and select the Backup tab > Settings button to perform the following:

- Set the backup location
- Specify how many backups the program is allowed to keep.

Note: If the number of backups is exceeded, iRescue prompts the user to delete one or more of the existing backups before performing a new backup.

- Enable/Disable automatic backup on a battery low event.

Note: Once the battery level reaches 10%, iRescue automatically performs a backup. If the level stays under 10%, iRescue performs a backup every two (2) hours until the battery is recharged. This option is enabled by default.

- Enable/Disable the auto discard feature when iRescue performs an automatic backup.

Note: For example, if iRescue is about to perform an automatic backup and either the maximum number backups is exceeded or the device does not have enough space for the next backup, iRescue deletes the oldest backup to free up space. If this option is not checked, the auto backup on low battery only occurs if the maximum number of backups is not exceeded and enough space is detected. This option is enabled by default.

- Select an automatic backup schedule. You can choose a daily, weekly, or monthly automatic backup schedule.

Note: During an automatic backup, whether scheduled or battery level initiated, iRescue will NOT close any running applications. Any open or running application will NOT be saved during the automatic backup. This does not apply to user initiated backups since iRescue will prompt you to close other running applications.

Manage Backups

1. Open iRescue and select the Backup tab.
2. Select the **Manage** button to bring up the Manage dialog box. From this page, you can:
 - View all available backups on all the removable storage media present on the device.
 - Delete a backup by selecting it from the backup list and tapping the Delete button. Once deleted, the entry for that backup disappears from the list.

Restore Backups

1. Open iRescue and select the Restore tab.
2. Select a backup file from the Select Date drop-down list. This displays all available backups from each removable storage media.
3. The tree view displays the contents of the selected backup. Double tap the Files item to view a list of folders and files contained in the backup.
4. To restore selected files, uncheck the files that you do not want to restore. By default, and each time a different backup is selected, all files and folders are selected.
5. Select the Restore button to restore the files and registry settings of a backup. Only selected items in the tree view are restored; all unselected items are skipped.

Wavelink Avalanche Enabler Configuration

An MX5X 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.

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

Terminology may appear different, based on your installed version:

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

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

Briefly . . .

The Wavelink Avalanche Enabler installation file is loaded on the mobile device by LXE; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

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

1. Doubletap the Avalanche Enabler CAB file in the System folder. The filename is LXE_MX5X_ENABLER.CAB.
2. Warm boot the mobile device.

Enabler Uninstall Process

To remove the LXE Avalanche Enabler from a Windows CE mobile device:

1. Delete the Avalanche folder located in the System folder.
2. 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 Wavelink Management Console (refer to the *Wavelink Avalanche Manager User Guide* for details and instruction).

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Management 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 Agent running on the host machine.

- Wired via a serial cable between the Agent PC and the LXE device.
- Wired via a USB connection, using ActiveSync, between the Agent PC and the mobile device.
- Wirelessly via the 2.4GHz network card and an access point

After installing the Enabler on the mobile unit, a reboot is required for the Enabler to begin normal functionality. Following a mobile device reboot, the Enabler searches for an Agent, first by polling all available serial ports and then over the wireless network. The designation of the mobile device to the Avalanche CE Manager is LXE_MX5X.

The Enabler running on LXE Windows CE devices will attempt to access COM1, COM2, and COM3. An Agent not found message will be displayed if the agent 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 an Agent or Management Console 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 Agent 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 Management Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE Units

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Avalanche icon on the desktop.
2. Select File | Settings. Enter the password.
3. Select the Adapters tab.
4. Choose settings for the Use Manual Settings parameter.
5. Choose settings for Manage Network Settings, Manage Wireless Settings and Use Avalanche Network Profile.
6. Click the OK button to save the changes.
7. Reboot the device.

See Also: LXE Computers and Wavelink Avalanche User's Guide.

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 3-27 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 Agent and Management Console. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the mobile device immediately upon a successful connection.
Abort	Stop transmission.
Settings	The Settings option under the File menu allows the user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected. The default password is system The password is not case-sensitive.
Scan Config	<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 Wavelink Avalanche Manager User Guide for details.
Exit	The Exit option is password protected. The default password is leave The password is not case-sensitive.
If changes were made on the Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed:	If changes were made on the Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed:  Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche control panel screen.

Avalanche Update Settings

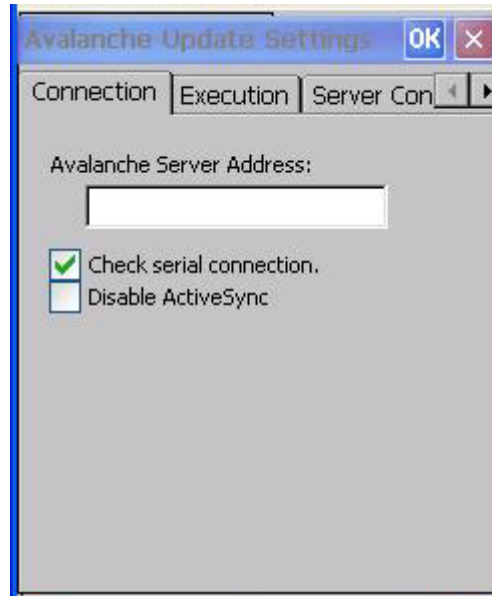
Access:  | Avalanche | File | Settings

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 Agent on the Wavelink Avalanche Management Console can be disabled until needed (refer to the Wavelink Avalanche Manager User Guide for details).

Menu Options

Connection	Enter the IP Address or host name of the Agent portion of the Avalanche Management Console. Set the order in which serial ports or RF are used to check for the presence of the Agent.
Execution	Unavailable in this release. LXE recommends using AppLock, which is resident on each Windows mobile device.
Server Contact	Setup synchronization, scheduled Agent 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. Not currently supported by LXE.
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection**Figure 3-28 Connection Options**

Avalanche Server Address	Enter the IP Address or host name of the Agent assigned to the mobile device.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Agent before checking for a wireless connection to the Agent.
Disable ActiveSync	Disable ActiveSync connection with the Agent.

Execution

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

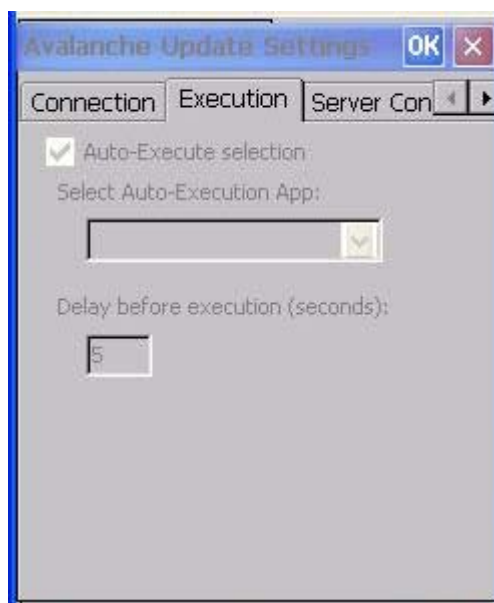
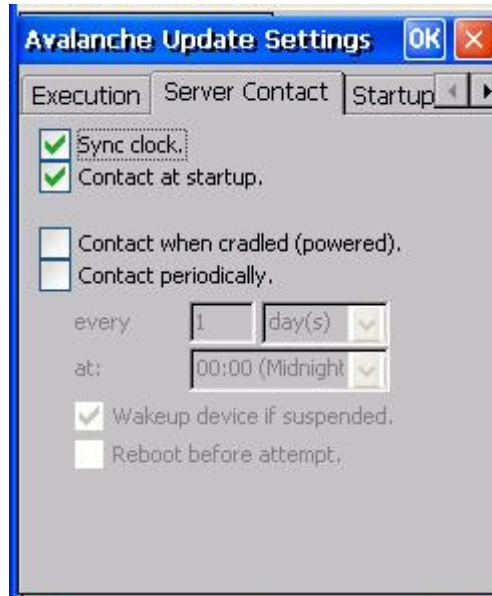


Figure 3-29 Execution Options (Dimmed)

Auto-Execute Selection	An application that has been installed with the Avalanche Management system can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Management System.
Delay before execution	Time delay before launching Auto-Execute application.

Server Contact**Figure 3-30 Server Contact Options**

Sync Clock	Reset the time on mobile computer based on the time on the Agent host PC.
Contact at startup	Connect to the Agent when the Enabler is accessed.
Contact when cradled	Initiate connection to the Agent based on a docking event. <i>Not available on the MX5X.</i>
Contact Periodically	Allows the administrator to configure the Enabler to contact the Agent and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Agent occurs, a mobile device that is in Suspend Mode can 'wakeup' and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Agent.

Startup/Shutdown

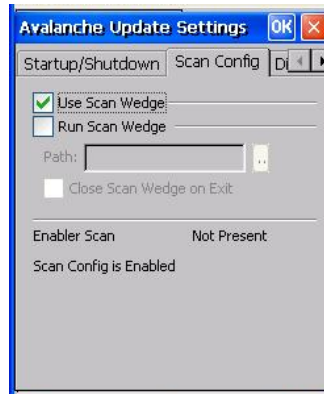
LXE recommends using LXE AppLock for this function. AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in Chapter 6.



Figure 3-31 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 Agent.
Monitor for updates	Attempt to connect to the Agent and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Agent 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 Agent for updates once the Enabler application is exited.

Scan Config



Note: Scan Config functionality is a standard option of the Wavelink Avalanche System but is not currently supported by LXE on Windows CE.

Figure 3-32 Scan Config Option

Display

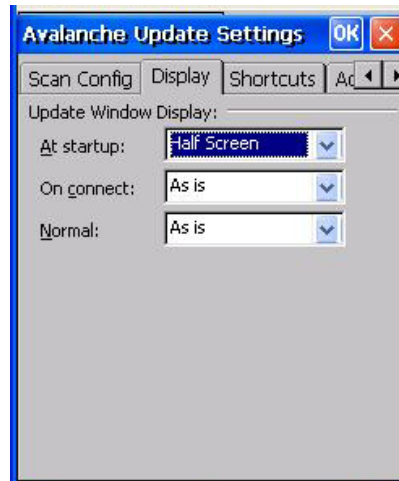


Figure 3-33 Window Display Options

Update Window Display

The user interface for the Enabler can be configured to dynamically change based on the status of the connection with the Agent.

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

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.

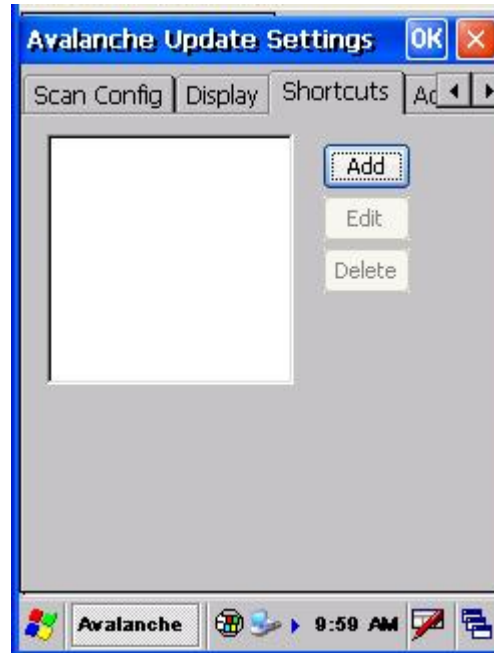


Figure 3-34 Application Shortcuts

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

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.

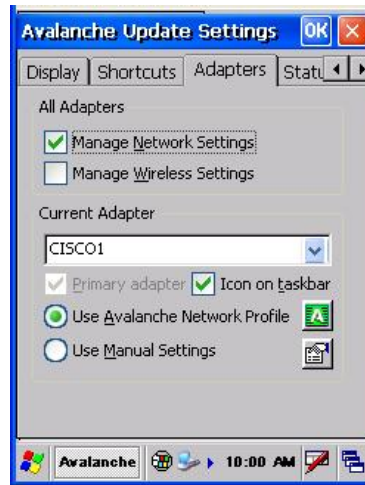


Figure 3-35 Adapters Options – Network

Manage Network Setting	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Management 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 <i>only</i> .
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.



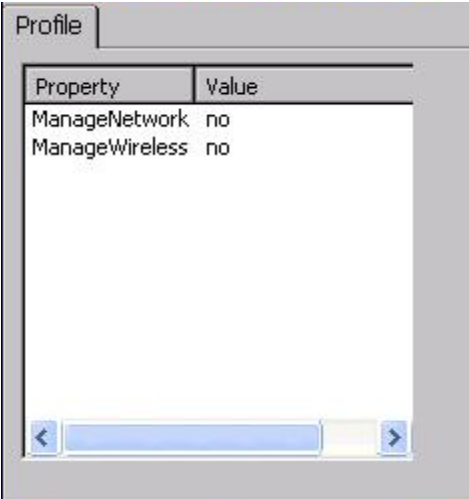


Use Avalanche Network Profile	<p>The Enabler will apply all network settings sent to it by the Management Console.</p> 						
<p>Avalanche Icon</p> 	<p>Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.</p>  <table border="1" data-bbox="870 520 1255 632"> <thead> <tr> <th>Property</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>ManageNetwork</td> <td>no</td> </tr> <tr> <td>ManageWireless</td> <td>no</td> </tr> </tbody> </table>	Property	Value	ManageNetwork	no	ManageWireless	no
Property	Value						
ManageNetwork	no						
ManageWireless	no						

Figure 3-36 Avalanche Network Profile Displayed

<p>Use Manual Settings</p>	<p>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.</p> 
<p>Properties Icon</p> 	<p>Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:</p>

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

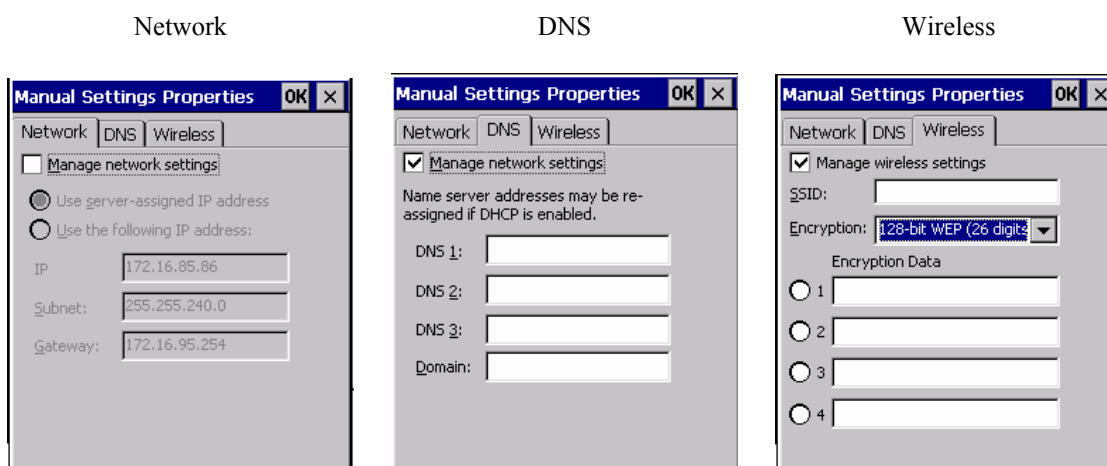


Figure 3-37 Manual Settings Properties Panels

For descriptions of these Enabler parameters, refer to *Chapter 5 Wireless Network Configuration*.

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

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 *Adapters Options – Network*).

Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

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..

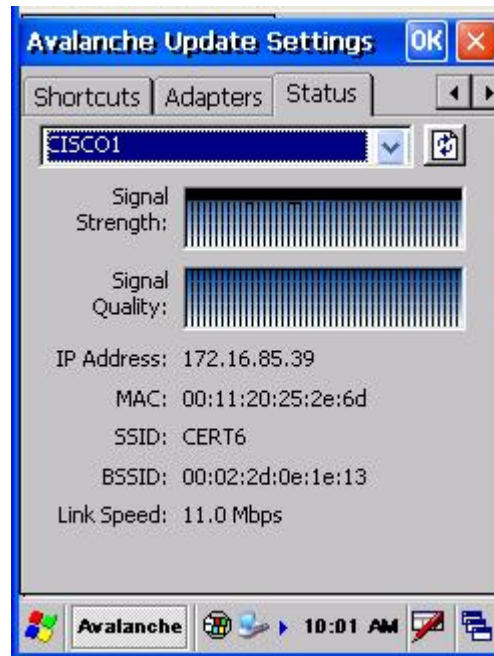


Figure 3-38 Status Display

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 Avalanche Enabler

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.

Chapter 4 Scanner

Introduction

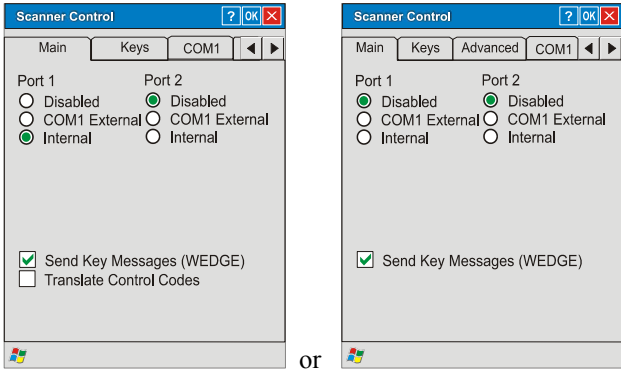
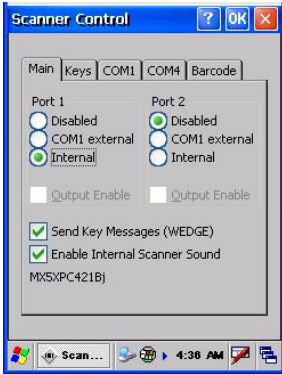
Access:  | Settings | Control Panel | Scanner

Set scanner keyboard wedge parameters, enable or disable symbologies from being scanned, 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 MX5X integrated scanner *only*. Barcode manipulation parameters apply to barcodes scanned by the integrated scanner 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 MX5X devices. Your Scanner options may or may not be as described in this section. To identify the current software version, go to Start | Settings | Control Panel | Handheld.

If the Scanner Control panel looks like this	Go to
	<p>Chapter 3 System Configuration, section titled</p>
	<p>This chapter</p>

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.

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 | Settings | Control Panel | Scanner. Tap the OK button and close the scanner applet. This action will synchronize all scanner formats.


Factory Default Settings

Factory Default Settings	
Main	
Port 1	Disabled
Enable Internal Scanner Sound	Enabled
Send Key Messages (WEDGE)	Enabled
Output Enable	Disabled (Dimmed)
Port 2	Disabled
Enable Internal Scanner Sound	Enabled
Send key messages WEDGE	Enabled
Output enable	Disabled (Dimmed)
Keys	
Left Scan key	Enter key
Right Scan key	Enter key
COM Ports (COM1 / COM4)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	8
Barcode	
Enable Code ID	None
Symbology Settings	Enable Dimmed / Min - 1 to Max - all
AIM (ID)	Enable Dimmed
Symbol (ID)	Enable Dimmed
Custom	Null
Control Character	Disabled
Translate All	Disabled
Character/Replacement	NULL / Ignore(drop)
Custom Identifiers	
Name	Blank
ID Code	Blank

Notes:

- If the internal scanner has to be configured to operate at any communication settings other than 9600, N, 8, 1 and the MX5X either loses power or a cold boot command is entered, the Scanner applet must be reconfigured to match the scanner communication settings.
- ActiveSync will not work over a COM port if that COM port is enabled in the Scanner applet as scanner input. For example, if COM 1 is being used by the scanner, COM 1 can't be used by any other program.
- LXE 8300 Tethered Scanners and Symbology Settings (AIM ID) – Before manipulating data received from 8300 tethered scanners, and Symbology settings are desired, the user must configure and append the Symbology ID as a prefix.
- 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

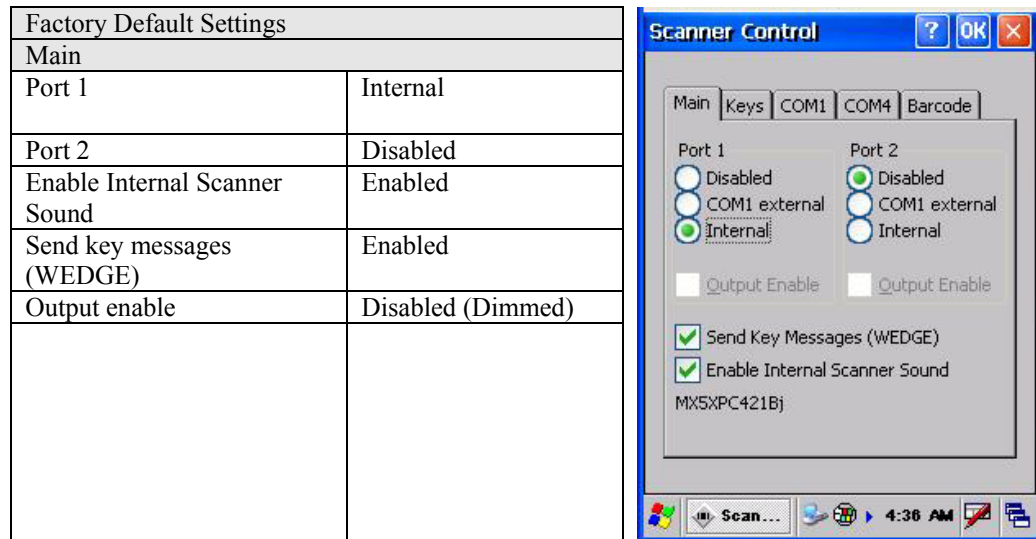


Figure 4-1 Scanner Control / Main

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

Note: The left and right Scan buttons have no effect on tethered external scanners.

Parameters

Port -- Port 1 default is Internal. Port 2 default is Disabled.

Send Key Messages (WEDGE) -- The default setting is Enabled. This feature coexists with the parameters and settings located on the Barcode tab. 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.

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

When using the scanner APIs, refer to the CE API Programming Guide and the ClearBuf setting. When two applications are reading the data using block mode, ClearBuf must be off so that the data is not erased when read.

Note: The user can also open the WDG: device and perform standard OS read functions to retrieve the data without using the LXE APIs.

Enable Internal Scanner Sound -- 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. Disable this parameter when good scan/bad scan sounds are to be handled by alternate means e.g. application-controlled sound files. Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned barcode data by the processing causes a bad scan beep from the MX5X on the same data.

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 MX5X is a single 2700 Hz beep, and a bad scan sound is a double beep.

Keys Tab

Access:  | Settings | Control Panel | Scanner | Keys

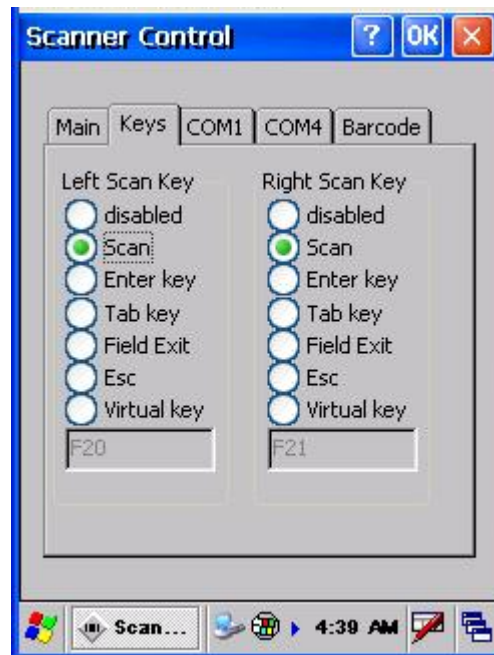


Figure 4-2 Scanner Properties / Keys Tab

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

L / R Scan Key	Function
Disabled	When either scan key is set to Disabled, it does nothing when pressed.
Scan	When set to Scan the integrated scanner is activated. If no integrated scanner is present, the Scan selection is greyed out.
Enter	When set to Enter, both the Enter key and the (Scan button) / Enter key perform the same function.
Tab	When set to Tab, both the Tab key and the (Scan button) / Tab key perform the same function.
Field Exit	<i>IBM TN5250 specific keypad only.</i> The left Scan key can be programmed as a Field Exit key.

L / R Scan Key	Function
Esc	When set to Esc the Scan key press halts the current function.
Virtual key	When set to Virtual, the Virtual Left (Scan button) key produces a default F20 and the Virtual Right (Scan button) key produces a default F21.

Change a Virtual Key (F20 or F21) Value


The virtual keys are set in the User Interface. The text name of the key is typed into the text box below the key. The strings listed below and, along with all single alphanumeric characters and punctuation, can be used as replacements for the default F20 and F21.

Left	Backspace	F7	F15	Del
Right	Tab	F8	F16	Space
Up	F1	F9	F17	Enter
Down	F2	F10	F18	Esc
Home	F3	F11	F19	Break
End	F4	F12	F20	
Page Up	F5	F13	F21	
Page Down	F6	F14	Ins	

Single letters, numbers and punctuation are valid;

a is valid but not **aaaaa**, 3 is valid but not **333**.

COM1/COM4 Tab

Access:  | Settings | Control Panel | Scanner | COM1 tab or COM4 tab

Factory Default Settings	
COM1 Port	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
COM4 Port	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8

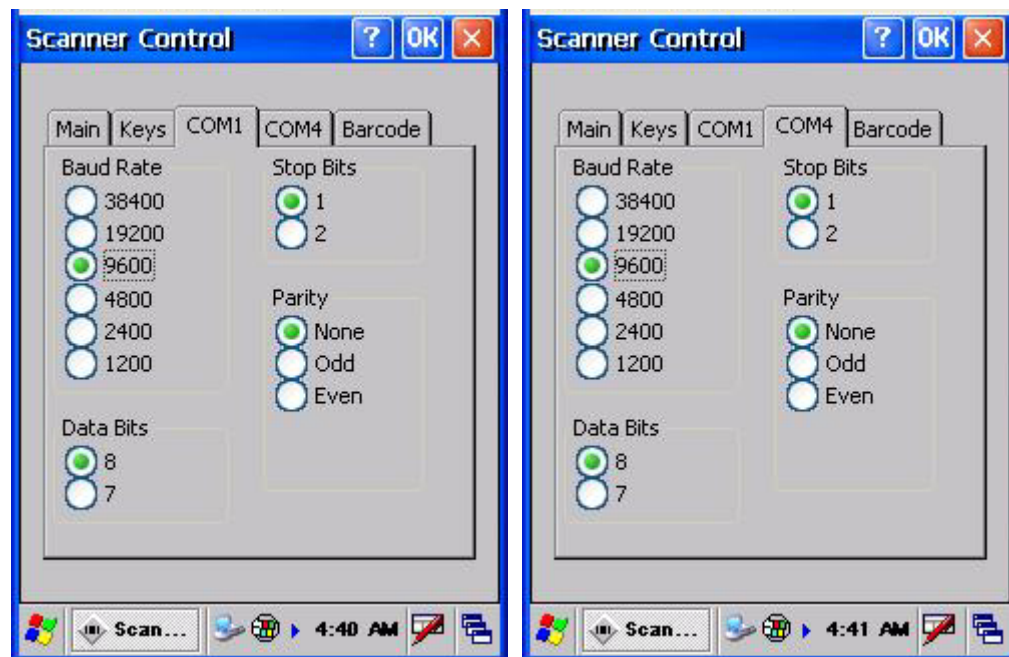



Figure 4-3 Scanner Control / COM1 and COM4

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

Note: Pin 9 power for tethered scanners is supported via the Handheld Settings control panel applet.

Barcode Tab

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

The Scanner application (Wedge) can only enable or disable the processing of a barcode inside the Wedge software.

The Scanner application enables or disables the Code ID that may be scanned.

Enabling or disabling a specific barcode symbology is done manually using the configuration barcode in the *Integrated Scanner Programming Guide* (available on the LXE Manuals CD and the LXE ServicePass website).

Choose an option from the Enable Code ID drop-down box: None, AIM ID, Symbol ID, or Custom ID.

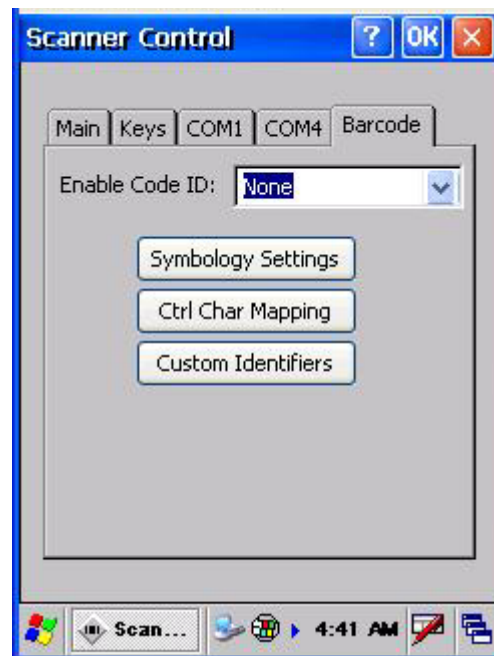


Figure 4-4 Scanner Control / Barcode tab

Buttons

Symbology Settings -- Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.

Ctrl Char Mapping -- Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.

Custom Identifiers -- Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

See Also: *Barcode Processing Overview* earlier in this chapter.

Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed. If the scanner being configured is not an integrated scanner, the scanner driver expects that the setting has been programmed into the scanner externally, and that the data will be coming in with the specified Code ID attached.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

Options

None	Programs the internal scanner to disable transmission of a Code ID. The only entry in the Symbology popup list is All.
AIM	Programs the internal scanner to transmit the AIM ID with each barcode. The combo box in the Symbology control panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.
Symbol	Programs the internal scanner to transmit the Symbol ID with each barcode. The combo box in the Symbology control panel is loaded with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.
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 tethered scanner operation cannot be controlled by the scanner driver; therefore, a 'good' beep may be sounded from the tethered scanner even if a barcode from a tethered scanner is rejected because of the configuration specified. The MX5X 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 MX5X. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is tapped. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.



Figure 4-5 Barcode Tab – Symbology Settings

Clear -- This button will erase any programmed overrides, returning to the default settings for the selected symbology. If Clear is pressed when All is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

- Code ID
- Leading / Trailing
- Barcode Data

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 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 <i>You are about to disable all scan input – Is this what you want to do?</i>. 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. 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

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.

See Also: *Barcode Processing Overview* earlier in this chapter.



Figure 4-6 Strip Leading / Trailing and Barcode Data

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. Programmed custom identifiers are always checked (in the order they are entered) and stripped, regardless of Enable Code ID setting. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

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

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

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

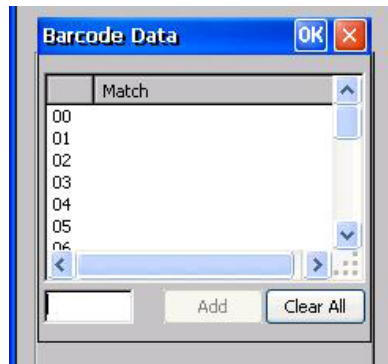


Figure 4-7 Barcode Data Match List

Barcode Data 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. <i>[Not available in this version: A popup dialog appears asking for confirmation is displayed and after approval, all items in the Custom IDs list are removed.]</i>
Remove	The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

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

Match List Rules

The data in the 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. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

See Also: *Barcode Processing Overview* earlier in this chapter.

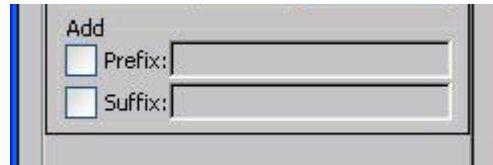


Figure 4-8 Add Prefix/Suffix Control

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 C 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 C Reference Material.

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. <F1>), arrow keys, Page up, Page down, Home, and End.

Barcode – Ctrl Char Mapping

See Also: *Barcode Processing Overview* earlier in this chapter.

The Ctrl Char Mapping button activates a dialog to define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.



Figure 4-9 Barcode Tab – Ctrl Char Mapping

See Hat Encoding and Decimal-Hexadecimal Chart in Appendix C Reference Material.

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 Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplayes the default Ignore (drop) 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).

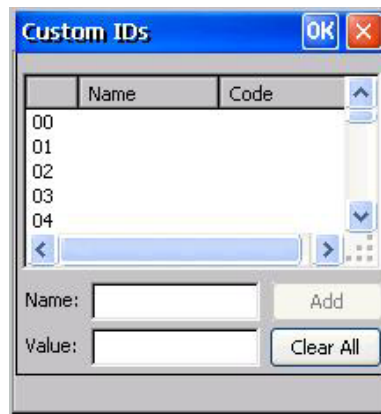


Figure 4-10 Barcode Tab – Custom Identifiers

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

Parameters

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

Buttons

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

Control Code Replacement Examples

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

Configuration data	Translation	Example Control Character	Example configuration	Translated data
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\0x0A'	Value 0x0C is a barcode is converted to text '0x0A'

Figure 4-11 Control Code Replacement Examples

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 previous 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	< rejected > (too short)


Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-13]E01234567890987	ccc]E04567890yyy
EAN-13]E01231234567890987	ccc]E0234567890yyy
EAN-13]E01234	ccc]E0yyy
I2/5]I04444567890987654321	< rejected > (too long)
I2/5]I04444567890123	ddd7890zzz
I2/5]I0444	dddzzz
I2/5]I022245622	ddd45zzz
Code-93]G0123456	< rejected > (disabled)
Code-93]G0444444	< rejected > (disabled)
Code-39]A01234567890	aaa4567890www
Code-39 full ASCII]A41231234567890	aaa1234567890www
Code-39]A4	< rejected > (too short)

Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

Figure 4-12 Barcode Processing Examples

Chapter 5 Wireless Network Configuration

Introduction

	<p>It may be necessary to upgrade client drivers in order to use certain Summit Client Utility (SCU) features described in this chapter. Please contact your LXE representative for details.</p>
---	--

The MX5X mobile device offers a choice of Cisco, Symbol and Summit clients. The Summit client is an 802.11g network device and is compatible with Windows CE operating systems. The Cisco and Symbol clients are 802.11b wireless devices and are *compatible only* with the Windows CE .NET 4.2 operating system. The wireless client can be configured for no encryption, WEP encryption or WPA security (WPA is N/A with Symbol client).



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

Please refer to the table below for the security options supported for each client type.

Security Options Supported	Summit (CE .NET 4.2 and CE 5)	Cisco (CE .NET)	Symbol (CE .NET)
None	Yes	Yes	Yes
WEP	Yes	Yes	Yes
LEAP	Yes	Yes	No
EAP-FAST	Yes	No	No
PEAP-MSCHAP	Yes	Yes	No
WPA/LEAP	Yes	Yes	No
WPA-PSK	Yes	Yes	No
PEAP-GTC	Yes	Yes	No
EAP-TLS	Yes	Yes	No

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.

	<p>Please refer to the <i>LXE Security Primer</i> to prepare the Authentication Server and Access Point for MX5X communication. It is available on the LXE Manuals CD and the LXE ServicePass website.</p>
	<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>

Summit Client Configuration



Summit Client Utility Icon

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

Start the Summit Client configuration by tapping the Summit Client Utility icon on the desktop. You can also start the Summit Client utility by tapping Start | Programs | Summit | SCU.

Important: After making changes to a profile, tap the Commit button and perform a Warm Reset / Suspend and Resume.

Summit Client Utility

Access: Start | Programs | Summit | SCU or SCU Icon on Desktop



or



Figure 5-1 Summit Client Utility (SCU)

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

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

The Status tab contains information on the current connection.

The Diags tab provides utilities to troubleshoot the client (network device). Update Driver and Site Survey functions are not available in this release. Contact your LXE representative for availability.


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.

Wireless Zero Config Utility and the Summit Client

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating the Wireless Zero Config application is enabled and the MX5X is not connected to a network. You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network.

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

To use Wireless Zero Config, first open the Summit Client Utility.

1. Select ThirdPartyConfig in the Active Config 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 MX5X in Suspend, then tap the Power button to wake the MX5X from Suspend mode.

The Wireless Zero Config utility begins.

Main Tab

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

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

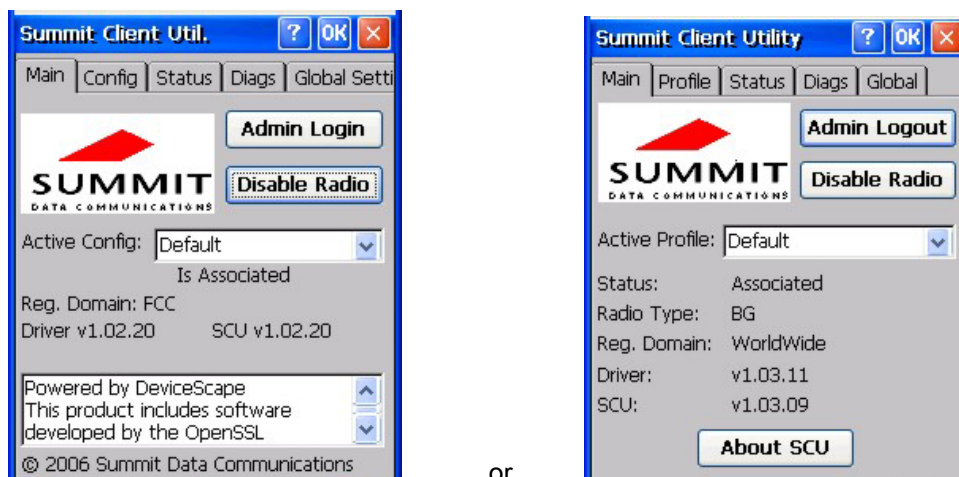


Figure 5-2 SCU – Main Tab

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

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

The Active Config or Active Profile can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Admin mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin password has been entered and accepted (LXE recommends that only the *default* profile be edited).

The Disable Radio button is 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 client parameters. Profile (or Config) and Global Settings (or Global) parameters 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 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 Settings or Global tab.

The end user can:

- Turn the radio on or off on the Main tab.
- Select active Config (Profile) on the Main tab.
- View the current parameter settings for the profiles on the Config or Profile tab.
- View the global parameter settings on the Global Settings or Global 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.

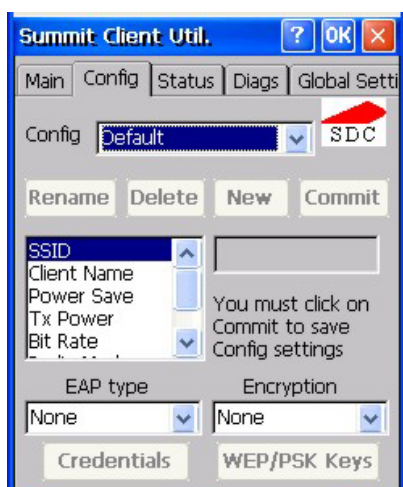
After Admin login, the end user can also:

- Create, edit, rename and delete profiles on the Config or Profile tab.
- Edit global parameters on the Global Setting or Global tabs.

Config or Profile Tab

Note: Tap the Commit button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!

Factory Default Settings	
Config / Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	BG Optimized or BG Rates Full
Auth Type	Open
EAP type	None
Encryption	None



or



Figure 5-4 SCU – Config / ProfileTab

When logged in as an Admin (see *Admin Login*), use the Config or Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, but cannot be changed. The buttons on this tab are dimmed if the Admin 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.

Button	Function															
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.															
New	Creates a new profile with the default settings (see <i>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 data-bbox="779 772 1161 1115" data-label="Image"> <table border="1"> <thead> <tr> <th>SSID</th> <th>RSSI</th> <th>Secure</th> </tr> </thead> <tbody> <tr> <td>Guest</td> <td>-52</td> <td>true</td> </tr> <tr> <td>wpapskr</td> <td>-52</td> <td>true</td> </tr> <tr> <td>Guest</td> <td>-51</td> <td>true</td> </tr> <tr> <td>CERT2</td> <td>-60</td> <td>false</td> </tr> </tbody> </table> </div> <p style="text-align: center;">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>	SSID	RSSI	Secure	Guest	-52	true	wpapskr	-52	true	Guest	-51	true	CERT2	-60	false
SSID	RSSI	Secure														
Guest	-52	true														
wpapskr	-52	true														
Guest	-51	true														
CERT2	-60	false														
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.															

Note: Unsaved Changes -- Some 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 Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW or 1mW. <i>Depending on the version of the SCU, the options for Tx Power are between Maximum and 1mW</i>
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the compact flash wireless device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Radio Mode	BG Optimized or BG Rates Full	Specify 802.11g and/or 802.11b when communicating with the Access Point. Options are: B rates only, BG Rates full, G rates only, BG optimized. Note: Default value may vary depending on installed SCU driver version.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.

Parameter	Default	Explanation
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, or EAP-TLS. Note: EAP type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.
Encryption	None	Type of encryption to be used to protect transmitted data. Options are: None, Manual WEP, Auto WEP, WPA PSK, WPA TKIP, WPA2 PSK, WPA2 AES, CCKM TKIP, CKIP Manual, CKIP Auto, Manual WEP CKIP, or Auto WEP CKIP.

Note: The Encryption type chosen determines if the WEP/PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.

Status Tab

This screen displays information on the current profile and wireless connection. Information cannot be edited or changed on the Status panel.

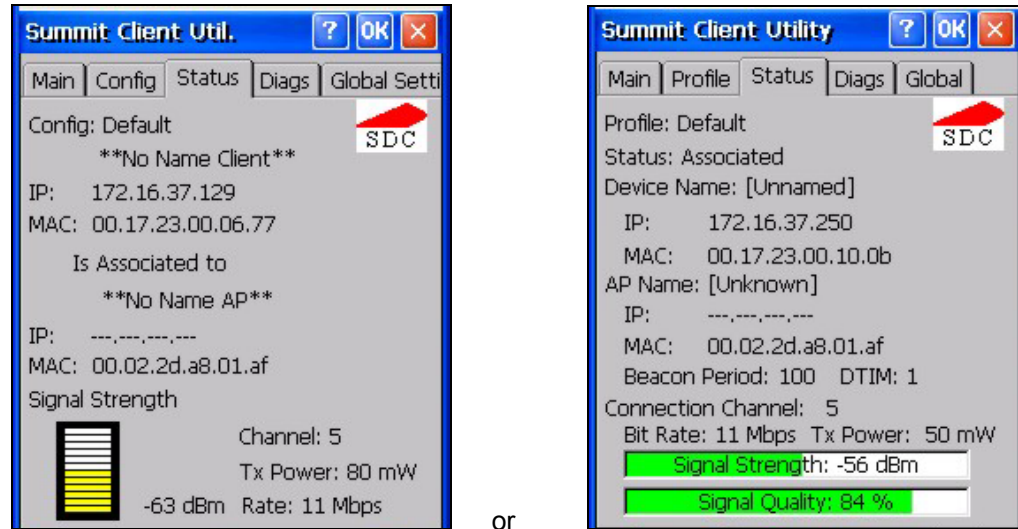


Figure 5-6 SCU – Status Tab

The panel displays:

- 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 wireless connectivity issues for the IP address shown above the Release/Renew button. Admin login is required for the (Re)connect button function.

Note: Diagnostics and Site Survey functions are not available in all SCU releases.

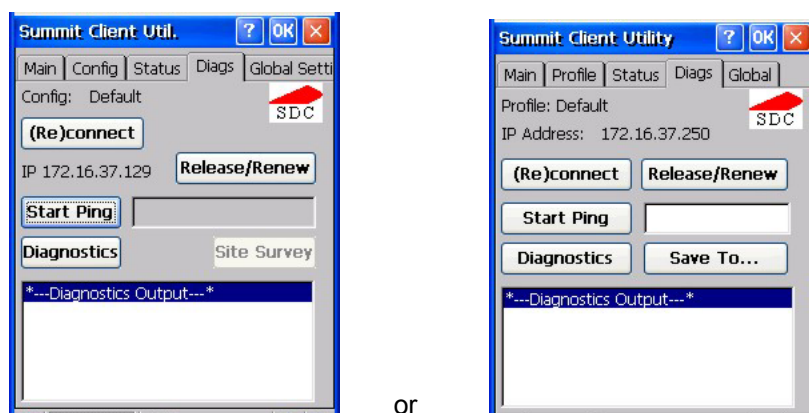


Figure 5-7 SCU – Diags Tab

Buttons

Button	Function
(Re)connect	Tap this button to apply, or reapply, the current config profile and attempt to associate or authenticate to the wireless LAN. Activity is logged in the Diagnostic Output text box on the lower part of the panel.
Release/Renew	Release the current IP address to obtain a new IP address. This option renews the IP address when applicable. Activity is logged in the Diagnostic Output text box. If a fixed IP address has been assigned to the wireless device, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed next to the Release/Renew button.
Start Ping	Tap the text box and type an IP address to Ping. Tap the Start Ping button to start pinging the IP address. The button name changes to Stop Ping. Tap Stop Ping to end the pinging process. The pinging process ends when any other button on this panel is tapped or a different menu tab is selected. Ping results are displayed in the Diagnostic Output text box.
Diagnostics	<p>Tapping this button begins an attempt to (re)connect to the wireless LAN. This option provides more data in the Diagnostics Output text box than the (Re)connect option. The data dump includes client state, profile settings, global settings, and a list of access points by SSID broadcasting in the wireless device's immediate area. The text file created, <code>_sdc_diag</code>, is placed in the Windows folder. It is overwritten when Diagnostics is run again. Not available in earlier releases.</p> <p>Tap the Save To . . . button to save the Diagnostics log to a TXT file in the (default) My Device folder.</p>

Button	Function
Site Survey	Not available in this release.

Global or Global Settings Tab

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

Note: Tap the Commit button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!

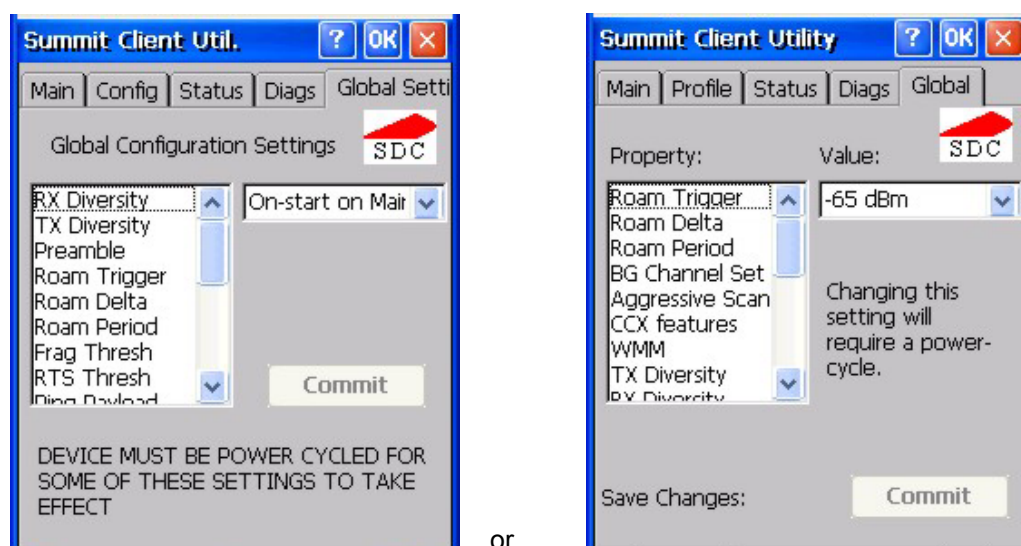


Figure 5-8 SCU – Global /Global Settings Tab

Custom Parameter Option

LXE does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value set in the registry.

Factory Default Settings

RX Diversity	On-Start on Main
TX Diversity	On
Preamble	Auto (not available in all versions)
G Short Slot	Auto (not available in all versions)
Roam Trigger	-65 dBm
Roam Delta	10 dBm
Roam Period	10 sec.
BG Channel Set	Full
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	Blank
Auth Timeout	8 sec. (not available in all versions)
Certs Path	System
CCX	Off
WMM	Off
Tray Icon	On

Global Parameters

Parameter	Default	Function
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).
Preamble	Auto	The type of network header, or preamble, for packets. (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. This parameter is not present in some versions of the SCU.
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	10 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.

Parameter	Default	Function
Roam Period	10 sec	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Hide Password	Off	If On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT	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. This value is masked when the Admin is logged out. Options are: none.

Parameter	Default	Function
Certs Path	System	<p>A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the directory path currently exists before assigning the path in this parameter. See sections titled Root Certificates and User Certificates later in this chapter for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out.</p> <p>Options are: none.</p> <p>For example, when the valid certificate is stored as My Computer/System/mycertificate.cer, enter System in the Certs Path text box as the directory path.</p>
CCX	Off	<p>Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features.</p> <p>Options are: On, Off</p>
WMM	Off	<p>Use of Wi-Fi Multimedia extensions.</p> <p>Options are: On, Off</p>
Tray Icon	On	<p>Determines if the Summit icon is displayed in the System tray.</p> <p>Options are: On, Off.</p>
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 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. 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 <i>Is not authenticated</i> or <i>Is not Associated</i> messages are displayed.
Adding, changing or renaming profiles	LXE recommends performing a Warm Reset function (using the Suspend/Resume key sequence) after tapping the Commit button.

Note: 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 tab.

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 device can access the network.
- The Username and Password are left blank on the Credentials screen. When the 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, click on the **Credentials** button.
2. Enter the **Username** and **Password** on the Credentials screen and click the **OK** button.
3. Click 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. Click the **OK** button then the **Commit** button.
12. Verify the device is authenticated by reviewing the Status tab. When the device is property 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, click on 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. Click 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**. Click 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 clicks **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.*

*If the user clicks 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 clicked or the profile is modified and the **Commit** button is clicked.*

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 click on the **Browse (...)** button.



Figure 5-10 Choose Certificate

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the **CA Cert** textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use the Certs Path

1. Follow the instructions later in this chapter for “Downloading a Root CA Certificate to a PC”.
2. Copy the certificate to a 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.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the **CA Cert** textbox.
5. Click **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 password and tap OK.

Tap the Config or Profile tab.

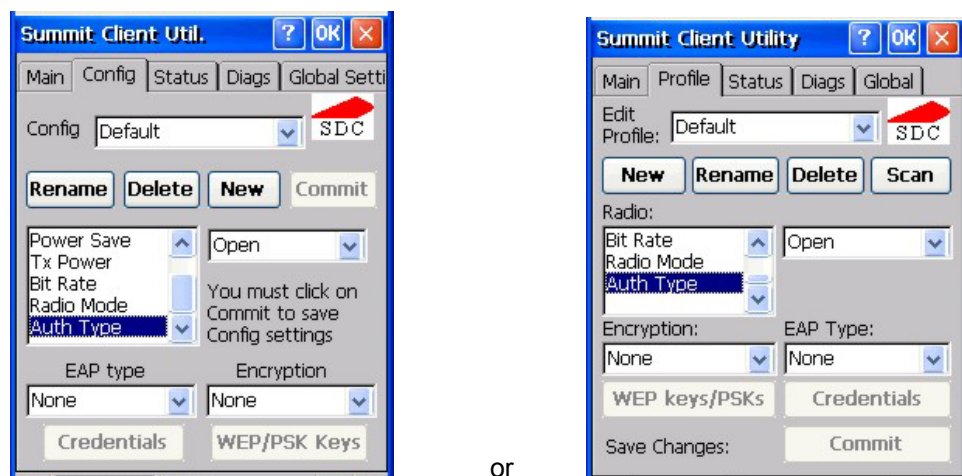


Figure 5-11 Configure a Summit Profile with No Security

Enter the SSID of the Access Point assigned to this profile.

Set Auth Type to Open.

Set EAP Type to None.

Set Encryption to None.

Tap the Commit³ button to save the new profile configuration.

Perform a warm reset function to connect using the new profile configuration.

³ LXE recommends performing a Warm Reset or Suspend/Resume function after making changes to the SCU configuration.

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 Summit WEP Key Dialog

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.

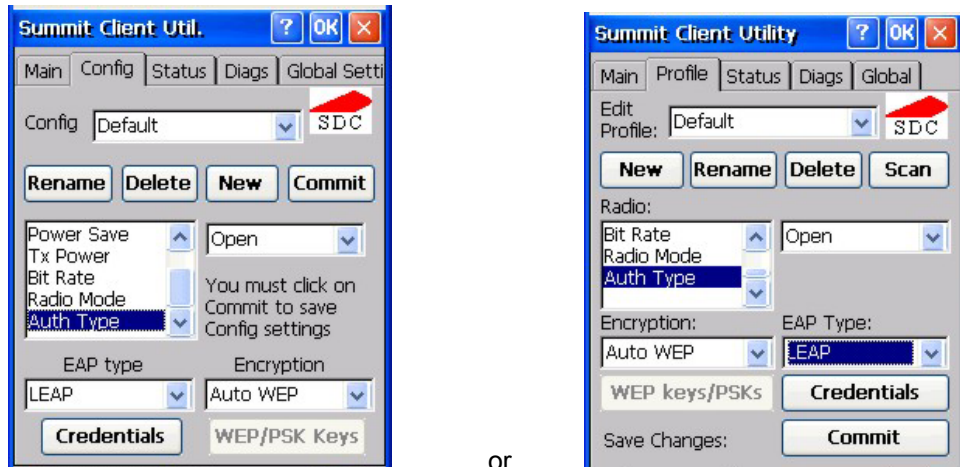
LEAP w/o WPA Authentication

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 password and tap OK. Tap the Config or Profile tab.



or

Figure 5-13 Configure a Summit Profile for LEAP w/o WPA

Enter the SSID of the Access Point assigned to this profile.

Set Auth Type to Open.

Set EAP Type to LEAP.

Set Encryption to Auto WEP.

To use Stored Credentials, tap the Credentials button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



Figure 5-14 LEAP Credentials Dialog

Enter the Username or Domain \Username in the Credentials popup text entry box, if desired.

Enter the Password, if desired. Tap OK.

Tap the Commit button to save the new profile configuration. Perform a warm reset to connect using the new profile configuration.

See Also: *WPA/LEAP Authentication* later in this section to configure the client for WPA LEAP.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

EAP-FAST Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the Admin Login button on the Main panel. Enter the Admin password and tap OK.

Tap the Config or Profile tab.

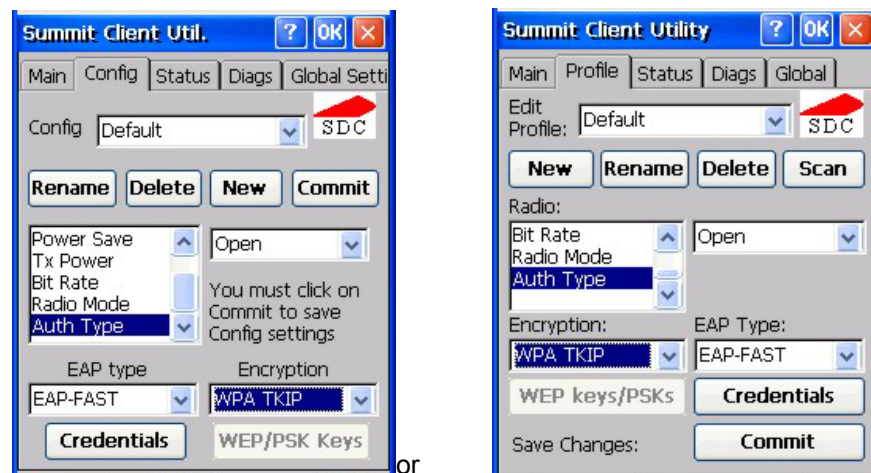


Figure 5-15 Configure a Summit Profile for EAP-FAST

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.

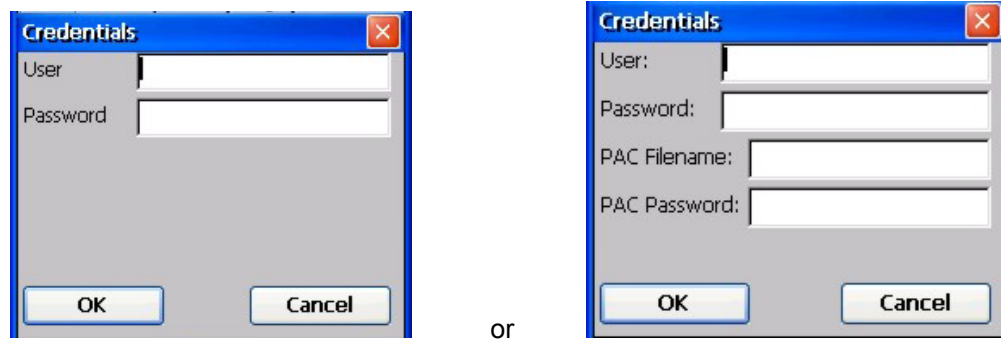


Figure 5-16 Summit EAP-FAST Credentials

Enter the Username or Domain \Username in the Credentials popup text entry box, if desired.

Enter the Password, if desired.

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.

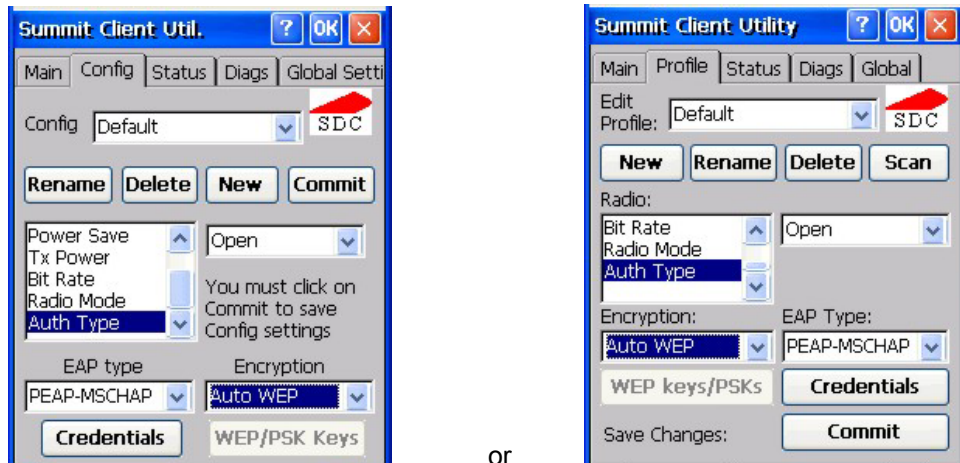
See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

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 password and tap OK.

Tap the Config or Profile tab.



or

Figure 5-17 Configure a Summit Profile for PEAP/MSCHAP

Enter the SSID of the Access Point assigned to this profile.

Set Auth Type to Open.

Set EAP Type to PEAP-MSCHAP.

Set Encryption to Auto WEP (without WPA). To configure PEAP-MSCHAP for WPA set Encryption to WPA TKIP.

To use Stored Credentials, tap the Credentials button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.

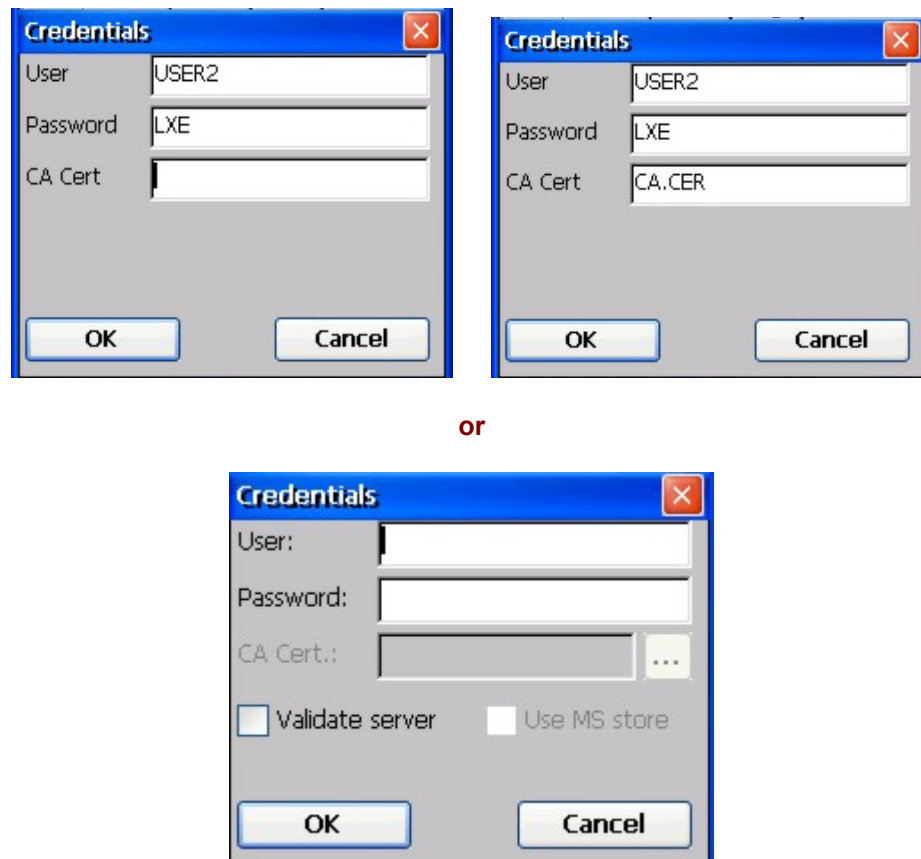


Figure 5-18 PEAP/MSCHAP Credentials Dialog

If using the **Windows certificate store**:

- Check 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 click 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.

Click **OK** then click **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.

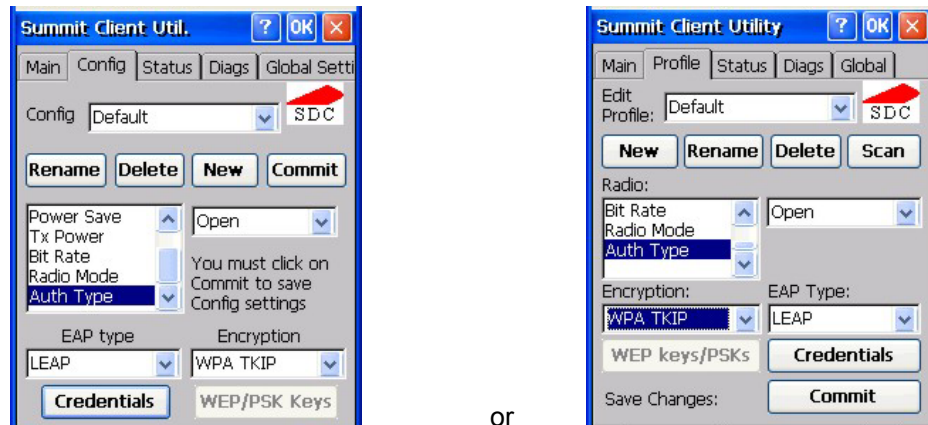
See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

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 password and tap OK.

Tap the Config or Profile tab.



or

Figure 5-19 Configure a Summit Profile with LEAP for WPA TKIP

Enter the SSID of the Access Point assigned to this profile.

Set Auth Type to Open.

Set EAP Type to LEAP.

Set Encryption to WPA TKIP.

To use Stored Credentials, tap the Credentials button.

No entries are necessary for Sign-On Credentials as the user will be prompted for the User name and Password when connecting to the network.



Figure 5-20 LEAP Credentials

Enter the Username or Domain \Username in the Credentials popup text entry box, if desired. Enter the Password, if desired. Tap OK.

Tap the Commit button to save the new profile configuration.

Perform a warm reset (or Suspend/Resume) to connect using the new profile configuration.

See Also: *LEAP w/o WPA* earlier in this section to configure the client for LEAP without WPA.

See Also: *Sign-On vs. Stored Credentials* earlier in this chapter if the username and password are left blank during setup.

WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the Admin Login button on the Main panel. Enter the Admin password and tap OK.

Tap the Config or Profile tab.

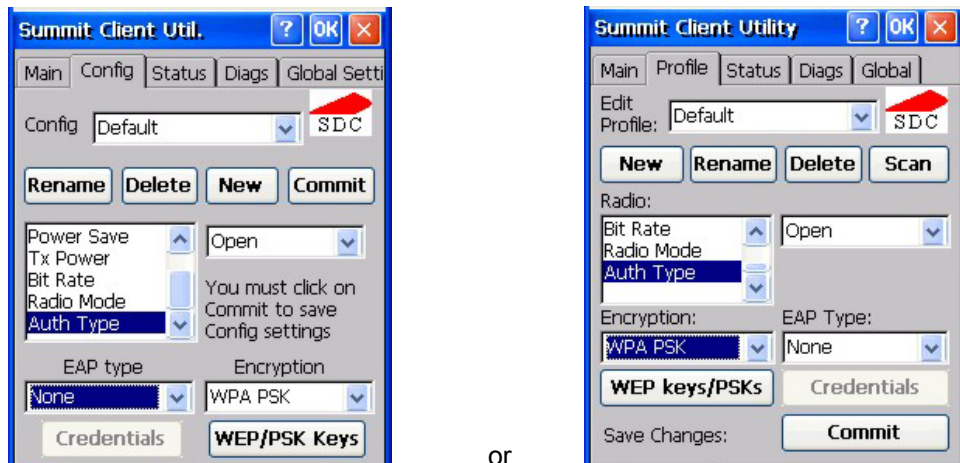


Figure 5-21 Configure a Summit Profile with WPA PSK Encryption

Enter the SSID of the Access Point assigned to this profile.

Set Auth Type to Open.

Set EAP Type to None.

Set Encryption to WPA PSK.

Tap the WEP/PSK Keys button.



Figure 5-22 Summit PSK Entry Dialog

Enter the Passphrase in the PSK Entry popup text entry box. This value can be a 64 hex character or an 8-63 byte ASCII value. Tap OK

Tap the Commit button to save the new profile configuration.

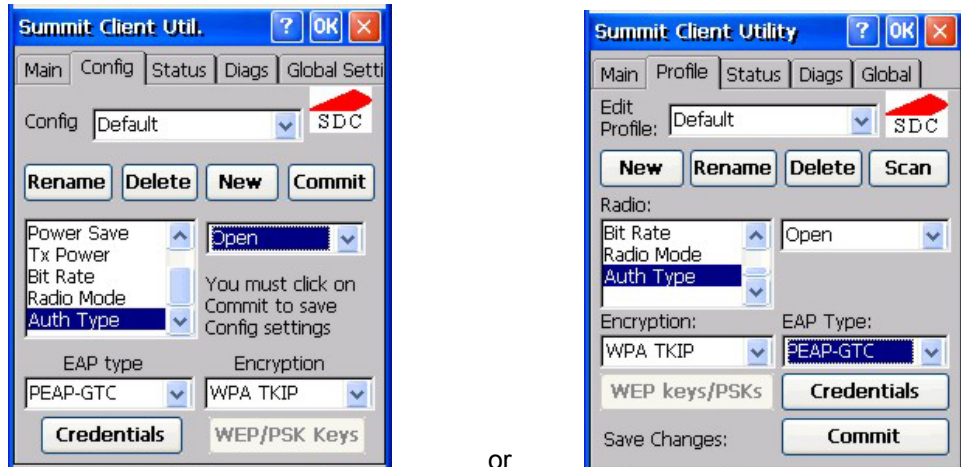
Perform a warm reset (or Suspend/Resume) to connect using the new profile configuration.

PEAP/GTC Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the Admin Login button on the Main panel. Enter the Admin password and tap OK.

Tap the Config or Profile tab.



or

Figure 5-23 Configure a Summit Profile with PEAP/GTC

Enter the SSID of the access point assigned to this profile.

Set Auth type to Open.

Set EAP type to PEAP-GTC.

Set Encryption to WPA TKIP.

To use stored credentials, tap the Credentials button.

No entries are necessary for sign-on credentials as the user will be prompted for the user name and password when connecting to the network.

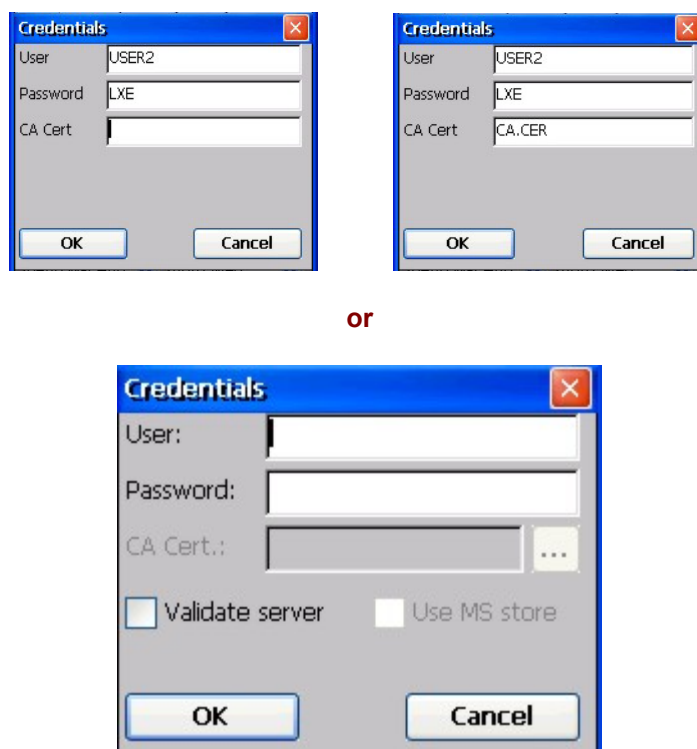


Figure 5-24 PEAP/GTC Credentials Dialog

If using the **Windows certificate store**:

- Check 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 click 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.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

For information on generating a Root CA certificate, please see “Root CA Certificate” later in this chapter.

Note: The date must be properly set on the device to authenticate a certificate.

Perform a Warm Reset function to connect using the new profile configuration.

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 password and tap OK.

Tap the Config or Profile tab.

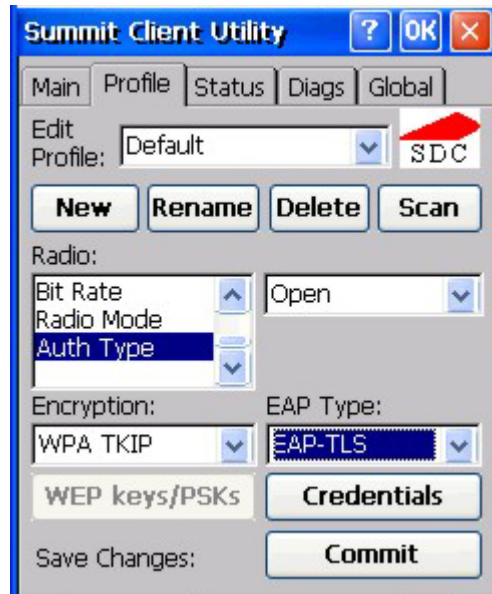


Figure 5-25 Configure a Summit Profile with EAP-TLS

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.

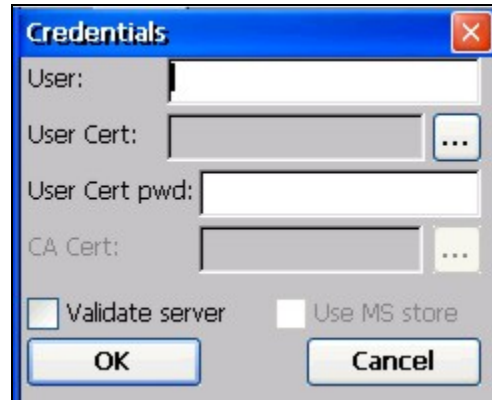


Figure 5-26 EAP-TLS Credentials Dialog

If using the **Windows certificate store**:

- Check 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 click 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.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using EAP-TLS for the user authentication.

Perform a Warm Reset function to connect using the new profile configuration.

Refer to *Sign-On vs. Stored Credentials* and *Windows Certificate Store vs Certs Path* earlier in this chapter

For information on generating a Root CA certificate, please see “Root CA Certificate” later in this chapter.

Cisco Client Configuration

Prerequisites

- Windows CE .NET 4.2 operating system
- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

Aironet Client Utility (ACU)

Access:  | Aironet Client Utility *or* ACU Icon on Desktop

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards.

Note: To configure WPA, please see Cisco Wireless Security, later in this chapter.

Profiles Tab

Use this option to manage profiles and review firmware information, status, statistics and wireless device survey data.

Profile Parameter	Default
SSID	Blank
Client Name	Blank
Infrastructure Mode	Yes
Power Save Mode	Fast PSP
Network Security Type	None
WEP	No WEP
Authentication Types	Open
LEAP	Disabled
Mixed Mode	Disabled
World Mode	Disabled
Data Rates	Auto
Transmit Power	MAX
Offline Channel Scan	Enabled

Select an active profile to manage. Tap the WEP Keys button to enter WEP information. If a key is already entered, the Already set? checkbox is checked. The previously entered key value is not displayed for security.

Firmware Tab

Displays the current firmware version and allows you to load new firmware. Tap the Browse button to locate the new firmware file.

Status Tab

Immediately runs status on signal strength and signal quality.

Statistics Tab

Select the Receive Stats or Transmit Stats. The data is displayed on the screen.

Survey Tab

Immediately runs signal strength and quality and link speed. An option is available to Setup parameters for Active Mode reporting.

Cisco Wireless Security

- Wi-Fi Protected Access (WPA) is only available on mobile device's equipped with the updated Cisco client driver (release 2.60 or later).
 - WPA requires software revision 1ED or greater. To identify the software revision, tap on the About icon in the Control Panel.
 - Refer to the *LXE Security Primer* to prepare the Authentication Server and Access Point for MX5X communication.
 - 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.
-

System Requirements

To support Wi-Fi Protected Access (WPA), the mobile device must be equipped with a Cisco 350 wireless card with driver release 2.60 (or later).

The LXE MX5X supports WPA and all authentications. The Microsoft supplicant and Cisco supplicants are used separately or together to provide support for the different authentications.

Most of the configuration is done with the Microsoft Wireless Configuration tool.

WPA/LEAP requires the Cisco supplicant and Cisco ACU configuration tool.

Installing Cisco Wireless Client Drivers

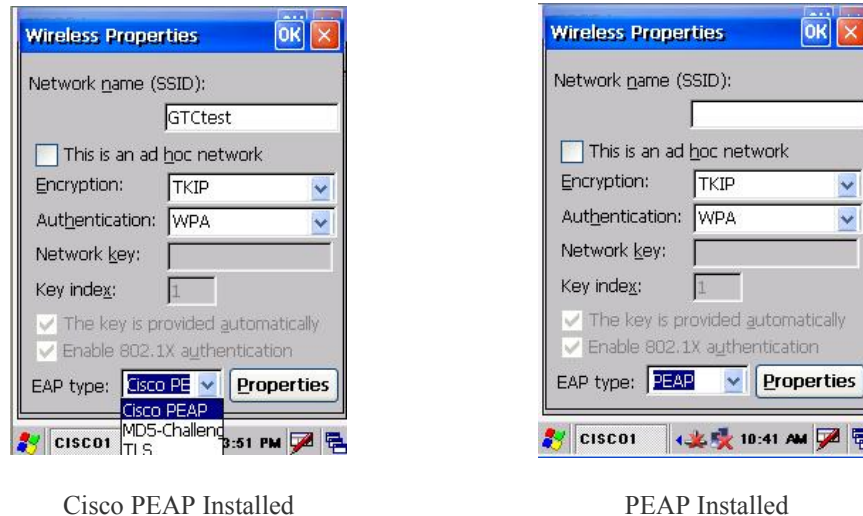
Which version of the Cisco client driver should be installed depends on what authentication protocol is to be configured.

- Cisco PEAP should not be installed if using PEAP/MSCHAP.
- Cisco PEAP must be installed if using PEAP/GTC.
- For all other authentications (LEAP, EAP-TLS, WPA-PSK) it does not matter if Cisco PEAP is installed or not.

To determine if Cisco PEAP is installed or to change the installation, refer to the instructions in the following sections.

Checking for the Cisco PEAP Supplicant

With a Cisco wireless device installed, open the Wireless network properties as described in *Wireless Network Configuration*, later in this chapter. With the Authentication tab selected check the text in the EAP type drop down box. Refer to the following figures to determine if Cisco PEAP is installed.



Cisco PEAP Installed

PEAP Installed

Figure 5-27 Cisco PEAP Authentications

If the Cisco installation is correct, continue with the configuration. If it is not correct, follow the procedures below.

Note: Instructions are also included in the README file located in the \SYSTEM folder.

There are two Cisco CAB files in the \SYSTEM folder of the MX5X. The default files are CISCO.CAB and CISCOPEAP.CAB.

The default CISCO.CAB file provides for all authentications except Cisco PEAP. When the default CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the previous figure labeled *PEAP Installed*.

If Cisco PEAP is desired:

1. Rename the CISCO.CAB file to CISCOMSCHAP.CAB.
2. Rename the CISCOPEAP.CAB file to CISCO.CAB.
3. Coldboot the mobile device to install the new driver with the registry.

The renamed CISCO.CAB file provides for Cisco PEAP and PEAP/GTC authentications. When the renamed CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the previous figure labeled *Cisco PEAP Installed*.

If it becomes necessary to switch to a different authentication than Cisco PEAP or PEAP/GTC,

1. Rename the CISCO.CAB file to CISCOPEAP.CAB.
2. Rename the CISCOMSCHAP.CAB file to CISCO.CAB
3. Coldboot the mobile device to install the new driver with the registry.

Cisco WPA Configuration

Use the following instructions for all authentication protocols to configure the Microsoft Wireless Network configuration utility unless WPA/LEAP is used.

WPA/LEAP is configured with the Cisco ACU (see section titled *WPA/LEAP Authentication Configuration*).

Tap the ACU icon on the desktop.

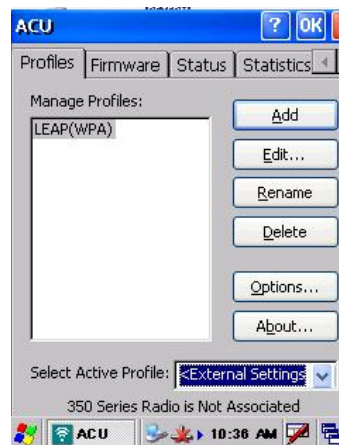


Figure 5-28 Cisco ACU Profile Selection

From the Select Active Profile pull down list, select <External Settings>.

Tap OK and warmboot.

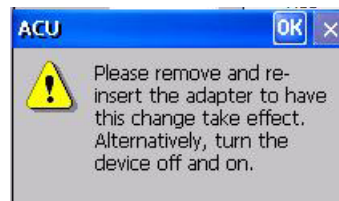


Figure 5-29 Cisco ACU Reboot Message

After booting up, the Microsoft Zero Config tool should start. If it does not, start configuring the wireless connection by tapping on the WZC icon (networked computers) in the toolbar.

The Wireless Network Connection screen appears.



Figure 5-30 Cisco Wireless Information Screen

Make sure the Notify me when new wireless networks are available box is *not* checked..

Tap the Advanced... button.

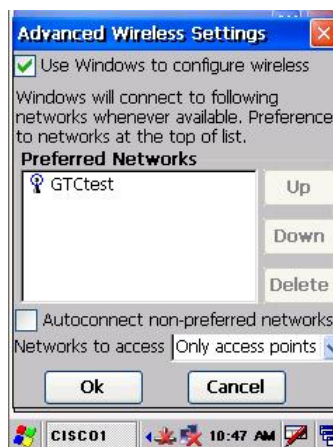


Figure 5-31 Cisco Advanced Wireless Settings

Make sure the Use Windows to configure my wireless settings box is checked.

Set the Networks to access drop down box to Only access points.

Tap the OK button on the Advanced Wireless Settings screen and the Wireless Information Screen is displayed.

On the Wireless Information screen tap the Add New ... line.

The Wireless Network Properties screen is displayed.



Figure 5-32 Cisco Wireless Network Properties

Enter the Network name (SSID) into the text field.

For PEAP/MSCHAP and EAP/TLS, set Encryption to TKIP and Authentication to WPA.

For WPA/PSK see WPA/PSK Authentication Configuration.

To configure the IEEE 802.1X Authentication box see the following sections for configuration of each authentication protocol.

PEAP/MS-CHAP Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/MS-CHAP protocol. The Cisco CAB file without Cisco PEAP must be used with PEAP/MS-CHAP. See *Installing Cisco Wireless Client Drivers*, earlier in this chapter, for more information.

Configuring the PEAP/MS-CHAP Supplicant



Figure 5-33 Cisco PEAP/MSCHAP Wireless Network Properties

With the wireless parameters configured (see *Wireless Network Configuration* in this chapter) set the EAP type to PEAP as shown above.

If the EAP type box text is not exactly as shown see *Installing Cisco Wireless Client Drivers* in this chapter, to change the wireless client CAB file.

Tap the Properties button.



Figure 5-34 Cisco Authentication Settings

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, come back to this screen and validate the server certificate.

The login screen appears for logging into the wireless network.



Figure 5-35 Cisco Wireless Network Login

Once authenticated, tap the IP Information tab.

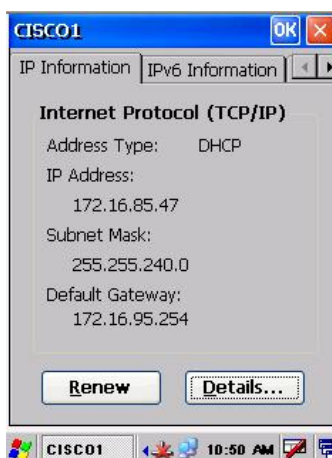


Figure 5-36 Cisco IP Information Tab

If the network is set to use DHCP, the mobile device displays the IP address assigned by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see *Root Certificates*, in this chapter.



Figure 5-37 Cisco Authentication Settings, Validate Server

Navigate to the Wireless Network Properties configuration screen.

Tap the Properties button.

Check Validate server.

Tap OK to dismiss the configuration boxes.



Figure 5-38 Cisco Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Tap on the IP Information tab and make sure there is a valid IP address as shown in the figure labeled *IP Information Tab*, earlier in this chapter.

PEAP / GTC Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/GTC protocol.

Configuring the PEAP/GTC Supplicant



Figure 5-39 Cisco PEAP/GTC Wireless Network Properties

With the client parameters configured (see *Wireless Network Configuration* in this chapter) set the EAP type to Cisco PEAP as shown above.

If the EAP type box text is not exactly as shown, see *Installing Cisco Wireless Client Drivers* in this chapter, to change the wireless client CAB file.

Tap the Properties button.



Figure 5-40 Cisco Authentication Settings

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, return to this screen and validate the server certificate as shown later in this section

The login screen appears for logging into the wireless network.



Figure 5-41 Cisco Wireless Network Login

Enter valid user credentials.

Once authenticated, tap the IP Information tab.

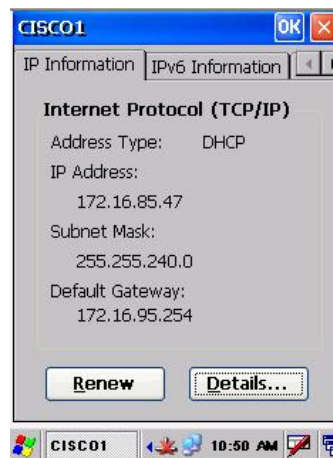


Figure 5-42 Cisco IP Information Tab

If the network is set to use DHCP, the mobile device displays the IP address assigned by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see *Root Certificates*, in this chapter.

Navigate to the Wireless Network Properties configuration screen.

Tap the Properties button.



Figure 5-43 Cisco Authentication Settings, Validate Server

Check Validate server.

Tap OK to dismiss the configuration boxes. If the login screen appears, enter valid user credentials.



Figure 5-44 Cisco Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the SSID, as shown in the figure above.

Tap on the IP Information tab and make sure there is a valid IP address as shown in the figure labeled *IP Information Tab* in this section.

WPA/LEAP

LEAP is a Cisco proprietary authentication protocol and is not supported by the Microsoft supplicant. To configure the mobile device for WPA/LEAP, use the Cisco ACU installed during normal installation of the Cisco client driver.

Cisco ACU

Start the Cisco ACU by tapping the icon on the desktop or navigate to Start | Programs | Cisco | ACU.

Tap on the Profile tab.

Tap the Rename button.

Name the profile.



Figure 5-45 Cisco Renaming Profile

Tap the Edit . . . button.

The profile properties screen is displayed.



Figure 5-46 Cisco Profile Properties Screen

Enter the SSID and Client Name in the correct fields.

Set the Network Security Type to LEAP(WPA).

Tap the OK button and the Profiles tab is displayed again.

Use the drop down box to choose the profile just configured.

Tap OK.

The mobile device associates and displays the sign on screen.



Figure 5-47 Cisco Login Screen

Tap the Status tab to display status.

EAP-TLS Authentication Configuration

To authenticate using the EAP-TLS protocol you need a user certificate file and a private key file. Once you have the user certificate files run the certificate installer from the Microsoft control panel. For EAP-TLS it does not matter which Cisco cab file is installed.

Note: It is important that all dates are correct on CE mobile devices when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificate

To check if a user certificate is installed navigate to Start | Control Panel | Certificates.



Set the drop down box to My Certificates as shown below.

The correct user certificate should be shown in the pane.

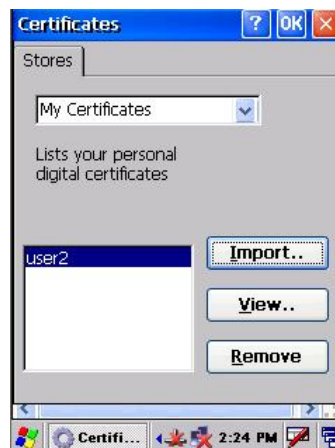


Figure 5-48 Cisco Certificate Stores

Tap the View . . . button.

Set the Field to Private Key.

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.

If there is no user certificate refer to *User Certificates* in this chapter, to acquire a user certificate and private key file.

Setting EAP/TLS Parameters

With the client parameters configured (see *Wireless Network Configuration*) set the EAP type to TLS as shown.



Figure 5-49 Cisco EAP/TLS Configuration

Tap the Properties button.



Figure 5-50 Cisco Authentication Settings

Tap the Select button to choose the user certificate.

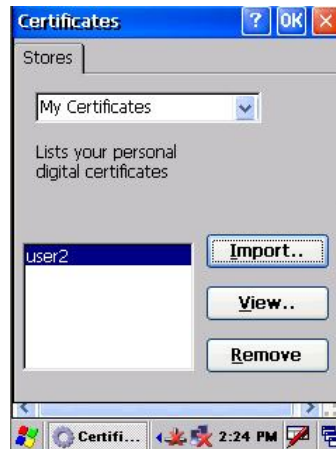


Figure 5-51 Cisco Select Certificate



Figure 5-52 Cisco Authentication Settings, Certificate Details

Do *not* check the Validate server certificate box. This allows the user to be authenticated as the first step.

When the user certificate successfully authenticates, come back to this screen and validate the server certificate as described in the next section.

Tap the OK button to dismiss the configuration screens. When the client re-connects the user is authenticated with the user certificate.

If the user does not authenticate, recheck the user certificate and the date on the computer.

Validating the Server Certificate

Before validating the server certificate, make sure the Root CA certificate is installed on the mobile device.

Navigate to the Wireless Network Properties configuration screen.

Tap the Properties button.

Check the Validate server box as shown below.



Figure 5-53 Cisco Validate Server

Tap OK to dismiss the configuration boxes.



Figure 5-54 Cisco SSID Authenticated

Once the authentication completes the status changes to show the mobile device has authenticated to <SSID> as shown above.

WPA PSK Configuration

Configure the Wireless Network Settings as described in *Wireless Network Settings* in this chapter.

Change the Network Authentication to WPA-PSK.

Enter an ASCII network key in the text field. Hex keys do not work in the Microsoft Zero Config utility at this time.

There is no server authentication when using WPA-PSK.

Tap the OK button to complete the configuration.

Symbol Client

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards unless noted otherwise.

Prerequisites

- Windows CE .NET 4.2 operating system
- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

Access: Tap the Network Connected Icon in the Status Bar

IP Information Tab

After the IP Address has been assigned to the mobile device, tap the Renew button to renew the IP address if necessary. Tap the Details button to view the Network Connection details.

IPv6 Information Tab

This is the TCP/IPv6 information screen. The contents cannot be edited by the user.

Configuring IPv6

By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up. To disable IPv6, run `\Windows\ipv6Disable.reg` and perform a warmboot. To enable IPv6, run `\Windows\ipv6Enable.reg` and perform a warmboot. Contact your LXE representative for `ipv6Disable.reg` and `ipv6Enable.reg` availability.

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

Wireless Information Tab

Factory Default Settings	
Wireless Information tab	
Notify when new networks available	Enabled
Advanced Button	
Use Windows to configure wireless settings	Enabled
Automatically connect to non-preferred networks	Disabled
Networks to access (Only Apps, Only comp-to-comp)	All available
Encryption (WEP, TKIP)	WEP
Authentication (WPA, Open, Shared, WPA-PSK)	WPA
Ad hoc network	Disabled
Key provided automatically	Enabled
Enable 802.1X authentication	Enabled
EAP Type (MDF-Challenge, PEAP, TLS)	TLS

View Log

Displays the logon/connection data for the current network connection.

Add a new connection

Select Add New. Enter the ESSID in the Network Name text box.

Disable WEP

- If WEP is to be disabled, tap the down arrow in the Authentication drop down box. Select Open.
- Tap the down arrow in the Encryption drop down box. Tap Disabled and WEP is disabled.
- Tap the OK button to return to the Wireless Information tab.

Enable WEP

- Tap the down arrow in the Authentication drop down box.
- Tap the WEP Authentication protocol.
- If the key is provided automatically by your network, check the Key provided automatically checkbox.
- If you wish to enter your Authentication key, uncheck the Key provided automatically checkbox and enter the Network Key in the Network Key text box.
- Tap the OK button to return to the Wireless Information tab.

Continue

Tap the Advanced ... button. Make sure there is a checkmark in the Use Windows to configure my wireless settings checkbox. Make sure there is *no* checkmark in the Automatically connect to non-preferred networks checkbox. Tap the Connect button.

Tap OK to return to the Wireless Information tab.



Tap the Connect button.

To access NETWLAN1 Properties again, tap the Network Connected icon in the Toolbar.

Select a User Certificate

1. Select Wireless Information Tab.
2. Select a network by doubletapping the network name.
3. In the IEEE 802.1X Authentication box, enable 802.1X authentication
4. Select an EAP type.
5. Tap the Properties button. Validate Server is enabled by default.
6. At the Authentication Settings display, tap the Select button to choose a User Certificate.

Certificates

	<p>Please refer to the <i>LXE Security Primer</i> to prepare the Authentication Server and Access Point for communication.</p>
 <p>Date/Time</p>	<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>

Root Certificates

Download a Root CA Certificate

The easiest way to get the root CA certificate is to use a browser on a desktop PC to navigate to the CA (Certificate Authority). To request the root CA certificate, open a browser to

`http://<CA IP address>/certsrv`

Sign into the CA with any valid username and password.

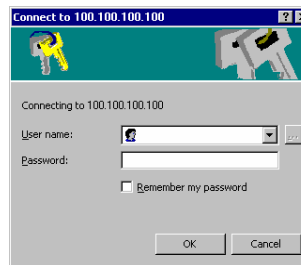


Figure 5-55 Logon to Certificate Authority

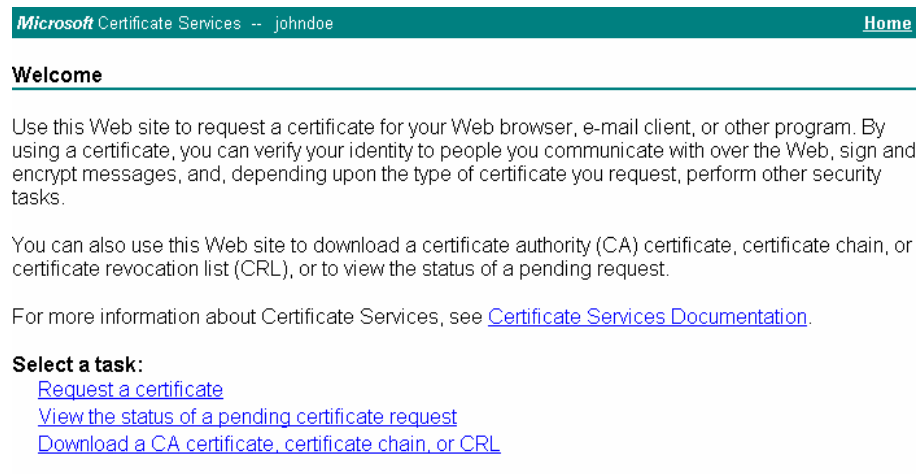


Figure 5-56 Certificate Services Welcome Screen

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.

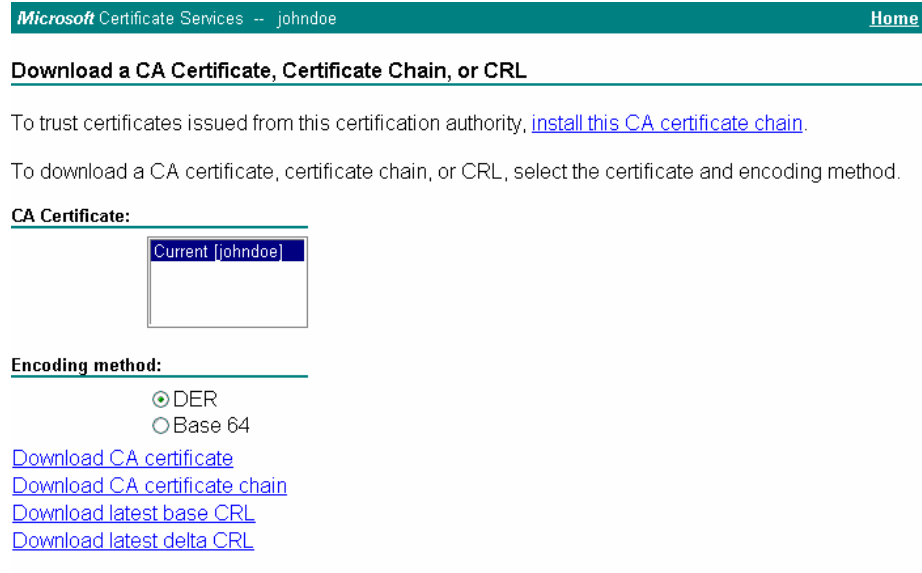


Figure 5-57 Download CA Certificate Screen

Tap the DER button.

To download the CA certificate, tap on the Download CA certificate link.

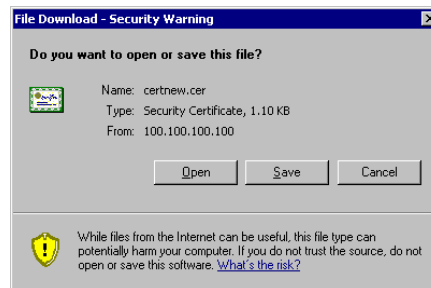


Figure 5-58 Download CA Certificate Save to Desktop

Tap the Save button and save the certificate to the desktop PC. Keep track of the name and location of the certificate as the certificate file name and file location is required in later steps.

Installing a Root CA Certificate on the Mobile Device

Copy the certificate file from the desktop PC to the mobile device. Import the certificate by navigating to Start | Control Panel | Certificates.



Figure 5-59 Certificate Stores

Tap the Import button.

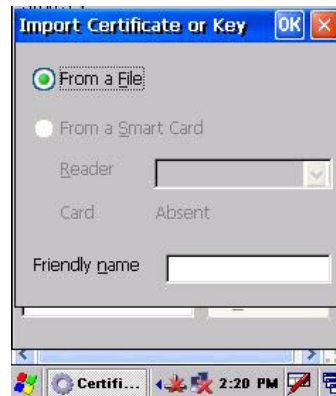


Figure 5-60 Import Certificate From a File

Make sure From a File is selected and tap OK.



Figure 5-61 Browsing to Certificate Location

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

Tap Yes to import the certificate.

Once the certificate is installed, return to the proper authentication section, described later in this chapter.

User Certificates

Generating a User Certificate for the MX5X

The easiest way to get the user certificate is to use a browser on a PC to navigate to the CA. To request the user certificate, open a browser to

`http://<CA IP address>/certsrv`

Sign into the CA with the username of the user certificate required.



Figure 5-62 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. CE devices such as the MX5X require the private key to be saved as a separate file rather than including the private key in the user certificate.

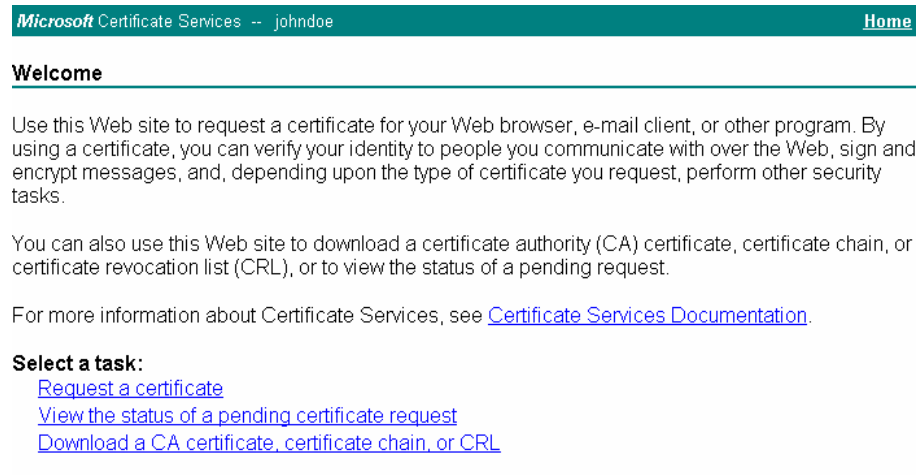


Figure 5-63 Certificate Services Welcome Screen

Tap the Request a certificate task link.

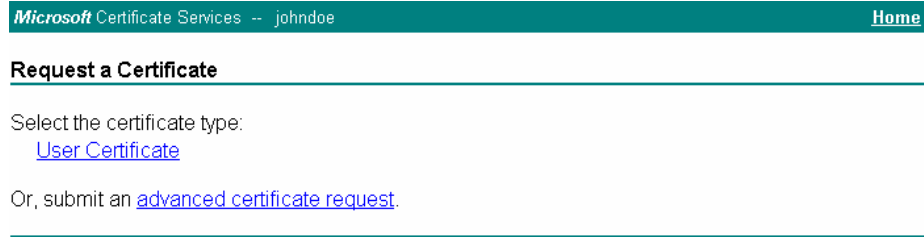


Figure 5-64 Request a Certificate Type

Tap on the advanced certificate request link.

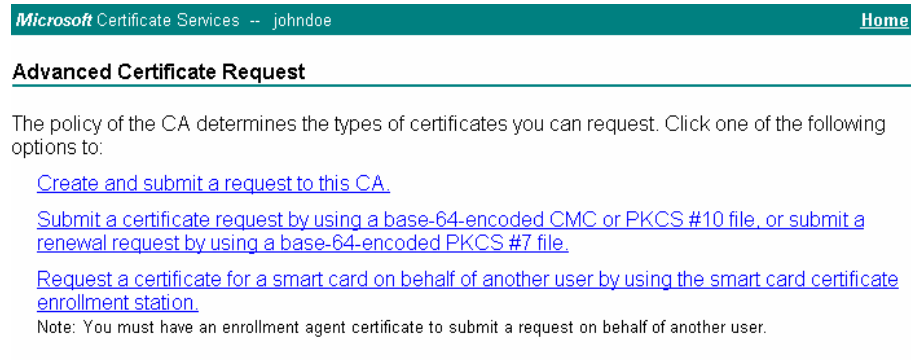


Figure 5-65 Advanced Certificate Request Screen

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:

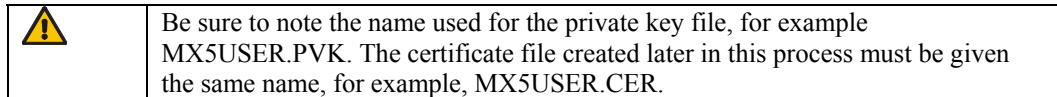
Submit >

Figure 5-66 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.



DO NOT check Enable strong private key protection.

Make any other desired changes and tap the Submit button.

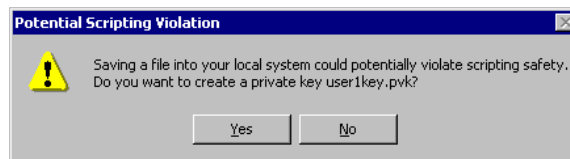
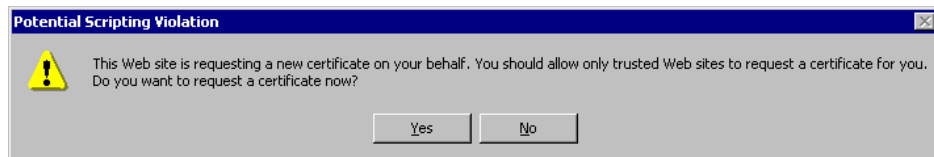


Figure 5-67 Script Warnings

If any script notifications occur, tap the Yes button to continue the certificate request.



Figure 5-68 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.

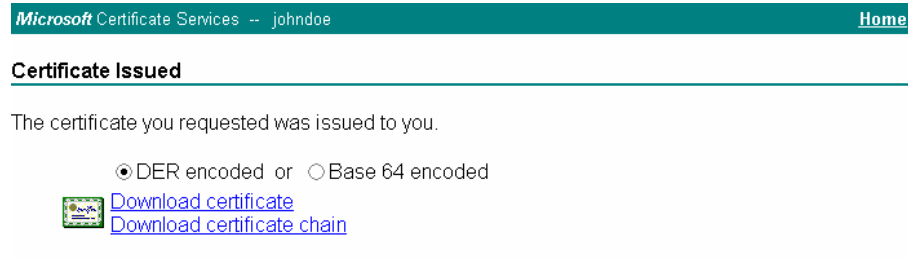


Figure 5-69 User Certificate Issued

Tap the Download certificate link.

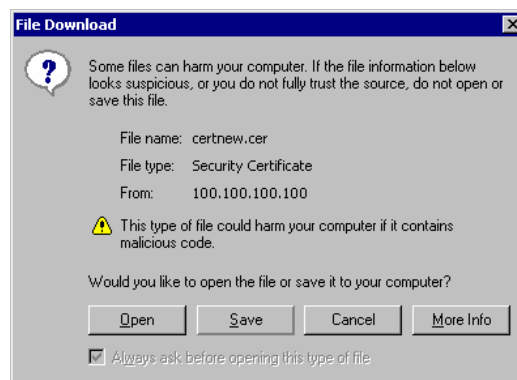



Figure 5-70 Download Certificate Security Warning

Tap Save to download and store the user certificate to the PC. Keep track of the name and location of the certificate as the file name and location is required in later steps. The private key file is also downloaded and saved during this process.

	Be sure use the same name for the certificate file as was used for the private key file. For example, if the private key was saved as MX5USER.PVK then the certificate file created must be given the same name, for example, MX5USER.CER.
---	--

Installing a User Certificate on the MX5X (WPA-TLS Only)

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to Start | Control Panel | Certificates.



Select My Certificates from the pull down list.

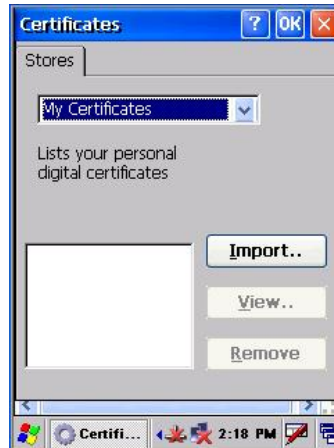


Figure 5-71 Certificate Stores

Tap the Import button.

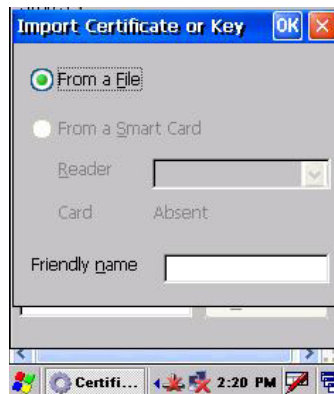


Figure 5-72 Import User Certificate

Make sure From a File is selected and tap OK.



Figure 5-73 Browsing to Certificate Location

Using the explorer buttons, browse to the location on the mobile device where you copied the certificate, select the certificate desired and tap OK.

Tap Yes to import the certificate.

The certificate is now shown in the list.



Figure 5-74 User Certificate Listing

Highlight the certificate you just imported and tap the View. . button.

From the Field pull down menu, select Private Key.

If the private key is present, the process is complete.

If the private key is not present, import the private key.

To import the private key, tap OK to return to the Certificates screen.
Tap import.



Figure 5-75 Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to Private Keys, select the certificate desired and tap OK.

Tap on View to see the certificate details again.

The private key should now say Present. If it does not, there is a problem. Possible items to check:

Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.

Make sure the certificate and private key file have the same name, for example mx5user.cer for the certificate and mx5user.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.



Chapter 6 AppLock

Introduction

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

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

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified application is automatically launched and runs in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact your LXE representative for assistance, downloads and update availability.

Determine Your AppLock Version

If the Administrator Control Menu looks like this ...



Go to ...

Appendix C –
Reference Material,
AppLock – Single
Application Version



This chapter.

Figure 6-1 Determine Your AppLock Version

Setup a New Device

Prerequisites:

- The touch panel must be enabled. Refer to the (*Start | Settings | Control Panel | Handheld | Misc |*) Touch Panel Disabled setting.
- An MX5X default input method (Input Panel, Transcriber, or custom input method) is assigned.

LXE CE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

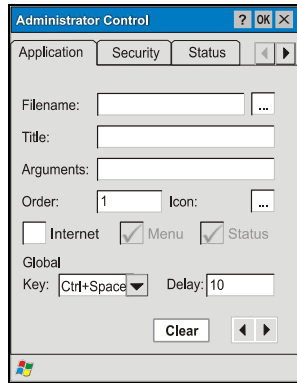
Briefly, the process to configure a new device is as follows:

1. Insert a fully charged battery and press the Power button. See *Chapter 1 – Introduction* for instruction.
2. Connect an external power source to the device (if required). See *Chapter 1 – Introduction* for instruction.
3. Adjust screen display, audio volume and other parameters if desired. Install accessories (e.g. handstrap, stylus). See *Chapter 1 – Introduction* for instruction.
4. Tap *Start | Settings | Control Panel | Administration* icon.
5. Assign a Switch Key (hotkey) sequence for AppLock. See *Security Panel*.
6. Assign an application on the Application tab screen. More than one application can be assigned. See *Application Panel*.
7. Assign a password on the Security tab screen. See *Security Panel*.
8. Select a view level on the Status tab screen, if desired. See *Status Panel*.
9. Tap OK.
10. Press the Switch Key sequence to launch AppLock and lock the configured application(s).
11. The device is now in end-user mode.

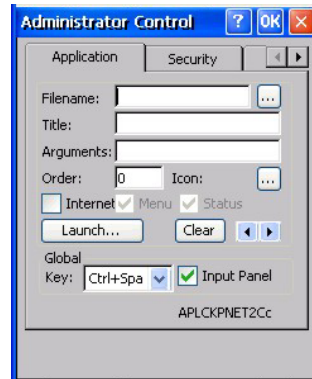
Note: LXE has made the assumption, in this appendix, that the first user to power up a new mobile device is the system administrator.

Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.

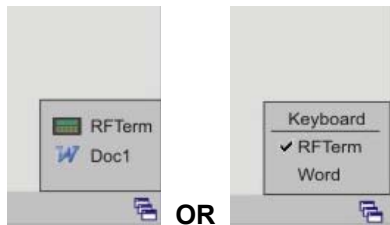
See Also: Appendix C – Reference Material, sections titled AppLock Error Messages and AppLock Registry Settings.



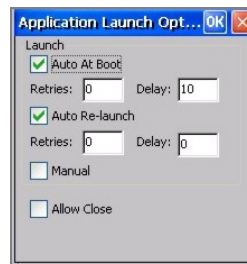
OR



Application Panel



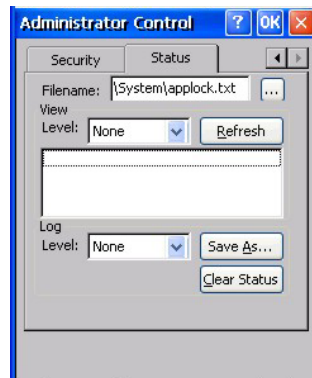
End User Switchpad



Application – Launch Panel



Security Panel



Status Panel

Figure 6-2 AppLock Panels

Administration Mode

Administration mode gives full access to the device and configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application, or applications, to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	Shift+Ctrl+A
Password	none
Application path and name	none
Application command line	none

End User Mode

End-user mode locks the end-user into the configured application (or applications). The end user can still reboot and respond to dialog boxes. The single application is automatically launched, and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user taps on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three attempts) to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

See Also: Appendix C – Reference Material, sections titled AppLock Error Messages and AppLock Registry Settings.

AppLock Password Troubleshooting

Can't locate the password that has been set by the administrator? Enter this LXE back door key sequence:

Ctrl+L Ctrl+X Ctrl+E

End-User Switching Technique

Note: The touch screen must be enabled. Refer to Start | Settings | Control Panel | Handheld | Misc | Touch Panel Disabled setting.

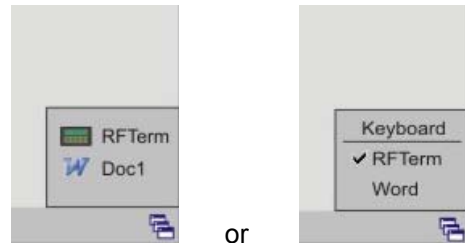


Figure 6-3 Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX5X default input method (Input Panel, Transcriber, or custom input method) is activated.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the taskbar. The taskbar is always visible on top of the application in focus. Note: If only one application is configured and the Input Panel is not enabled, the Switchpad icon is not displayed.

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

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

See Also: Application Panel | Launch | Manual (Launch) and Allow Close

Using the Switch Key Sequence

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

See Also: Application Panel | Global Key

Multi-Application Configuration

Access:  | Settings | Control Panel | Administration icon

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Note: *AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.*

Application Panel

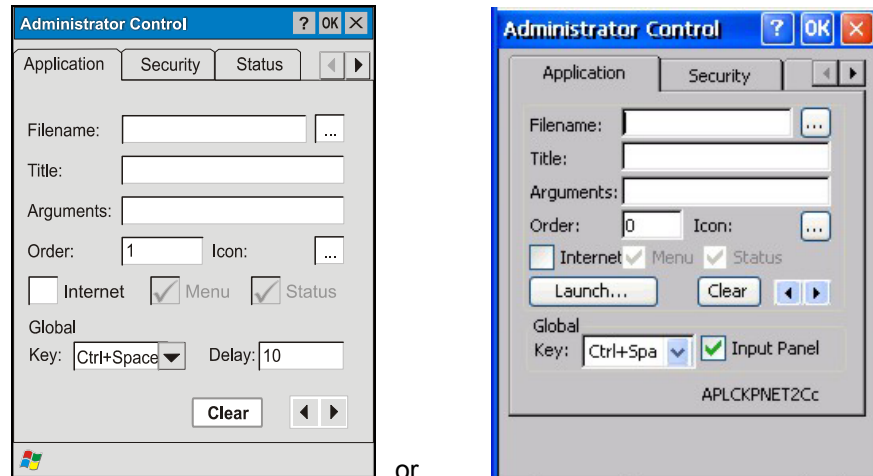


Figure 6-4 Application Panel – Multi-Application

Note: *If your Application Panel does not look like the figures shown above, you may have the Single Application version. Refer to Appendix C – Reference Material, AppLock - Single Application Version for instruction.*

Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the application switcher panel.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.

Option	Explanation
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button. <i>Note: AppLock Administrator Control panel file Launch option does not interrelate 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 Activation 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.

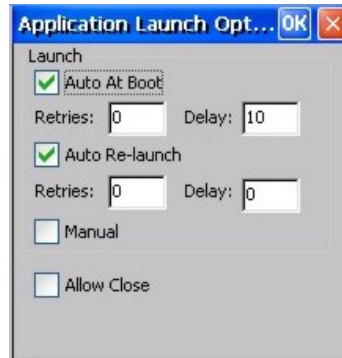


Figure 6-5 Application Launch Options

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.

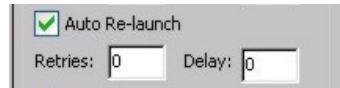
The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before 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 6-6 Security Panel – Multi-Application

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.

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 user modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Setting a Password in the Security Panel

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords and Troubleshooting Multi-Application AppLock

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

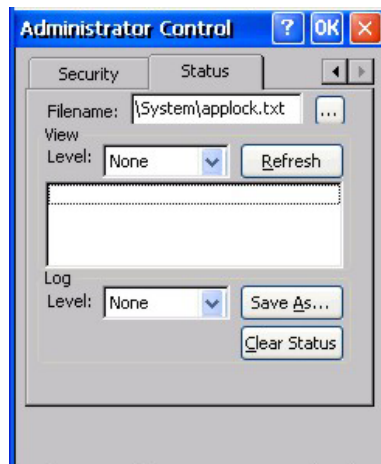


Figure 6-7 Status Panel – Multi-Application

Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

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

The default is None.

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.

Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None (default)
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'... button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

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 two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

See Also: *Appendix C – Reference Material*, sections titled *AppLock Error Messages* and *AppLock Registry Settings*.

Appendix A Key Maps

Keypad



ANSI / Batch Keypad

Remember :

The Orange (on the left) and Blue (on the right) keys are *2nd function* keys.

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.

Key Map 101-Key Equivalencies

Note: This key mapping is used on hand held computers that are NOT running RFTerm.

- 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.

Note: 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 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctrl	Alt	Shft	Caps Lock	
Power / Suspend							Power
Volume Adjust	x						V
Backlight Toggle for Display and Keypad	x						Right Scan Key
Adjust Backlight Brightness Down ⁴		x					7
Blue Mode							Blue
Orange Mode							Orange
Start button	x						Right Arrow
Shift							Shft
Alt							Alt
Ctrl							Ctrl
Scan							Left Scan Key or Right Scan Key ⁵
Esc	x						Alt
Space							Spc
Enter							Enter
CapsLock (Toggle)	x						Tab
Back Space		x					Spc
Tab							Tab
BackTab		x					Tab
Break	x						B
Pause	x						P
Print Screen	x						R
Scroll Lock	x						S
Up Arrow							Up Arrow
Down Arrow							Down Arrow
Right Arrow							Right Arrow
Left Arrow							Left Arrow
Insert	x						I
Delete		x					DOT
Home		x					Left Arrow
End		x					Right Arrow
Page Up		x					Up Arrow

⁴ Backlight must be toggled On. Once the backlight is off, the Blue key / Right Scan key sequence toggles the backlight on and at it's brightest intensity.

⁵ Both Scan keys are programmable. Before using as Scan key, make sure key has been programmed to Scan. See section titled "Programmable Buttons."

To Get This Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctrl	Alt	Shft	Caps Lock	
Page Down		x					Down Arrow
F1		x					1
F2		x					2
F3		x					3
F4		x					4
F5		x					5
F6		x					6
F7		x					7
F8		x					8
F9		x					9
F10		x					0
F11	x						1
F12	x						2
F13	x						3
F14	x						4
F15	x						5
F16	x						6
F17	x						7
F18	x						8
F19	x						9
F20	x						0
F21		x			x		1
F22		x			x		2
F23		x			x		3
F24		x			x		4
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 Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctrl	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
. (DOT)							DOT
<	x						G
[x						Y
]	x						Z
>	x						H
=	x						T
{	x						W
}	x						X
/	x						J
-	x						Spc
+	x						DOT
*		x					I
: (colon)		x					D

To Get This Key / Function	Press These Keys and Then ...						Press This Key
	Blue	Orange	Ctrl	Alt	Shft	Caps Lock	
; (semicolon)		x					F
. (period)		x					K
?		x					L
`		x					N
_ (underscore)		x					M
, (comma)		x					J
' (apostrophe)		x					H
~ (tilde)		x					B
\		x					S
		x					A
“		x					G
!		x					Q
@		x					W
#		x					E
\$		x					R
%		x					T
^		x					Y
&		x					U
(x					O
)		x					P

IBM Keypad Overlays



3270 Keypad Overlay

Please refer to the *RFTerm Reference Guide* for further information about 3270 key functions on the mobile device.

Note: The MX5X device approved for use in Hazardous Locations has a blue keypad overlay with the same 3270 keymap markings as shown in this figure.

3270 Keypad

Legend	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
Dup	Duplicate	Ctrl + U
E-Inp	Erase Input	Ctrl + Q
Fld -	Field Minus	Ctrl + M
Fld +	Field Plus	Ctrl + L

Legend	Explanation	Key Sequence
Ins	Insert	Ctrl + I
LDub	Ctrl + B	Not Supported
RDub	Ctrl + F	Not Supported
NL	New Line	Ctrl + N
PA1	PA1	Ctrl + 1
PA2	PA2	Ctrl + 2
PA3	PA3	Ctrl + 3
Reset	Reset	Ctrl + R
SysReq	System	Ctrl + S



5250 Keypad Overlay

Please refer to the RFTerm Reference Guide for further information about 5250 key functions on the mobile device.

Note: The MX5X device approved for use in Hazardous Locations has a blue keypad overlay with the same 5250 keymap markings as shown in this figure.

5250 Keypad

Legend	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
Dup	Duplicate	Ctrl + U
E-Inp	Erase Input	Ctrl + Q
FBk	Fast Back Ctrl + B	Not Supported
FFwd	Fast Forward Ctrl + F	Not Supported
Fld -	Field Minus	Ctrl + M
Fld +	Field Plus	Ctrl + L
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
SysReq	System	Ctrl + S

Appendix B Technical Specifications

Physical Specifications

Features		Specifications	Comments	
CPU		Intel Xscale operating at 400 MHz	32 bit CPU (with on-chip cache)	
Memory	ROM RAM	64 MB Flash (N/A January 2006) 128 MB low power DRAM	40 MB available for programs and data System Memory	
Display	LCD	Transflective Color	Transflective LCD with touchscreen. Customer Configurable Display and Keypad Backlighting	
Mass Storage	Removable CF Card (Customer Installable)	ATA Flash Type II PC Cards (Various Sizes)	Type I Compact Flash Card ATA Flash PC Card, or ATA Hard Drive PC Card	
PCMCIA Interface		One PCMCIA Slot: Slot 0 accepts Type II Slot 1 accepts Type I and II CF	Compatible with the PCMCIA version 2.1 standard.	
Weights		Unit with network card, battery and scanner endcap	1.7 lbs	800g
		Battery	6.4 oz	180 g
		Wireless Card - 2.4GHz Type II	1.0 oz 1.6 oz	28g 45g
		Compact Flash Card	1 oz	28g
External Connectors/Interface		IrDA Connector (COM 3) bi- directional half-duplex	Supports 115k baud	
		RS-232 COM1 mini D serial port (left)	26 Position D (female) Connector. Provides connection to external devices such as a powered cradle, printer, USB cable, AC power supply cable.	
		RS-232 COM4 mini D serial port (right)	26 Position D (female) Connector. Provides connection to external devices such as a powered cradle, printer, AC power supply cable.	
Audio/Microphone Connector			Audio Jack	
Dimensions		Length	9.6"	24.3 cm
		Width	4"	10.1 cm
		Depth	2.1"	5.4 cm
Scanner		No Scanner Symbol SE 1224 Fuzzy Logic Symbol SE 1223 Long Range Symbol SE 1223 Adv Long Range Symbol SE 2223 2D Scanner	Integrated	
Batteries	Main	Li-Ion battery pack 7.4V 2.8Ah	In-Unit Chargeable or Externally Chargeable	
	Backup (CMOS)	Internal Nickel Metal Hydride (NiMH) 5.7V 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	

Display Specifications

Feature	Specification
Type	LCD - Transflective Color / CCFL Front Light
Resolution	320 x 240 pixels
Size	1/4 VGA portrait
Diagonal Viewing Area	3.8 in (150.4mm)
Dot Pitch	0.22mm
Dot Size	0.20mm x 0.20mm
Color Scale	Reflective – 256 colors

Environmental Specifications

MX5X

Feature	Specification
Operating Temperature	-6°F to 140°F (-21°C to 60°C)
Storage Temperature	-60°F to 160°F (-51°C to 71°C)
Water and Dust	IP67
Operating Humidity	Up to 90% non-condensing at 140°F (60°C)
Standards	See Appendix B in the <i>MX5X User's Guide</i> .
Contamination	Resistant to exposure to skin oil and other lubricants.
Vibration	Based on MIL Std 810F
ESD	8 KV air, 4kV direct contact
Shock	Multiple 2 meter (6.6') drops to concrete.

AC Wall Adapter

Feature	Specification
Input Power Switch	None
Power "ON" Indicator	LED
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	26 position D serial interface
Output Voltage	+12VDC, unregulated
Output Current	0 Amps min, 3.75 A max
Operating Temperature	32° F to 104° F / 0° C to 40° C
Storage Temperature	-13° F to 158° F / -25° C to 70° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

Network Card Specifications

Summit Client 2.4GHz Type II

Bus Interface:	Compact Flash via a PCMCIA adapter
Network Frequencies:	2.4 - 2.4897 GHz IEEE 802.11b 802.11g DSSS OFDM
RF Data Rates:	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level:	18 dBm 64mW Max
Channels	11 US, 13 Europe, 13 Japan
Operating Temperature	see <i>MX5X Environmental Specs</i>
Storage Temperature	see <i>MX5X Environmental Specs</i>
Connectivity:	Novell, TCP/IP, Ethernet, ODI

Symbol Client 2.4GHz Type II

Bus Interface:	PCMCIA 2.0, Type II slot
Network Frequencies:	2.4 - 2.5 GHz IEEE 802.11b DS SS
RF Data Rates:	11 Mbps maximum
RF Power Level:	100 mW
Channels	11 US, 13 Europe, 4 France, 1 Japan
Operating Temperature	see <i>MX5X Environmental Specs</i>
Storage Temperature	see <i>MX5X Environmental Specs</i>
Connectivity:	TCP/IP, Ethernet, NDSI

Cisco Client 2.4GHz Type II

Bus Interface	PCMCIA 2.0, Type II slot
Network Frequencies	2.4 - 2.4835 GHz IEEE 802.11b DS SS
RF Data Rates	11 Mbps
RF Power Level	100 mW max.
Channels	11 US, 13 Europe, 4 France, 14 Japan
Operating Temperature	see <i>MX5X Environmental Specs</i>
Storage Temperature	see <i>MX5X Environmental Specs</i>
Connectivity	TCP/IP, Ethernet, NDSI
Antenna	Internal

Appendix C Reference Material

Introduction

Contents of this Appendix include:

- AppLock – Single Application Configuration.
- Includes information and instruction for an MX5X using AppLock to manage a single application. AppLock error messages and registry settings are also included.
- MX5X Reference Guide Revision History

and the following charts:

- Valid VK Codes for CE .NET and CE Devices
- ASCII Control Codes
- Hat Encoding
- Decimal-Hexadecimal Chart

AppLock - Single Application Configuration

Access:  | Settings | Control Panel | Administration icon

LXE's AppLock is designed to be run on LXE certified Windows CE .NET / 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.

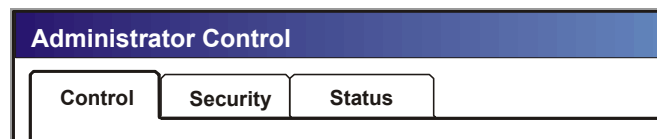
End-user mode locks the end-user into the configured application. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified application is automatically launched and run in full screen mode when the device completes the boots up process.

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.

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

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 an application to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Insert a fully charged battery and press the Power button. 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. Install accessories (e.g. handstrap, stylus). See *Chapter 1 – Introduction*.
4. Tap  | Settings | Control Panel | Administration icon.
5. Assign a hotkey switching sequence.
6. Assign an application on the Control tab screen. See *Control 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: LXE has made the assumption, in this appendix, that the first user to power up a new mobile device is the system administrator.

Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.

Administration Mode

Administration mode gives full access to the device and configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application, or applications, to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	Shift+Ctrl+A
Password	none
Application path and name	none
Application command line	none

End User Mode

End-user mode locks the end-user into the configured application (or applications). The end user can still reboot and respond to dialog boxes. The single application is automatically launched, and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user taps on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the 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

Single 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 tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

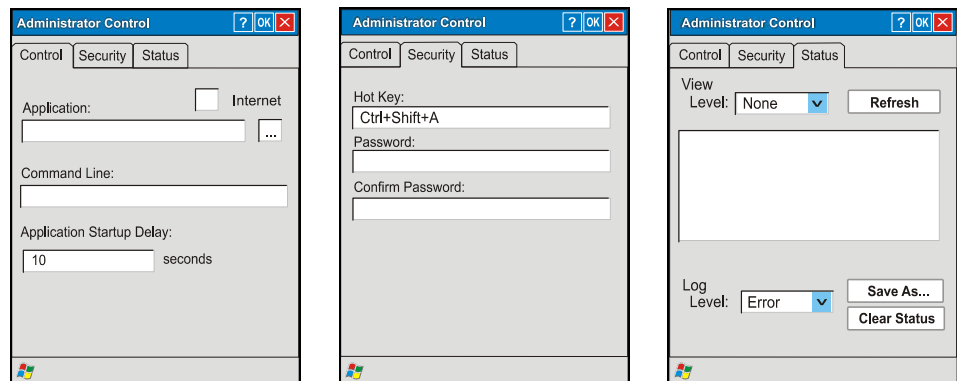
The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Administrator Control Panels

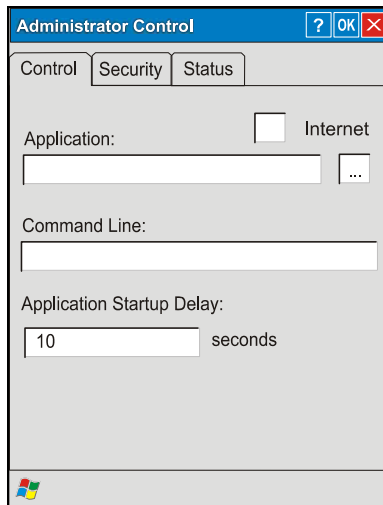
Access:  | Settings | Control Panel | Administration icon

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

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.

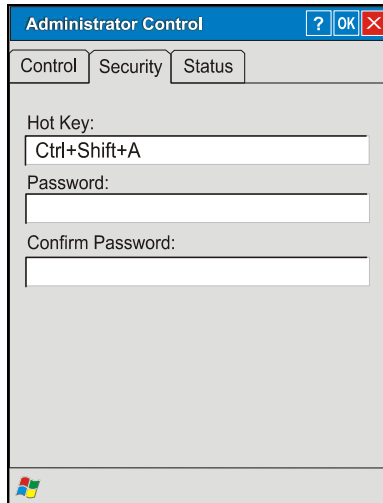
End User Internet Explorer

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

Specify a Hotkey Sequence

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

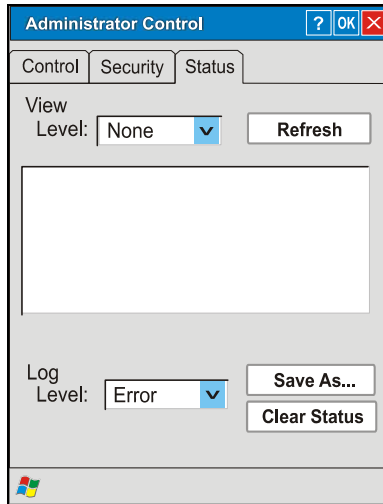
Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

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

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: 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
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

Message	Explanation and/or corrective action	Level
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
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

Message	Explanation and/or corrective action	Level
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
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
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

Message	Explanation and/or corrective action	Level
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. . If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the "Registry read failure" above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCMG 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
CAN	17	^X	CANcel line	Ctrl-x

Char	Hex	Control-Key	Control Action	
EM	19	^Y	End of Medium	Ctrl-y
SUB	1a	^Z	SUBstitute	Ctrl-z
ESC	1b	^[ESCape	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1b VK_PACKET up VK_CONTROL up
FS	1c	^\	File Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1c VK_PACKET up VK_CONTROL up
GS	1d	^]	Group Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1d down WM_CHAR (0x1d) up VK_PACKET up VK_CONTROL up
RS	1e	^^	Record Separator	VK_CONTROL (0x11)down VK_SHIFT (0x10) down WM_CHAR 0x36 down WM_CHAR 0x36 up VK_SHIFT up VK_CONTROL up
US	1f	^_	Unit Separator	VK_CONTROL (0x11) down VK_SHIFT (0x10) down VK_PACKET (0xe7) down WM_CHAR 0x1f VK_PACKET (0xe7) up VK_SHIFT (0x10) up VK_CONTROL (0x11) up

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded
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	^?
	0x80	~^@
	0x81	~^A
	0x82	~^B
	0x83	~^C
IND	0x84	~^D
NEL	0x85	~^E
SSA	0x86	~^F

Desired ASCII	Hex Value	Hat Encoded
ESA	0x87	~^G
HTS	0x88	~^H
HTJ	0x89	~^I
VTS	0x8A	~^J
PLD	0x8B	~^K
PLU	0x8C	~^L
RI	0x8D	~^M
SS2	0x8E	~^N
SS3	0x8F	~^O
DCS	0x90	~^P
PU1	0x91	~^Q
PU2	0x92	~^R
STS	0x93	~^S
CCH	0x94	~^T
MW	0x95	~^U
SPA	0x96	~^V
EPA	0x97	~^W
	0x98	~^X
	0x99	~^Y
	0x9A	~^Z
CSI	0x9B	~^[
ST	0x9C	~^\\
OSC	0x9D	~^]
PM	0x9E	~^^
APC	0x9F	~^_ (Underscore)
(no-break space)	0xA0	~ (Tilde and Space)
¡	0xA1	~!
¢	0xA2	~"
£	0xA3	~#
¤	0xA4	~\$
¥	0xA5	~%
¦	0xA6	~&
§	0xA7	~'
¨	0xA8	~(
©	0xA9	~)
ª	0xAA	~*
«	0xAB	~+
¬	0xAC	~,
(soft hyphen)	0xAD	~- (Dash)

Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded
®	0xAE	~. (Period)
—	0xAF	~/
°	0xB0	~0 (Zero)
±	0xB1	~1
²	0xB2	~2
³	0xB3	~3
´	0xB4	~4
µ	0xB5	~5
¶	0xB6	~6
·	0xB7	~7
¸	0xB8	~8
¹	0xB9	~9
º	0xBA	~:
»	0xBB	~;
¼	0xBC	~<
½	0xBD	~=
¾	0xBE	~>
¿	0xBF	~?
À	0xC0	~@
Á	0xC1	~A
Â	0xC2	~B
Ã	0xC3	~C
Ä	0xC4	~D
Å	0xC5	~E
Æ	0xC6	~F
Ç	0xC7	~G
È	0xC8	~H
É	0xC9	~I
Ê	0xCA	~J
Ë	0xCB	~K
Ì	0xCC	~L
Í	0xCD	~M
Î	0xCE	~N
Ï	0xCF	~O
Ð	0xD0	~P
Ñ	0xD1	~Q
Ò	0xD2	~R
Ó	0xD3	~S
Ô	0xD4	~T
Õ	0xD5	~U
Ö	0xD6	~V

Desired ASCII	Hex Value	Hat Encoded
×	0xD7	~W
Ø	0xD8	~X
Ù	0xD9	~Y
Ú	0xDA	~Z
Û	0xDB	~[
Ü	0xDC	~\
Ý	0xDD	~]
Þ	0xDE	~^
ß	0xDF	~_ (Underscore)
à	0xE0	~`
á	0xE1	~a
â	0xE2	~b
ã	0xE3	~c
ä	0xE4	~d
å	0xE5	~e
æ	0xE6	~f
ç	0xE7	~g
è	0xE8	~h
é	0xE9	~i
ê	0xEA	~j
ë	0xEB	~k
ì	0xEC	~l
í	0xED	~m
î	0xEE	~n
ï	0xEF	~o
ð	0xF0	~p
ñ	0xF1	~q
ò	0xF2	~r
ó	0xF3	~s
ô	0xF4	~t
õ	0xF5	~u
ö	0xF6	~v
÷	0xF7	~w
ø	0xF8	~x
ù	0xF9	~y
ú	0xFA	~z
û	0xFB	~{
ü	0xFC	~
ý	0xFD	~}
þ	0xFE	~
ÿ	0xFF	~^?

Hat Encoded Characters Hex AE through FF

Decimal – Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42 ⁶	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)⁶ 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 C, Dec 2006

Notices	Updated trademark statements.
Chapter 1 – Introduction	<p>Added “Troubleshooting” to “Getting Started”. Added Right Arrow + Blue key as the Start button key sequence to troubleshooting.</p> <p>Added Multi AppLock activation key instruction “Entering the Multi AppLock Activation Key”.</p> <p>Added “Manuals” section. Noted obsolescence of MX5 PPC device.</p> <p>Updated Accessories. Added ROHS information. Added separate accessory sections for MX5 CE .NET standard and MX5 CE .NET I-SAFE mobile device.</p>
Chapter 3 – System Configuration	<p>Added sections titled “JAVA (Option)”, “RFTerm (Option)”, “AppLock (Option)” and “Wavelink Avalanche Enabler (Option)”.</p> <p>Added Summit client to “Start Menu Program Options”.</p> <p>Added “Determine Your Scanner Software Version” chart at beginning of “Control Panel Scanner” section.</p> <p>Noted the newest scanner applet is now in Chapter 4 “Scanner”.</p> <p>Added “Wavelink Avalanche Enabler Configuration”.</p>
Chapter 4 – AppLock	Renumbered to Chapter 6.
Chapter 4 – Scanner	New.
Chapter 5 – Wireless Network Configuration	<p>Added Summit client. Separated chapter into four sections: Summit Client, Cisco Client, Symbol Client, and Certificates.</p> <p>Added “Sign-on Screen for LEAP, PEAP/MS-CHAP, PEAP/GTC”.</p> <p>Added configuration instruction for PEAP/GTC on Summit devices.</p> <p>Updated parameters and options based on Summit version 1.2.10 differences.</p>
Chapter 6 – AppLock	Renumbered from Chapter 4 (now Scanner). Added Multi AppLock application instruction.
Appendix A – Keymaps	Added Right Arrow + Blue key as the Start button key sequence.
Appendix B – Technical Specifications	<p>Added note about 64M flash not available after 2005.</p> <p>Added “Hat Encoding” and “Decimal-Hexadecimal Chart” for Chapter 4 “Scanner” user. Added “Revision History” section. Added technical specifications for Summit client device.</p>
Entire Manual	<p>Changed “radio” to “wireless” or “client” in context, where applicable. Changed chapter cross-references to match Chapter number changes. Updated equipment figures to show new LXE logo on equipment.</p>

Revision B, Nov 2005

Entire Manual	Added note (for backward compatibility) to all references to “Bluetooth”: <i>Note Bluetooth access, modules and Bluetooth Manager are not supported by LXE.</i>
Chapter 1 – Introduction	Added explanatory note to “Tapping the Touchscreen with a Stylus” <i>right mouse click</i> function. Removed headset with microphone from “Accessories”. Added Neoprene trigger handle cover to “Accessories”.
Chapter 3 – System Configuration	Added “2.4GHz Radio Configuration” section and “Configuring IPv6”. Updated “Audio” section to reflect differences between initial bootloader release and upgraded bootloader release. Added “How to Disable Touch and / or Calibration upon Cold Reset”. Added “How to Enable Touch and / or Calibration upon Cold Reset” to “Handheld” section. Updated Scanner panels with barcode wedge additions. Added updated Bootloader Version panel information to “Handheld” section. Added “Transcriber”. Removed “Cisco – Aironet Configuration Utility (ACU)” and “Symbol” sections. This information is now included in Chapter 5 “Wireless Network Configuration”. Updated miscellaneous Figures.
Chapter 5 – Wireless Network Configuration	Added new chapter containing ACU and Symbol sections removed from Chapter 3. Added WPA information and instruction.
Appendix A – Key Maps	Added clearer pictures and 3270/5250 keymapping sequences.

Revision A, Initial Release, Dec 2004

Index

2, 3, 5

2 nd key function	48
3270 key functions.....	240
5250 key functions.....	241

A

About	
software, hardware, version, network IP.....	80
AC External Power Supply, How to.....	16
AC Power	
and LEDs on cradles	58
Accessibility settings	74
Accessing Files on CF Card	50
Accessories	
Electrostatic Discharge	8
Installing	8
ActiveSync	109
Backup Data Files	109
Cold Boot and Loss of Host Re-connection.....	111
Connect	108, 109
Create Comm Option	87
Explore.....	110
Troubleshooting.....	111
ActiveSync Help.....	68, 106
ActiveSync Options.....	111
ActiveSync Setup Wizard.....	106, 107
ActiveSync version 3.7.....	106
Add Prefix	97
Add Suffix	97
adjust speaker volume	23
Admin Hotkey	
AppLock	225
Administration	
AppLock	74
Administrator	
Summit client utility.....	157
Advanced tab	
Scanner properties.....	97
Align touch screen.....	20
Allow Close.....	229
Allow Connection.....	89
Alt key function.....	48
API calls	105
API.CAB	104
Application Panel	225
AppLock	24
EUIE	229
Passwords.....	223

Setup	219
Single Application.....	248
AppLock Administrator.....	62
ASCII Control Codes.....	263
At Power On	
Password protect	89
ATA CF Card file access.....	39
Audio	23, 51
Audio Interface location	35
Audio jack location.....	22
Audio/Microphone Connector	244
Authenticate using the EAP-TLS protocol	199
Auto hide	71
Avalanche Enabler.....	63
installation.....	115
Avalanche Enabler Configuration	115

B

Background and Window colors	79
Backlight Timer.....	21
Backlight timers.....	79
Backup and restore	113
Backup Battery	
Time Limit	54
Backup battery information	91
Backup Data Files.....	109
Barcode	
Enable or Disable	138
Barcode data match list.....	143
Barcode processing overview	132
Barcode Scanner	
Integrated	41
Tethered	41
Barcode scanner decode symbologies	41
Barcode Tab.....	138
Batteries.....	244
Battery	
Backup	55
Charger.....	56
Charging.....	34
Handling Safely	54
Lithium-Ion (Li-Ion)	34
Low Warning timing.....	53
Nickel Metal Hydride (NiMH).....	34
Battery Auto Turn Off	79
Battery Chargers.....	56
Battery Charging LED location	16
Battery Life	
Approximate	54
Battery status LED explanation.....	55

Battery tab	91
Battery voltage.....	37
Battery, Main.....	53
Baud Rate	131
Bluetooth Manager	105
Bootloader versions	81, 83

C

CAB files.....	104
Cable connections	
COM1 and COM4.....	42
Calibrate touchscreen	20
Calibration	101
Calibration disabled.....	80
Caps mode function.....	49
Cautions and Warnings	
Hazardous Location	7
CE .NET 4.2 or CE 5.0.....	1
Certificates.....	76
Root CA.....	206
User.....	210
Certificates are date sensitive	153, 186
Change the MX5X Time and Date	36
Change virtual keys	136
Character Recognition	
Touch screen.....	70
Charger	
Battery.....	56
Charger, battery	56
Charging Battery	
Time Required	34
Check the battery status and power reading	15
Cisco	
PEAP Supplicant.....	187
Cisco Client	185
Cisco Network Card Specifications.....	245
CISCO.CAB	187
Clean display and aperture.....	51
Clear Contents of Document Folder	71
Cold Reset	36
Color display timer expires.....	21
Color displays.....	50
Color screen	
Backlight.....	79
COM port settings tab.....	99, 137
COM Ports.....	93, 131
Configurations.....	35
COM Ports described.....	40
Command Prompt.....	69
Commit button	
Config	158
Communication	
ActiveSync.....	68
Get Connected.....	68
Remote Desktop Connection.....	69
compact flash card location	37

Compact Flash Cards, CAB Files and Programs ..	104
Compact flash memory.....	34
Components.....	11
Config buttons	159
Config parameters	
Summit.....	160
Connect External PS.....	16
Connect Using	89
Contacting LXE.....	29
Control characters.....	146
Control Panel options	72
Controls, Physical.....	36
Copied at startup.....	65
Copyrights	103
Core Logic	33
CPU Xscale	33
Cradles.....	58
Create a dialup, direct, or VPN connection	87
Ctrl Char mapping	138
Ctrl Char Mapping.....	146
Ctrl key function.....	48
Current Time	77
Custom ID parameters	148
Custom identifiers.....	138
Custom IDs.....	148
Custom Parameter Option.....	164
Customize dates, times, currency	92

D

Data entry	26
Data Loss	
Backup Battery.....	2
Cold Reset.....	8
Daylight Savings	77
Decimal – Hexadecimal Equivalent	
0 – 159	267
160 – 255	268
default value for the battery power timer.....	21
default value for the external power timer	21
Delay	86
Desktop.....	8, 64
Desktop cradle	58
Determine scanner software version.....	131
Determine Your Scanner Software Version	93
Device Name and description.....	103
Diagnostics	163
Diags tab	
Summit.....	163
Dialup properties for dial up access.....	78
Dimensions	244
Disable ActiveSync with Enabler.....	121
Disable Enabler launch	124
Display	
Features.....	50
Pixels.....	50
Specifications.....	244

display and the keypad backlights	22
Display Backlight Timer	50
Display owner notes	21
Display setting with Enabler	125
Display Timer	50
Document Conventions	3

E

EAP-FAST Authentication, Summit	175
EAP-TLS Authentication Configuration	199
electrostatic discharge	8
Electrostatic Discharge	37
Enable Code ID	139
notes	139
Enable or Disable specific symbology	138
Enabler	
communication	118
installation	115
Enabler Configuration	115, 118
Enabler Uninstall Process	115
End user switching	
Touch	24, 224
Enter key function	47
Entering Data	26
Environmental Specifications	244
Hazardous Location	7
Error Messages	
AppLock	256
Ethernet port	40, 58
EUIE	229
Example	
Barcode processing	150
Control Code replacement	149
Expand Control Panel	71
External Auto Turn Off	79
External PS	16

F

Factory Default Settings	
Cisco Client	185
Symbol Client	205
Failure	
Battery Pack	55
Features	5
Field Exit key function	48
Files preserved upon reboot	66
Flash Cards	
Install and remove	38
Flash Specifications	34
Folders	
copied at startup	65
My Computer	65
My Device	66
Function	

2 nd Key	48
Alt Key	48
Caps Mode	49
Ctrl Key	48
Enter Key	47
Field Exit Key	48
Scan Key	47
Shft Key	48
Spc Key	48

G

General	102
Getting Started	8
Getting the Most from Your Batteries	55
Global parameters	165
Glossary	29
graphics modes	34

H

Handle, Installation	17
Handling Batteries	54
Handstrap, Install	18
Hardware	
Configuration	33
Hardware version	186
Hat Encoded Characters	265
Hatch	
CF Card file access	39
PC Card file access	39
Hazardous Location, Please Read	7
Headset	51
Help	29, 154
Hexadecimal – Decimal Equivalent	
0x00 to 0x9F	267
0xA0 to 0xFF	268
Host Connection prerequisites	10
Hot Swapping Main Battery	54
Hotkey	
AppLock	230
HyperTerminal, ActiveSync	112

I

Icons	
Explorer, Internet	64
My Computer - My Device	64
My Documents	64
Recycle Bin	64
Start	64
Transcriber	64
Wireless Client Setup	64
Idle Time	79
IEC IP65	244
IEC IP67	7

Important Battery Information.....	2
Inbox	
Outlook	69
Increase or Decrease Keypad and Display Backlight Intensity	22
Indicators	
LEDs	46
Infrared (IR) port, described	43
Input Panel.....	84
Install ActiveSync on Desktop or Laptop.....	107
Install LXEbooks.....	25
Integrated scanner barcode reading parameters	36
Integrated Scanner Programming Guide.....	41
Internet Explorer	
AppLock	229
Network card and ISP required	69
Internet Options	
CE .NET 4.2.....	85
CE 5	86
IO Components.....	33
IPv6 Broadcast Messages	204
IR operating envelope.....	43
IR Port	
bi-directional half-duplex.....	43
IRDA (Infrared Data Access).....	43
iRescue program	113

J

JEM-CE.....	63
JmpStart.....	37

K

Keyboard	
Onscreen only	84
Keyboard 0409	86
Keymaps.....	235
Keypad.....	47
Keypad and entering data	26
Keypad Shortcuts.....	20
Keys tab.....	96, 135

L

LEAP without WPA Authentication, Summit	174
Li-Ion battery life.....	15
Link speed	130
List configured ActiveSync connections	89
Lithium Ion battery warning.....	2
Lithium-Ion (Li-ion).....	53
Logging	
AppLock	232
Loss of Host Re-connection.....	111
Low Battery Warning	55
LXE Manuals CD	29

LXE Security Primer	153, 206
LXE_MX5X.....	63
LXE_MX5X_ENABLER.CAB.....	115
LXEbook – MX5X Users Guide	25

M

Main.....	93, 131
Main Battery	
and Critical Suspend state	54
Hot Swapping.....	54
Main Battery Pack	54
Main tab	
Summit.....	156
Manage wireless settings with Enabler.....	127
Match List.....	144
Match List Rules.....	144
Media Player.....	70
Memory	102
allocate for programs or storage.....	102
Memory installed.....	102
Menu Options	
Start.....	67
Microsoft Wireless Network configuration utility.....	188
Mode	
Off.....	46
On.....	45
Suspend.....	46
Mode Key Functions	49
Modes	
AppLock	222
MX5X family of computers.....	4, 29
My Computer	
Folders	66

N

Network Card Specifications.....	245
Network ID for Owner	88
No Security	
Summit.....	172

O

Off Mode	46
ON Mode characteristics	45
Operating Temperature.....	244
Hazardous Location	7
US AC to DC	244
Optional Software	
JAVA	63
RFTerm.....	63
WaveLink Avalanche Enabler	63
Owner	
Identification.....	88
Notes	88

Owner information	21
<hr/>	
P	
Parts is Parts	11
Password.....	89
AppLock	223
Passwords	
AppLock Save As	232
PC Card	37
Storage	38
PC Card Management software	34
PC Cards	
Install and remove.....	38
PCMCIA.....	37
PCMCIA Slots.....	37
PEAP MSCHAP Authentication, Summit.....	177
PEAP/GTC Authentication Configuration	194
PEAP/MS-CHAP Authentication Configuration.....	191
PEAP-MSCHAP for WPA	177
Pen Stylus	20, 50
Pen Stylus and data entry.....	26
Persistent Storage Memory.....	104
Phillips Screwdriver and handstrap	19
Physical Specifications	243
Pin 9 Power.....	93
Pin 9 power unavailable	131
Pistol Grip Handle	17
Pocket PC 2002 API calls.....	105
Port 1 and Port 2	35
Port, Infrared.....	43
Power key	36
Power key location	14
Power Off timer default settings.....	22
Power Port 1 while asleep.....	95, 134
Power Properties.....	91
Power Supply	
Battery Packs	34
Power Supply, AC/DC	57
Prefix and Suffix.....	98
Prefix and Suffix control	145
Pre-loaded Files	61
Processor speed	33
Programmable Buttons	44
Programmable keys	
Setup	96, 135
Prompt	
Command.....	69
<hr/>	
Q	
Quick Start Instructions	8
<hr/>	
R	
Rate.....	86

Reboot	36
Recalibration.....	101
Re-enable Touch and / or Calibration upon Cold	
Reset	80
Reference Material	247
Regional settings, defaults	92
Registry	96
Registry and save settings.....	10
Release/Renew button	163
Remote desktop connection.....	69
Remove user installed programs.....	92
Repeat	86
Replacing PCMCIA cards	38
Reset warm and reset cold	36
<i>Revision Level</i>	
Hardware.....	186
Summit	154
RTerm	63
RTerm access	10
RJ45 Ethernet port	40
Root CA Certificates	
Generating.....	206
Installing on mobile device	208
RS-232	
Data Entry	28
RS-232 Pinouts.....	42
Rules	
Match list	144
<hr/>	
S	
Save settings.....	10
Scan	
Good and Bad Scan sounds.....	99, 135
Scan button, reprogram.....	44
Scan buttons	
and tethered scanners	41
Scan key function	47
Scan Keys	
Left and Right	93
SCANBAD.WAV.....	99, 135
ScanCodeLeft and ScanCodeRight.....	96
SCANGOOD.WAV	99, 135
Scanner Advanced	93
Scanner Code ID notes	133
Scanner Control Characters Tab	146
Scanner engine type.....	244
Scanner LED illuminated	41, 131
Scanner LED, functioning	27
Scanner range	41
Scanner, factory defaults	131
Scanning and data entry.....	27
Schemes tab.....	91
SCU Help.....	154
SE1223, SE1224 or SE2223	36
Security options, supported	153
Security Panel	

-
- AppLock 230
 - Send Key Messages (WEDGE) 41
 - Send Key Messages and Wedge 95, 134
 - Set the double-click sensitivity for stylus taps 87
 - Set up RFTerm 10
 - Setup
 - AppLock 219
 - Setup new device
 - AppLock 220
 - Setup Software 61
 - Shift key function 48
 - Show Clock 71
 - Shutdown time limits 55
 - Site Survey 164
 - Soft Keyboard 84
 - Soft keypad, virtual keyboard 28
 - Software and Files 61
 - Software Load 62
 - Space key function 48
 - Speaker 51
 - Speaker volume, How to 52
 - Specifications
 - Environmental, Hazardous Location 7
 - SSID 160
 - Standard keypad illustrated 235
 - Start Menu 67
 - Shutdown 64
 - Start Ping 163
 - Status panel 130
 - Status Panel
 - AppLock 231
 - Stop the Enabler Service 116
 - Storage Manager
 - devices 100
 - Storage Temperature 244
 - US AC to DC 244
 - Store data 26
 - Stored certificates 76
 - Storing PC Cards 38
 - Strip Leading and Strip Trailing 97
 - Strip leading and trailing controls 142
 - Stylus 50
 - Stylus and data entry 26
 - Stylus properties 101
 - Stylus sensitivity 101
 - Stylus, How to 20
 - Suffix and Prefix 98
 - Summit
 - EAP-FAST Authentication 175
 - LEAP without WPA Authentication 174
 - No Security 172
 - PEAP GTC Authentication 181, 183
 - PEAP MSCHAP Authentication 177
 - WEP keys 173
 - WPA LEAP Authentication 179
 - WPA PSK Authentication 180
 - Summit Client configuration 154
 - Summit client utility 154
 - Summit client utility (SCU)
 - Config tab 158
 - Diags tab 163
 - Status tab 162
 - Summit Network Card Specifications 245
 - Summit tray icon 155
 - Suspend button 64
 - Suspend mode 46
 - Suspend mode and ActiveSync 36
 - Suspend Mode key 14
 - Switch active scanner Com port 41
 - Switching COM ports 40
 - Symbol Network Card specifications 245
 - Symbology settings 138, 140
 - Sync Clock for Enabler 123
 - Synchronizing from the MX5X 68
 - System Configuration 61
 - System Hardware Configuration 33
 - System Requirements, WPA 186
-
- T**
- TCP/IPv6 information 204
 - Technical Specifications 243
 - Terminal Emulator, connect 10
 - Tethered scanner
 - Data entry 27, 42
 - Tethered Scanner
 - Setup using a Cradle 59
 - Tile 79
 - Time Zone 77
 - Toggle Backlight 22
 - Touch panel disabled 80
 - Touch Screen 20, 50
 - Keypad Shortcuts 20
 - Touch screen adjustment 20
 - Touch Screen and data entry 26
 - Touchscreen, stylus tap 20
 - Transcriber 70
 - Transflective Display 34
 - Translate All 146
 - Translate control codes 95, 97
 - Translate Control Codes 97
 - Troubleshooting
 - AppLock 233
 - Troubleshooting
 - ActiveSync 111
 - AppLock Password 223
 - Avalanche 130
 - Getting Started 9
 - Type of installed scan engine 41
-
- U**
- upgrade radio drivers 153
-

USB port.....	40
USB port pinout.....	43
Use Avalanche network profile	128
User Certificate on the MX5.....	215
User Certificates	
Generating.....	210

V

Vehicle cradle.....	58
Video Subsystem	
Display Characteristics	34
View	
Display	50
Virtual Key, change.....	96
Virtual keyboard.....	49
Virtual Keyboard.....	84
Virtual Keys	
modify.....	136
VK_Code List.....	262
Volume	
adjust audio volume	51, 52
adjustments	23

W

Wake the device from Suspend	64
Warm Reset	36
Warning	

Low Battery beeps	55
Wavelink Avalanche Enabler	
installation.....	115
Wavelink Avalanche Enabler Configuration	115
Wedge.....	95, 134
WEDGE.CAB	104
WEP Keys	
Summit.....	173
When to use this guide.....	2
Where is the ---	11
Windows Explorer.....	70
Windows version	102
Wireless network configuration.....	153, 188
Wireless Security	
Summit Client	168
Wireless Zero Config Utility	
Summit Client	155
WPA	
Supported Authentications	186
System Requirements.....	186
WPA LEAP Authentication, Summit	179
WPA PSK Authentication, Summit.....	180
WPA PSK Configuration.....	203
WZC icon	155

Z

Zero Config Utility, Microsoft	188
--------------------------------------	-----

