MX3X Reference Guide

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

LXE

E-EQ-MX3XRG-H

JAVA POWERED

Microsoft Windows Embedded

Notices

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

Copyright:

Trademarks:

Li-Ion Battery

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

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

	**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

Entire Manual	Added CE 5.0 information and instruction where applicable.
Chapter 5 – Wireless Network Configuration	Updated information for EAP-FAST support, Summit tray icon, help feature, etc., included in latest version of the Summit Client Utility.
Appendix A – Key Maps	Added 3270 and 5250 key sequence charts.

Table of Contents

CHAPTER 1 INTRODUCTION 1

Overview 1
- Features/Options for the MX3X Family 2
- Related Manuals 3

Components 4
- Front and Back Views 4
- Endcap Options 5
- MX3-RFID Module 5
- Battery Well Vent Aperture 6

When to Use This Guide 7
- Document Conventions 7

Getting Started 8
- Insert Main Battery 9
  - Check Battery Status 9
  - About Lithium-Ion Batteries 9
- Optional Devices 10
  - Attach Handstrap (Optional) 10
  - Attach the Stylus Clip (Optional) 10
  - Attach to Hip-Flip (Optional) 11
  - Connect External Power Supply to MX3X or Cradle (Optional) 12
  - Connect External Power Supply to the MX3P 13
    - MX3P Specific Power Accessories 13
    - 24/72 Maximum VDC MX3P Power Supply Input/Output Cable Connection 13
    - 12V VDC MX3P Power Cable Connection 15
  - Connect MX3X Audio Jack (Optional) 16
- Power Button 16
  - Restart Sequence 16
- Tapping the Touchscreen with a Stylus 17
  - Keypad Shortcuts 17
- Entering the Multi AppLock Activation Key 18
  - Touch 18
  - Hotkey 18
- Touchscreen Calibration 19
- Set The Display Contrast 20
- Set the Display Backlight Timer 20
- Set The Display Brightness 20
- Set the Power Schemes Timers 21
  - Battery Power Scheme 21
  - AC Power Scheme 21
- Set The Audio Speaker Volume 22
  - Using the Keypad 22
  - Using the Touchscreen 22

Setup the Client and Network 23

Access the Terminal Emulation Parameters 23

Installing PCMCIA and CF Cards 24

Installing / Removing Cards 25
Preparation 25
Installation 25
Removal 25
Enter Data 26
Keypad Entry 26
Stylus Entry 26
Input Panel 26
Integrated Laser Scanner Data Entry 27
Using a Headset and Voice for Data Entry 28
Connecting the Audio Cable and a Headset 28
Adjust Microphone and Secure the Cable 28
Entering Data 29
Tethered Scanner 29
MX3P and the MX3 Cradles 29
ActiveSync 30
Introduction 30
Initial Setup 31
Serial Connection 31
USB Connection 31
Network 31
IrDA Connection 32
Synchronizing from the Mobile Device 32
Connect and Communicate 33
Explore 33
Copy the MX3X LXEbook to the MX3X (Optional) 33
Backup Data Files using ActiveSync 34
Prerequisites 34
Serial Port Transfer 34
Infrared Port Transfer 34
USB Transfer 34
Connect 34
Disconnect 34
Cold Boot and Loss of Host Re-connection 35
ActiveSync with a Cradle 35
Troubleshooting ActiveSync 36
Docking Cradles 37
Status LED 37
Desktop Cradle 38
Connectors 38
Vehicle Mount Cradle 38
Connectors 38
ActiveSync with a Cradle 39
Tethered Scanner and a Cradle 39
The Passive Vehicle Cradle 39
Getting Help 40
Manuals 40
Accessories 40

CHAPTER 2 PHYSICAL DESCRIPTION AND LAYOUT 43

Hardware Configuration 43
Central Processing Unit 43
System Memory 43
Core Logic 44
Video Subsystem 44
Power Supply 44
Audio Interface 45
PCMCIA Slots 45
Slot 0 – Network or SRAM Cards 45
Slot 1 – Compact Flash Card 45
Power Modes 46
Primary Events Listing 46
On Mode 47
The Display 47
The Mobile Device 47
User Idle Mode 47
System Idle Mode 48
Suspend Mode 48
Critical Suspend Mode 49
Off Mode 49
Physical Controls 50
Power Button 50
Restart Sequence 50
Endcaps and COM Ports 51
Endcap Combinations 52
COM Port Switching 52
Integrated Scanner Port 53
Serial Port 53
LXE Connection Cable Technical Specification 54
RTS/CTS Handshaking and the Serial Port 54
USB Host / Client Port 55
USB Host Cable 55
ActiveSync 55
USB Client Cable 56
Tethered Scanners 56
Programmable Scan Buttons 57
Field Exit Key Function (IBM 5250/TN5250 Only) 57
Scan Buttons and the SCNR LED 57
The Keypad 58
Key Functions 58
Caps Key and CapsLock Mode 59
Keypad Shortcuts 59
Keypress Sequences 59
Custom Key Maps 60
LED Functions 61
Display 62
Display and Display Backlight Timer 62
Touchscreen 62
Cleaning the Glass Display/Scanner Aperture 63

Applying the Protective Film to the Display ... 63
Speaker ... 64
Infrared (IR) Port ... 64
Power Supply ... 65
Check Battery Status ... 65
Handling Batteries Safely ... 65
Main Battery ... 66
Battery Hot-Swapping ... 66
Low Battery Warning ... 66
Critical Suspend State ... 67
Backup Battery ... 67
Backup Battery Maintenance ... 67
Battery Chargers ... 68
MX3 Multi-Charger Plus ... 68
Important Battery Charger Version Information ... 69
Battery Chargers Affected ... 69
Battery Label Location ... 69
External Power Supply (Optional) ... 70

CHAPTER 3 SYSTEM CONFIGURATION 71

Introduction ... 71
Windows Operating System ... 71
2.4 GHz Network Configuration ... 71
Installed Software ... 71
Software Load ... 72
Software Applications ... 72
Optional ... 72
JAVA (Option) ... 72
LXE RFTerm (Option) ... 73
AppLock (Option) ... 73
Wavelink Avalanche Enabler (Option) ... 73
Desktop ... 74
My Computer Folders (CE .NET 4.2) ... 75
Folders Copied at Startup ... 75
My Device Folders (CE 5.0) ... 75
Start Menu Program Options ... 76
Communication ... 77
ActiveSync ... 77
Connect ... 77
Start FTP Server / Stop FTP Server ... 77
Command Prompt ... 78
Inbox ... 78
Internet Explorer ... 78
Media Player ... 78
Remote Desktop Connection ... 79
Transcriber ... 79
Windows Explorer ... 79
Taskbar ... 80
Advanced Tab ... 80

Settings | Control Panel Options 81
About 82
Language and Fonts 83
Identifying Software Versions 83
MAC Address 83
Accessibility 84
Administration – for AppLock 84
Battery 85
Bluetooth Manager 85
Certificates 86
Date/Time 87
Dialing 88
Display 89
Background 89
Appearance 89
Backlight 89
Input Panel 90
Internet Options 90
Windows CE .NET 4.2 90
Windows CE 5.0 91
Keyboard 92
Mixer 92
Mouse 93
Network and Dialup Connections 93
Create a Connection Option 93
Owner 94
Password 95
PC Connection 96
PCMCIA 97
Power 98
Battery 98
Schemes 99
Battery Power Scheme 99
AC Power Scheme 99
Device Status 99
Regional Settings 100
CE . NET 4.2 Default Settings 100
CE 5.0 Default Settings 100
Remove Programs 100
Scanner 101
Determine Your Scanner Software Version 101
Factory Default Settings 102
Main 103
Keys 104
Change a Virtual Key (F20 or F21) Value 105
COM Ports 105
Storage Manager 106
Stylus 107
Double Tap 107
Calibration 107
System 108

General 109
Memory 109
Device Name 110
Copyrights 110
Terminal Server Client Licenses 110
Volume and Sounds 111
Good Scan and Bad Scan Sounds 111
Utilities 112
LAUNCH.EXE 112
REGEDIT.EXE 115
REGLOAD.EXE 115
WARMBOOT.EXE 115
WAVPLAY.EXE 115
Enabling GrabTime 115
Disabling the Touchscreen 116
Configuring CapsLock Behavior 116
Configuring IPv6 116
Command-line Utility 117
COLDBOOT.EXE 117
PrtScrn.EXE 117
API Calls 117
Wavelink Avalanche Enabler Configuration 118
Briefly 118
Enabler Install Process 118
Enabler Uninstall Process 118
Stop the Enabler Service 119
Update Monitoring Overview 119
Mobile Device Wireless and Network Settings 120
Enabler Configuration 121
File Menu Options 122
Avalanche Update Settings 123
Menu Options 123
Connection 124
Execution 125
Server Contact 126
Startup/Shutdown 127
Scan Config 128
Display 128
Shortcuts 129
Adapters 130
Status 132
Troubleshooting 132
Reflash the Mobile Device 133
Preparation 133
How To : Reflash using Keypress Method 133
How To: Reflash using TAG file Method 134
Clearing Persistent Storage 134

CHAPTER 4 SCANNER 135

Introduction 135

Determine Your Scanner Software Version 135
Barcode Processing Overview 136
Barcode Manipulation 136
Main Tab 138
Keys Tab 139
Change a Virtual Key (F20 or F21) Value 139
COM Port Tabs 140
Barcode Tab 141
Buttons 141
Enable Code ID 142
Barcode – Symbology Settings 143
Strip Leading/Trailing Control 145
Barcode Data Match List 146
Barcode Data Edit Buttons 146
Match List Rules 147
Add Prefix/Suffix Control 148
Barcode – Ctrl Char Mapping 149
Translate All 149
Barcode – Custom Identifiers 150
Control Code Replacement Examples 152
Barcode Processing Examples 153
Advanced 154
Main Tab 155
Keys Tab 156
Change a Virtual Key (F20 or F21) Value 156
COM1, COM2, COM3 Tabs 157
Advanced Tab 158
Translate Control Codes 158
Strip Leading / Strip Trailing Characters 158
Prefix / Suffix 159
Barcode Tab 160
Prefix / Suffix 160
Strip Leading / Strip Trailing Characters 160
Prefix / Suffix 161
Interaction between Strip Leading/Trailing and Prefix/Suffix Settings 162
Ctrl Char Mapping 163
Translate All 163
Scancode Enable 164
Advanced Processing 165
Strip Code ID 166
Strip Identifiers from EAN128 Barcodes 166
Adding Codes to the Match List for EAN128 Barcodes 167

CHAPTER 5 WIRELESS NETWORK CONFIGURATION 169

Introduction 169
Summit Client Configuration 170
Summit Client Utility 170
Help 170
Summit Tray Icon 171
Wireless Zero Config Utility and the Summit Client 171

Main Tab 172
Administrator Login 173
Config Tab 174
Buttons 174
Config Parameters 175
Status Tab 177
Diags Tab 178
Buttons 178
Global Settings Tab 179
Global Parameters 179
Summit Wireless Security 182
Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP and PEAP/GTC 182
No Security 183
WEP Keys 184
LEAP w/o WPA Authentication 185
EAP-FAST Authentication 186
PEAP/MSCHAP Authentication 187
WPA/LEAP Authentication 189
WPA PSK Authentication 190
PEAP/GTC Authentication 191
Cisco Client Configuration 192
Aironet Client Utility (ACU) 192
Profile Parameters 193
Cisco Wireless Security 194
System Requirements 194
Installing Client Device Drivers 194
Checking for the Cisco PEAP Supplicant 195
Cisco WPA Configuration 196
PEAP/MS-CHAP Authentication Configuration 199
Configuring the PEAP/MS-CHAP Supplicant 199
Server Authentication 200
PEAP/GTC Authentication Configuration 202
Configuring the PEAP/GTC Supplicant 202
Server Authentication 204
WPA/LEAP 205
Cisco ACU 205
EAP-TLS Authentication Configuration 208
User Certificate 208
Setting EAP/TLS Parameters 209
Validating the Server Certificate 211
WPA PSK Configuration 212
Symbol Client Configuration 213
Profile Parameters Menu 213
Wireless Information Tab 214
View Log 214
Add a new connection 214
Disable WEP 215
Enable WEP 215
Continue 215
Select a User Certificate 216
Certificates 217

Root Certificates 217
Generating a Root CA Certificate 217
Installing a Root CA Certificate on the Mobile Device 219
User Certificates 221
Generating a User Certificate for the MX3X 221
Installing a User Certificate on the MX3X (WPA-TLS Only) 226

CHAPTER 6 APPLOCK 229

Introduction 229
Setup a New Device 229
Multi-Application Version 230
Single Application Version 231
Administration Mode 232
End User Mode 232
Passwords 233
Multi-Application Configuration 234
Application Panel 234
End User Internet Explorer (EUIE) 235
Security Panel 236
Password 237
Status Panel 237
End-User Switching Technique 239
Using a Stylus Tap 239
Using a Hotkey Sequence 239
Troubleshooting Multi-Application AppLock 240
Single Application Configuration 241
Control Panel 241
End User Internet Explorer 242
Security Panel 242
Status Panel 244
Error Messages 245
AppLock Registry Settings 254

APPENDIX A KEY MAPS 255

Keypad 255
Key Map 101-Key Equivalencies 255
3270 Key Sequences 259
5250 Key Sequences 259
Creating Custom Key Maps 260
Introduction 260
Programmable Scan Buttons and Custom Key Mapping 261
Keymap Source Format 261
COLxROWx Format 261
GENERAL Section 262
SPECIAL Section 262
MAP Section 263
Keycomp Error Messages 265
Sample Input File 269

Sample Output File 276
List of Valid VK Codes for CE .NET and CE 278

APPENDIX B TECHNICAL SPECIFICATIONS 279

Physical Specifications 279
Display Specifications 280
Cable Specifications 281
Cable Ends 281
Cable Pinouts and Diagrams 281
Environmental Specifications 283
Mobile Device and Endcaps 283
Power Supplies 283
US AC Wall Adapter 283
International AC Adapter 284
Network Device Specifications 285
Summit Client in PCMCIA Adapter 2.4GHz 285
PCMCIA Cisco Client 2.4GHz Type II 285
PCMCIA Symbol Client 11Mb 2.4GHz Type II 285
Hat Encoding 286
Decimal - Hexadecimal Chart 288
Revision History 290

INDEX 293

Illustrations

Figure 1-1 Front 4
Figure 1-2 Back 4
Figure 1-3 Endcaps 5
Figure 1-4 Side View 5
Figure 1-5 Vent Aperture in Battery Well – Do Not Cover 6
Figure 1-6 Battery Contacts and Main Battery 9
Figure 1-7 MX3X With Handstrap Installed 10
Figure 1-8 Hip-Flip Accessory 11
Figure 1-9 US AC/DC 12V Power Supply and Automotive Power Adapter 12
Figure 1-10 International AC/DC 12V Power Supply 12
Figure 1-11 Connect External Power Supply 12
Figure 1-12 Connect External Power Supply 13
Figure 1-13 Vehicle Power Supply, 24 – 72 Maximum VDC (Fuse Not Shown) 13
Figure 1-14 Connecting the Power Supply to the MX3P Endcap Power Jack 14
Figure 1-15 Vehicle Power Supply Footprint 14
Figure 1-16 Vehicle Connection Wiring Color Codes 15
Figure 1-17 Connect Audio Jack 16
Figure 1-18 Power Button 16
Figure 1-19 End-User Multi Applock Touch Panel 18
Figure 1-20 Touchscreen Recalibration 19
Figure 1-21 PCMCIA and CF Card Location 24
Figure 1-22 Scan Beam 27
Figure 1-23 Scanner LED Location 27
Figure 1-24 Audio Cable and Headset 28
Figure 1-25 ActiveSync Cable Connected to Serial port on Cradle 35
Figure 2-1 Hardware 43
Figure 2-2 Power Modes – On, Suspend, Critical Suspend and Off 46
Figure 2-3 Location of the Power (PWR) Button 50
Figure 2-4 Endcap and COM Ports 51
Figure 2-5 Serial Ports and Cables 51
Figure 2-6 Endcap Combinations 52
Figure 2-7 RS-232 Port 53
Figure 2-8 9-Pin RS-232 Pinout 53
Figure 2-9 Pinout – Serial Cable for Synchronization 54
Figure 2-10 Endcap Ports 55
Figure 2-11 USB Type A to Serial Port Cable Pinout 55
Figure 2-12 USB Type B to Serial Port Cable Pinout 56
Figure 2-13 Programmable Buttons 57
Figure 2-14 The QWERTY Keypad 58
Figure 2-15 LED Functions 61
Figure 2-16 Infrared Port – COM2 Port 64
Figure 2-17 Main Battery 65
Figure 2-18 MX3 Multi-Charger Plus 68
Figure 2-19 Insert Main Battery in Charge Pocket 68
Figure 2-20 US AC/DC 12V Power Supply and Cigarette Lighter Adapter 70
Figure 2-21 International AC/DC 12V Power Supply 70
Figure 3-1 Pocket CMD Prompt Screen 78
Figure 3-2 Taskbar Properties 80
Figure 3-3 Battery 85
Figure 3-4 Date/Time Properties 87
Figure 3-5 Dialing 88
Figure 3-6 Display Properties / Backlight Tab 89
Figure 3-7 Mixer 92
Figure 3-8 Owner Properties 94

Figure 3-9 Password Properties 95
Figure 3-10 Communication / PC Connection Tab 96
Figure 3-11 Power Schemes 99
Figure 3-12 Determine Your Scanner Software Version 101
Figure 3-13 Scanner Properties / Main Tab 103
Figure 3-14 Scanner Properties / Keys Tab 104
Figure 3-15 Scanner Properties / COM Port Settings 105
Figure 3-16 Stylus Properties / Recalibration Start 107
Figure 3-17 Stylus Properties / Recalibration 107
Figure 3-18 System / General tab 109
Figure 3-19 System / Memory 109
Figure 3-20 System / Device Name 110
Figure 3-21 Volume and Sounds 111
Figure 3-22 Avalanche Enabler Opening Screen 121
Figure 3-23 Connection Options 124
Figure 3-24 Execution Options (Dimmed) 125
Figure 3-25 Server Contact Options 126
Figure 3-26 Startup / Shutdown Options 127
Figure 3-27 Scan Config Option 128
Figure 3-28 Window Display Options 128
Figure 3-29 Application Shortcuts 129
Figure 3-30 Adapters Options – Network 130
Figure 3-31 Avalanche Network Profile Displayed 131
Figure 3-32 Manual Settings Properties Panels 131
Figure 3-33 Status Display 132
Figure 4-1 Determine Your Scanner Software Version 135
Figure 4-2 Scanner Control / Main Tab 138
Figure 4-3 Scanner Control / Keys Tab 139
Figure 4-4 Scanner Control / COM Port Tab 140
Figure 4-5 Scanner Control / Barcode tab 141
Figure 4-6 Barcode Tab – Symbology Settings 143
Figure 4-7 Strip Leading/Trailing Controls 145
Figure 4-8 Barcode Data Match List 146
Figure 4-9 Add Prefix/Suffix Controls 148
Figure 4-10 Barcode Tab – Ctrl Char Mapping 149
Figure 4-11 Barcode Tab – Custom Identifiers 151
Figure 4-12 Advanced – Main Tab 155
Figure 4-13 Advanced – Translate Control Codes 158
Figure 4-14 Advanced – Strip Leading/Trailing Characters 158
Figure 4-15 Advanced – Prefix/Suffix 159
Figure 4-16 Barcode Tab 160
Figure 4-17 Barcode – Prefix / Suffix 160
Figure 4-18 Barcode – Ctrl Translation 163
Figure 4-19 Barcode – Scancode Enable/Disable 164
Figure 4-20 Barcode – Advanced Processing 165
Figure 4-21 Barcode – Advanced Processing – Strip Code ID 166
Figure 4-22 Barcode – Advanced Processing – EAN128 Barcodes 166
Figure 5-1 Summit Client Utility 170
Figure 5-2 SCU – Main Tab 172
Figure 5-3 Admin Password Entry 173
Figure 5-4 SCU – Config Tab 174
Figure 5-5 SCU – Status Tab 177
Figure 5-6 SCU – Diags Tab 178
Figure 5-7 SCU – Global Settings Tab 179
Figure 5-8 Credential Sign-on Screen 182
Figure 5-9 Summit Profile with No Security 183
Figure 5-10 Summit WEP Keys 184

Figure 5-11 Summit Profile for LEAP w/o WPA 185
Figure 5-12 Summit LEAP Credentials 185
Figure 5-13 Summit Profile for EAP-FAST 186
Figure 5-14 Summit EAP-FAST Credentials 186
Figure 5-15 Summit Profile for PEAP/MSCHAP 187
Figure 5-16 Summit PEAP/MSCHAP Credentials 188
Figure 5-17 Summit Profile with LEAP for WPA TKIP 189
Figure 5-18 Summit WPA/LEAP Credentials 189
Figure 5-19 Summit Profile with WPA/PSK Encryption 190
Figure 5-20 Summit PSK Entry 190
Figure 5-21 Configure a Summit Profile with PEAP/GTC 191
Figure 5-22 PEAP/GTC Credentials 191
Figure 5-23 Cisco Aironet Client Utility 192
Figure 5-24 Cisco Profile Properties Screen 193
Figure 5-25 No Cisco PEAP 195
Figure 5-26 Cisco PEAP Installed 195
Figure 5-27 Cisco ACU Profile Selection 196
Figure 5-28 Cisco ACU Reboot Message 196
Figure 5-29 Microsoft Wireless Connection Icon 196
Figure 5-30 Wireless Information Screen 197
Figure 5-31 Advanced Wireless Settings 197
Figure 5-32 Wireless Network Properties 198
Figure 5-33 PEAP/MSCHAP Wireless Network Properties 199
Figure 5-34 Authentication Settings 199
Figure 5-35 Wireless Network Login 200
Figure 5-36 IP Information Tab 200
Figure 5-37 Authentication Settings, Validate Server 200
Figure 5-38 Advanced Wireless Settings, Authenticated SSID 201
Figure 5-39 PEAP/GTC Wireless Network Properties 202
Figure 5-40 PEAP Properties 202
Figure 5-41 Login Screen 203
Figure 5-42 IP Information Tab 203
Figure 5-43 Authentication Settings, Validate Server 204
Figure 5-44 Advanced Wireless Settings, Authenticated SSID 204
Figure 5-45 WPA/LEAP using ACU Profile Tab 205
Figure 5-46 Renaming Profile 205
Figure 5-47 Profile Properties Screen 206
Figure 5-48 Select Profile 206
Figure 5-49 Login Screen 207
Figure 5-50 ACU Status Tab 207
Figure 5-51 Certificate Stores 208
Figure 5-52 View Certificate Details 208
Figure 5-53 EAP/TLS Configuration 209
Figure 5-54 Authentication Settings 209
Figure 5-55 Select Certificate 210
Figure 5-56 Authentication Settings, Certificate Details 210
Figure 5-57 Validate Server 211
Figure 5-58 SSID Authenticated 211
Figure 5-59 WPA PSK Configuration 212
Figure 5-60 Symbol NETWLAN Screen 213
Figure 5-61 Symbol Wireless Information Tab 214
Figure 5-62 Symbol Wireless Network Properties 214
Figure 5-63 Symbol Advanced Wireless Settings 215
Figure 5-64 Logon to Certificate Authority 217
Figure 5-65 Certificate Services Welcome Screen 217
Figure 5-66 Download CA Certificate Screen 218
Figure 5-67 Download CA Certificate Screen 218

Figure 5-68 Certificates 219
Figure 5-69 Import Certificate 219
Figure 5-70 Browsing to Certificate Location 220
Figure 5-71 Certificate Import Confirmation 220
Figure 5-72 Logon to Certificate Authority 221
Figure 5-73 Certificate Services Welcome Screen 221
Figure 5-74 Request a Certificate Screen 222
Figure 5-75 Advanced Certificate Request Screen 222
Figure 5-76 Advanced Certificate Details 223
Figure 5-77 Script Warnings 224
Figure 5-78 Script Warnings 224
Figure 5-79 Certificate Issued 224
Figure 5-80 Download Security Warning 225
Figure 5-81 Certificates 226
Figure 5-82 Import Certificate 226
Figure 5-83 Browsing to Certificate Location 227
Figure 5-84 Certificate Listing 227
Figure 5-85 Private Key Not Present 227
Figure 5-86 Browsing to Private Key Location 228
Figure 5-87 Private Key Present 228
Figure 6-1 Administrator Control Panels – Multi-Application 230
Figure 6-2 Administrator Control Panels – Single Application 231
Figure 6-3 Application Panel – Multi-Application 234
Figure 6-4 Security Panel – Multi-Application 236
Figure 6-5 Status Panel – Multi-Application 237
Figure 6-6 End-User Multi-Application Touch Panel 239
Figure 6-7 Administrator Control Panel 241
Figure 6-8 Administrator Security Panel 242
Figure 6-9 Administrator Status Panel 244

Chapter 1 Introduction

Overview

The LXE® **MX3X** is a rugged, portable, hand-held Microsoft® Windows® CE .NET 4.2 or Windows CE 5.0 equipped mobile computer capable of wireless data communications. The mobile device can transmit information using a 2.4 GHz wireless device (with an internally mounted antenna) and it can store information for later transmission through an RS-232, InfraRed, or USB port. The device can be scaled from a limited function batch computer to an integrated wireless scanning computer.

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

The **MX3-RFID** version of the MX3X has an RFID module permanently attached to the back of the device. The module protects the RFID antenna and tag reader. A passive vehicle cradle is available that has been designed specifically for the MX3-RFID device deeper back cover.

The **MX3P** is another version of the MX3X with a deeper back cover. The deeper back cover allows it to use the MX3-RFID passive vehicle mount cradle. The MX3P does not have an integrated laser scanner nor does it have an RFID tag reader.

Device-specific cables are available for all versions. The stylus in the Stylus Kit (shipped with each unit) is used to assist in entering data and configuring the unit. Protective film for the touchscreen is available as an accessory.

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

Note: A mobile device functioning as a Summit client can run Microsoft Windows CE .NET 4.2 or CE 5.0. Microsoft Windows CE 5.0 is available on a Summit client mobile device only.

Features/Options for the MX3X Family

Feature	MX3X	MX3-RFID	MX3P	VX3X
Operating System - CE .NET 4.2	X	X	X	X
Operating System - CE 5.0	X	-	X	X
MX3X Main Battery	X	X	X	-
AC/DC Power Supply	X	X	X	X
Color and Touch Panel	X	X	X	X
SE 923 Laser Scanner	X	X	-	-
SE 955 Laser Scanner	X	X	-	X
RFID Module Enclosure	-	X	X	-
RFID Tag Reader	-	X	-	-
Power/Communication Cradles	X	-	-	X
Passive Vehicle Cradle	-	X	X	X
Summit Client Utility	X	-	X	X
Cisco Client Utility	X	X	-	-
Symbol Client	X	-	-	-
RFTerm®	X	X	X	X
Voice Compatible	X	-	-	X
Wavelink Avalanche Enabler	X	-	X	X
ActiveSync specific cables	X	X	X	X
Hip-Flip Accessory	X	-	-	-
IP 66 Compliant	X	-	-	-
IP 65 Compliant	-	X	X	-

Related Manuals

MX3X The "MX3X User's Guide" contains MX3X and MX3P user information and instruction. An abbreviated user's guide (LXEbook – MX3X User's Guide) is available for download to the MX3X device from the LXE Manuals CD or the LXE ServicePass website.

MX3-RFID The "MX3-RFID User's Guide" and "MX3-RFID Reference Guide" contain user and technical information and instruction for the MX3-RFID mobile device.

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

Charger Please refer to the "MX3 Multi-Charger Plus User's Guide" for instruction and technical information relating to charging/analyzing MX3X batteries in a multi-charging station.

Scanner To set up the integrated SE923 or SE955 scanner barcode parameters with barcodes, please refer to the "Integrated Scanner Programming Guide" on the LXE Manuals CD or the LXE website. The SE923 scanner was replaced with the SE955 scanner in July 2006.

Note: The MX3P does not contain an integrated laser scanner nor an RFID tag reader.

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

Components

Front and Back Views

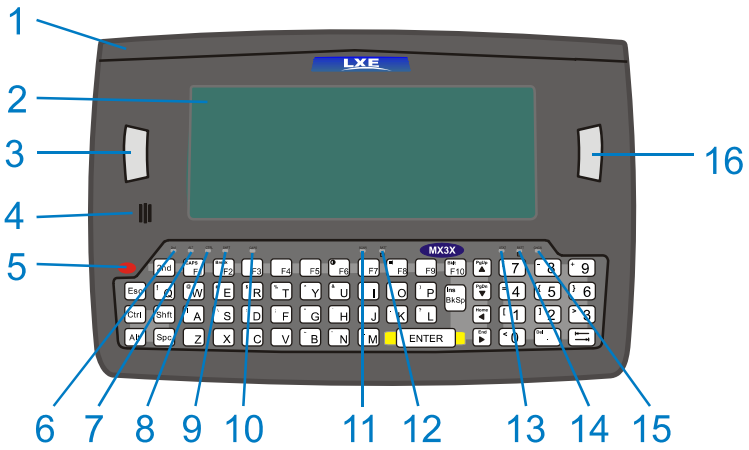


Figure 1-1 Front

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

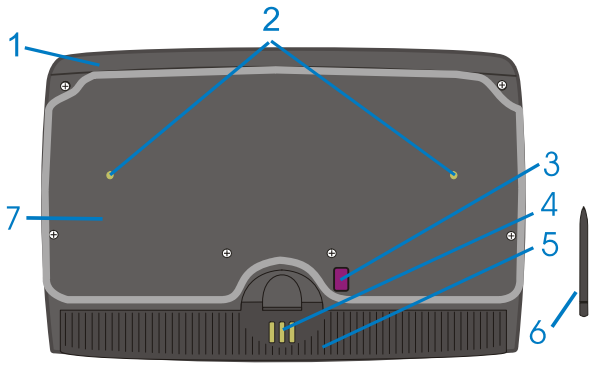


Figure 1-2 Back

1	Endcap	5	Main Battery
2	Leather Handstrap Connector	6	Stylus
3	IR Port (Com 2 Port)	7	Back Cover (MX3P only)
4	Cradle Input Contacts		

Endcap Options

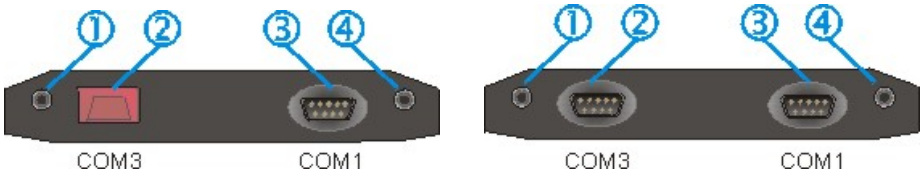


Figure 1-3 Endcaps

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

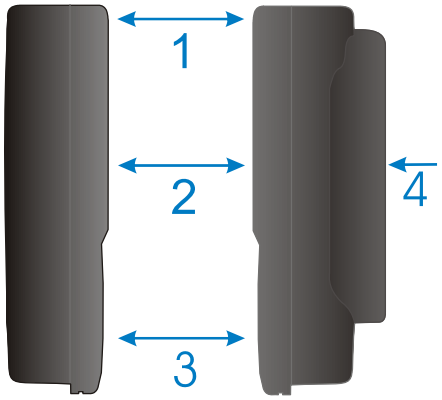
MX3X / MX3P*	
Left Port	**Right Port**
Serial COM3	Serial COM1
Serial COM3	USB Client
USB Host	Serial COM1
USB Host	USB Client
Scanner*	Serial COM1
Scanner*	USB Client

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

* The MX3P does not have an integrated scanner nor an RFID tag reader.

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

MX3-RFID Module



1 Endcap w/Laser Scanner

2 Touchscreen

3 Keypad

4 RFID Module or MX3P Back Cover

Figure 1-4 Side View

Battery Well Vent Aperture

Caution

The vent aperture in the battery well should never be blocked with any device *other than an approved LXE main battery*. The vent aperture functions to relieve any heat or pressure that may build up in the mobile device during everyday use.

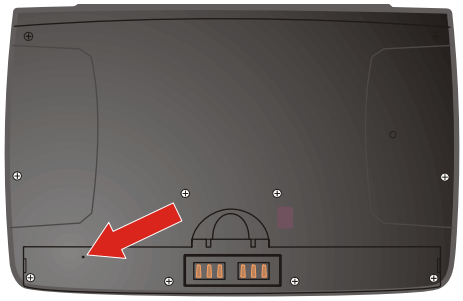


Figure 1-5 Vent Aperture in Battery Well – Do Not Cover

If the vent hole is covered by an object, e.g. a tracking label, other than an approved LXE main battery, the touch screen may be damaged. If damage occurs to the touch screen, please contact your LXE representative for the process to follow when returning the device to LXE for repair.

When to Use This Guide

As the reference for LXE's MX3X / MX3-RFID computer, this guide provides detailed information on its features and functionality. Use this reference guide as you would any other source book – reading portions to learn about the device and it's capabillities, and then referring to it when you need more information about a particular subject. This guide takes you through all aspects of installation and configuration.

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

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

Chapter 2 "Physical Description and Layout", describes the function and layout of the configuration, controls and connectors. Power sources and battery charging stations are included in this chapter.

Chapter 3 "System Configuration" takes you through the system setup and file structure.

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

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

Chapter 6 "AppLock" is a self-contained chapter covering all aspects of the LXE AppLock program. A mobile device running AppLock becomes a dedicated, single or multiple application device.

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

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

Document Conventions

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

Getting Started

Important

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

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

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

Use this guide as you would any other source book – reading portions to learn about the device, and then referring to it when you need more information about a particular subject. This guide takes you through an introduction to and operation of the MX3X.

In general, the sequence of events is:

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

Troubleshooting

Can't align the screen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts access to the control panels. Contact your System Administrator. See *Chapter 6 AppLock*.
Touchscreen is not accepting stylus taps or need recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and cursor keys to move the cursor from element to element.

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

Insert Main Battery

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

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

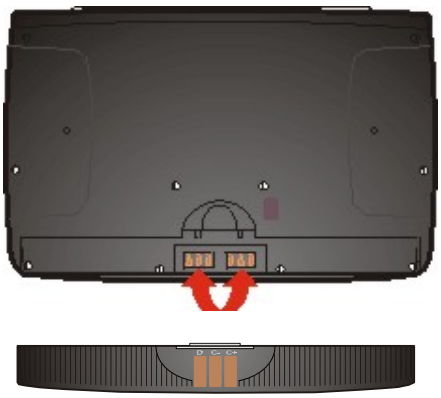


Figure 1-6 Battery Contacts and Main Battery

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

Place the battery in the compartment, making sure the side of the battery with six contacts matches up with the battery contacts in the battery well. Do not slide the battery sideways into the battery well. Firmly press the battery into the well until the Retaining Clip on the battery clicks. The battery is now securely fastened to the computer. The computer draws power from the battery immediately upon successful connection.

Note: *Do not cover the vent aperture in the battery well (located in the left side of the battery well) with anything other than the main battery.*

Check Battery Status

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

About Lithium-Ion Batteries

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

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

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

Optional Devices

Attach Handstrap (Optional)

Note: These instructions are not to be used for the MX3P. See "Accessories" for MX3P holding accessories e.g. holster mounted, shoulder straps, etc.

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

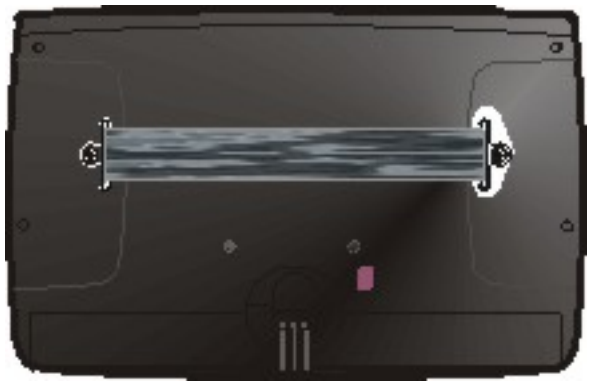


Figure 1-7 MX3X With Handstrap Installed

Tool Required: #1 Phillips Screwdriver

Installation

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

Attach the Stylus Clip (Optional)

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

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

Attach to Hip-Flip (Optional)

Note: The MX3P does not fit the Hip-Flip accessory. The Hip-Flip is not to be used with the MX3P device. See "Accessories" for MX3P holding accessories e.g. holster mounted, shoulder straps, etc.

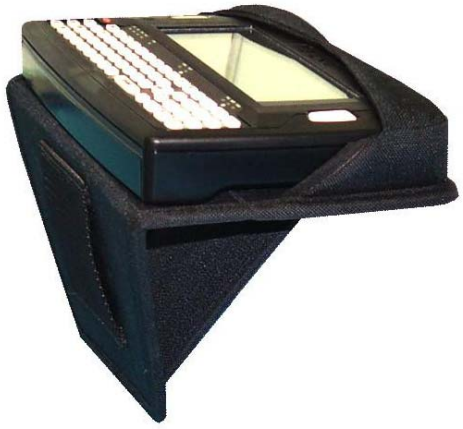


Figure 1-8 Hip-Flip Accessory

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

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

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

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

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

Installation

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

Connect External Power Supply to MX3X or Cradle (Optional)

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

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

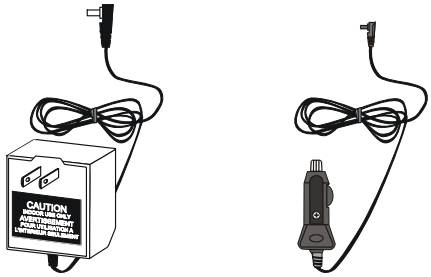


Figure 1-9 US AC/DC 12V Power Supply and Automotive Power Adapter

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

The DC power jack is located on the endcap. The standard MX3 cradle power jack is located on the back of the cradle (the passive vehicle cradle does not have a power jack).

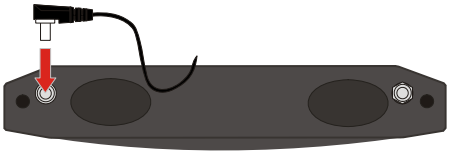


Figure 1-11 Connect External Power Supply

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

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

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

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

Connect External Power Supply to the MX3P

The DC power jack is located on the endcap. The passive cradle does not have a power jack.

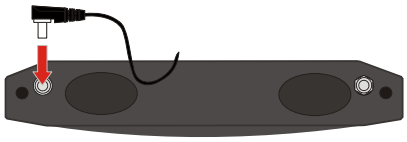


Figure 1-12 Connect External Power Supply

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

2. The CHGR LED above the keypad illuminates when the MX3P is receiving external power through the power jack.

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

MX3P Specific Power Accessories

Part Number	Description
9000A060CBL12V	POWER CABLE, BARE WIRE, 12 FT, 12V, DC JACK
9000A316PS24V72VMX3P	PS, 24V-72V, BARE WIRE INPUT, MX3P OUTPUT

24/72 Maximum VDC MX3P Power Supply Input/Output Cable Connection

Caution

For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. This fused circuit requires a 5 Amp maximum time delay (slow blow) fuse. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery positive (+) terminal.

Recommended for vehicle electrical systems that use between 2 and 5 twelve volt batteries in series.

LXE Part Number: 9000A316PS24V72VMX3P

1. Power Switch
2. Power On Indicator
3. Output to MX3P
4. Input from Vehicle Battery

Figure 1-13 Vehicle Power Supply, 24 – 72 Maximum VDC (Fuse Not Shown)

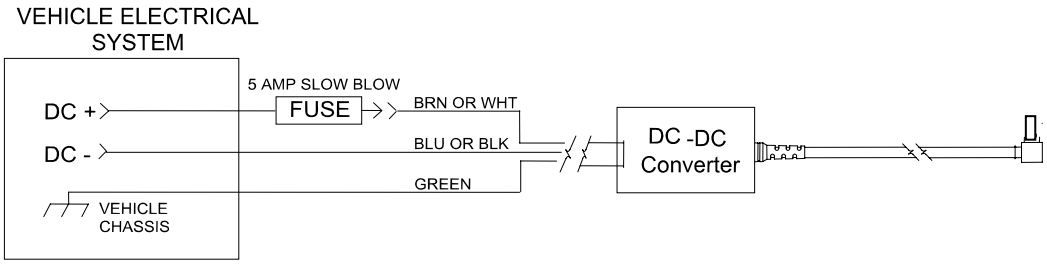


Figure 1-14 Connecting the Power Supply to the MX3P Endcap Power Jack

Power Supply Dimensions

Length 9.25”

Height 2.5”

Width 4.7”

Mounting hole center Width: 3.5”

Mounting hole center Length: 8.75”

DIAGRAM IS NOT TO SCALE

Figure 1-15 Vehicle Power Supply Footprint

1. If the mobile device is in the cradle, it can be either On or in Suspend Mode during this process.
2. Turn the Power Supply toggle switch to the Off position.
3. While observing the fuse requirements specified above, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

   IMPORTANT:

   For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.

4. Route the cable the shortest way possible. The input cable from the connection to the battery is rated for a maximum temperature of 60°C (140°F). When routing this cable it should be protected from physical damage and from surfaces which might exceed this temperature.

   Additionally do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate.

   Note: If the vehicle is equipped with a panel containing Silicon Controlled Rectifiers (SCR's), avoid routing the power cable in close proximity to these devices.

   Always route the cable so that it does not interfere with the operator's safe operation and maintenance of the vehicle.

Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination.

Wiring color codes for LXE supplied DC input power cabling:

Vehicle Supply		Wire Color
+24-72 Max VDC	(DC +)	Brown or White
Return	(DC -)	Blue or Black
Vehicle Chassis	(GND)	Green

Figure 1-16 Vehicle Connection Wiring Color Codes

Note: The input power cord for the DC-DC Power Supply uses white, black and green wires. Some LXE products have DC input power cords with brown, blue and green wires. The previous table shows the correct electrical connection for either type of cable.

5. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.
6. Connect the Power Supply to the MX3P by plugging the computer end into the Power Jack on the endcap.
7. Turn the Power Supply on. The ON LED on the Power Supply illuminates when it is receiving power from the vehicle.
8. The mobile device CHGR LED illuminates.

12V VDC MX3P Power Cable Connection

9000A060CBL12V	POWER CABLE, BARE WIRE, 12 FT, 12V, DC JACK

If the mobile device is in the cradle, it can be either On or in Suspend Mode during this process.

Connect the two-wire end of the power cable to the 12V power source battery terminals.

Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.

Connect the 12V power source to the MX3P by plugging the computer end into the Power Jack on the endcap.

The mobile device CHGR LED illuminates.

Connect MX3X Audio Jack (Optional)

The audio jack is located on the endcap.

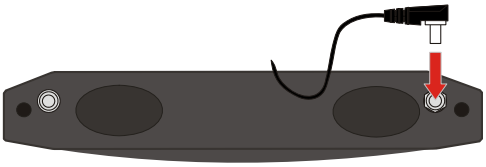


Figure 1-17 Connect Audio Jack

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

Note: The audio option draws power from the battery.

Power Button

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

Figure 1-18 Power Button

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

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

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

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

Restart Sequence

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

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

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

Tapping the Touchscreen with a Stylus

Note: Always use the point of the stylus for tapping or making strokes on the touchscreen. Never use an actual pen, pencil, 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 when the stylus is not in use.

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

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

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

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

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

Entering the Multi AppLock Activation Key

The appearance of taskbar icons are different on various mobile device platforms and may differ from the example shown below. This example is shown only to aid in describing how the user can switch between applications using a stylus. If RFTerm® and Microsoft® Word® were the two applications locked, and the user tapped the taskbar icon to place the popup menu on screen, a switching menu showing both application icons is displayed on the screen.

Figure 1-19 End-User Multi Applock Touch Panel

Touch

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

Alternatively you can use the Tab, BackTab and/or cursor keys to move the on-screen cursor. Then press the Enter key to activate the highlighted choice.

Hotkey

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

Touchscreen Calibration

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

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

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

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

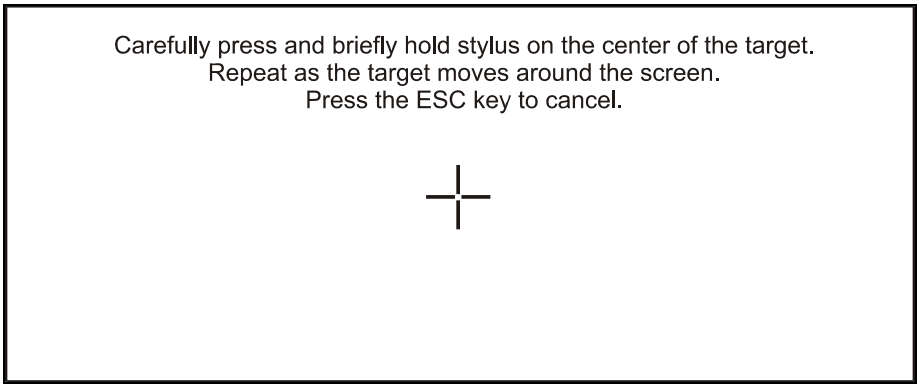


Figure 1-20 Touchscreen Recalibration

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

Set The Display Contrast

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

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

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

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

Set the Display Backlight Timer

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

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

The first option affects the mobile device when it is running on battery power only. The second option affects the device when it is running on external power (e.g. AC adapter, cigarette adapter, powered cradle).

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

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

Set The Display Brightness

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

Color – To adjust color screen brightness, locate the <F10> key at the top of the keypad. Adjust the display brightness by pressing the:

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

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

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

Set the Power Schemes Timers

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

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

Battery Power Scheme

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

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

AC Power Scheme

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

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

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

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

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

Set The Audio Speaker Volume

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

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

Using the Keypad

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

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

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

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

Using the Touchscreen

Select **Start | Settings | Control Panel | Volume & Sounds | Volume** tab. Change the volume setting and tap OK to save the change. You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

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

Setup the 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 the Terminal Emulation Parameters

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

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

to properly set up your host session.

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

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

Installing PCMCIA and CF Cards

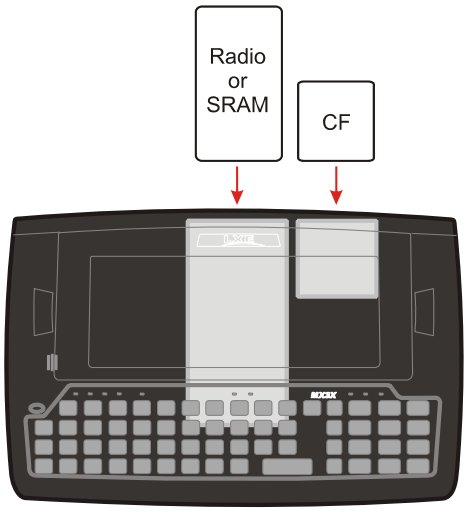


Figure 1-21 PCMCIA and CF Card Location

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

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

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

Installing / Removing Cards

Preparation

Requirement: A screwdriver (not supplied by LXE)

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

Installation

1. Slide the card, connector side first, into the slot until it seats. Use caution not to pull or snag the antenna connector.
2. If the card is difficult to seat in the slot, remove the card, turn it around and re-install.
   - The antenna connector must be positioned up and toward the front of the device (near the display).
   - Gently snap the antenna cables into the connectors on the wireless client card. Use caution not to damage either the antenna cable connectors or the connectors on the wireless client card. Connect **all** antenna cables to the PCMCIA wireless client card.
3. Replace the endcap, making sure all connections are secure and ribbons/antennas are not crimped between the endcap and the body of the mobile device.

Removal

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

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

Enter Data

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

Keypad Entry

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

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

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

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

Stylus Entry

The stylus performs the same function as a mouse that is used to point to and click elements on a desktop computer. The stylus is used in the same manner as a mouse – single tap or double tap to select menu options, drag the stylus across text to select, hold the stylus down to activate slider bars, etcetera. Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp or abrasive object to write on the touchscreen.

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

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

- Touch the stylus to the field of the data entry form to receive the next data feed.
- The cursor begins to flash in the field.
- The unit is ready to accept data from either the keyboard, integrated scanner or a scanner connected to the serial port, if the scanner applet is configured correctly.

Input Panel

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

Integrated Laser Scanner Data Entry

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

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

Figure 1-22 Scan Beam

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

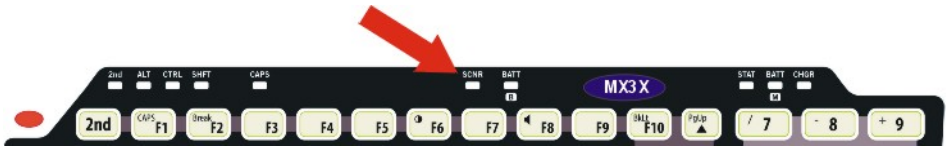


Figure 1-23 Scanner LED Location

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

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

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

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

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

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

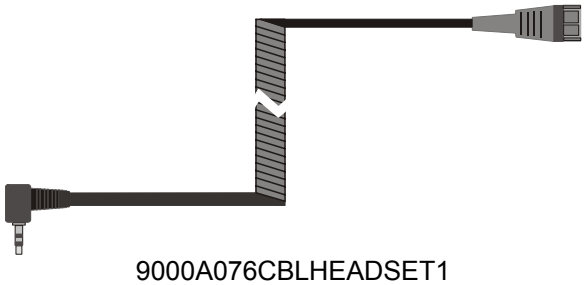
See the “Integrated Scanner Programming Guide” for barcode samples, default scanning ranges, barcode reading instruction and troubleshooting.

Using a Headset and Voice for Data Entry

Connecting the Audio Cable and a Headset

Note: The audio option draws power from the main battery. The Headset and Voice option is not available for an MX3-RFID configuration. The speaker is disabled when a headset is plugged into the audio jack

The headset consists of an earpiece, a microphone and an attached cable. The headset attaches to an audio cable which attaches to the MX3X. The audio jack is located on the MX3X endcap.



9000A076CBLHEADSET1

Figure 1-24 Audio Cable and Headset

Insert the 2.5mm barrel end of the connector into the audio jack on the endcap and push the connector in firmly.

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

Adjust Microphone and Secure the Cable

Do not twist the microphone boom when adjusting the microphone.

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

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

The microphone cable can be routed over or under clothing.

Under Clothing

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

Over Clothing

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

Entering Data

Data is entered into the mobile device by speaking into the headset's microphone when prompted.

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

Tethered Scanner

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

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

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

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

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

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

MX3P and the MX3 Cradles

The MX3P does not fit in the standard MX3 powered cradles. There is a passive vehicle cradle available for the MX3P that secures the device to the cradle only. See section titled "Accessories".

Main battery charging and host communication is not available directly through the passive vehicle cradle. The passive vehicle cradle does not have LEDs or indicators. It does not accept DC power connection. The MX3P can be directly connected to external power through the power jack located on the mobile device's endcap. Host communication is available wirelessly while the mobile device is secured in the passive vehicle cradle.

ActiveSync

Introduction

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 mobile device.

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

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

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

For example, you can:

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

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

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

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

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

Initial Setup

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

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

Serial Connection

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

Serial 1 @ 57600

Note: The default is 57600 baud.

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

Tap OK to return to the Control Panel.

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

USB Connection

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

USB "Client"

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

Tap OK to return to the Control Panel.

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

The MX3P requires USB connection for ActiveSync. There is no ActiveSync connection through the passive cradle. Cable connection occurs only on the endcap.

Network

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

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

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

IrDA Connection

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

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

IR @ 115200

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

Tap OK to return to the Control Panel.

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

Synchronizing from the Mobile Device

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

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

Tap Sync to connect and synchronize. View synchronization status.

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

Tap Stop to stop synchronization.

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

Connect and Communicate

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

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

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

** Cables for initial ActiveSync Configuration:

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

Explore

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

Copy the MX3X LXEbook to the MX3X (Optional)

Note: The LXEbook user guides do not contain the illustrations and regulatory information contained in the full user guides on the LXE Manuals CD and on the LXE ServicePass website. See the full format User Guide"MX3X User's Guide" on LXE Manuals CD.

Mobile Device	Required Adobe Acrobat Reader Version
MX3X	Windows PDF Viewer (pre-installed by LXE).

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

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

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

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

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

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

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

Backup Data Files using ActiveSync

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

Prerequisites

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

Serial Port Transfer

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

Infrared Port Transfer

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

USB Transfer

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

Connect

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

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

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

Disconnect

Serial Connection

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

IRDA Connection

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

USB Connection

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

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

Network Connection

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

Cold Boot and Loss of Host Re-connection

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

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

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy *that* partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

ActiveSync with a Cradle

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

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

Figure 1-25 ActiveSync Cable Connected to Serial port on Cradle

Troubleshooting ActiveSync

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

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

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

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

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

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

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

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

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

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

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

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

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

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

Docking Cradles

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

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

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

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

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

A passive vehicle cradle is available for the MX3-RFID and MX3P devices. Power and communication is cabled through the endcaps, only, for these devices.

Status LED

An LED indicator on the front of the standard MX3 cradle shows the status of the cradle. When the indicator is not illuminated, there is no power applied to the cradle.

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

Desktop Cradle

*Note: LXE recommends the correct Desktop Cradle always be used to store / charge / communicate with the MX3X. The MX3X Desktop Cradle label is located on the bottom of the device. The MX3X Desktop cradle Product Number is **MX3RA002DESKCRADLE**.*

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

Note: Do not "slam" or slide the mobile device sideways into the cradle. Damage may result. The MX3-RFID and MX3P devices do not fit in the MX3 desktop cradle.

Connectors

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

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

Vehicle Mount Cradle

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

Connectors

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

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

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

ActiveSync with a Cradle

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

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

Note: The MX3-RFID and the MX3P use a passive, non-powered cradle (refer to "The Passive Vehicle Cradle"). ActiveSync connects only through the endcap on these devices.

Tethered Scanner and a Cradle

To use a tethered scanner connected to the RS-232 port on the cradle, the cradle must be powered off, the ActiveSync cable removed and the cradle powered up. Then, the scanner can be attached to the cradle's serial port.

The Passive Vehicle Cradle

The MX3P cannot fit in standard MX3 charging cradles. There is a passive vehicle cradle available (as well as a RAM bracket installation kit) for the MX3P that secures the mobile device to the cradle. See "Accessories".

Mobile device main battery charging and RF communication is not available in the passive vehicle cradle unless the mobile device is receiving external power through the power jack in the endcap.

The passive vehicle cradle does not have LEDs or indicators. The passive vehicle cradle does not require an external power source.

The mobile device in the passive cradle requires a power source, either from the main battery or from power applied via the power jack on the endcap.

Getting Help

All LXE user guides are now available on one CD and they can also be viewed/downloaded from the LXE ServicePass website. Contact your LXE representative to obtain the LXE Manuals CD. You can also check the LXE ServicePass website for the latest manual releases.

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

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

Manuals

MX3X User's Guide
LXEbook – MX3X User's Guide (download to MX3X)
MX3 Cradle Reference Guide
MX3 Multi-Charger Plus User's Guide
CE API Programming Guide
RFTerm Reference Guide
Integrated Scanner Reference Guide

Accessories

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.

R	1	Cable, USB Host D9F to USB, 6' (Endcap only) MX3XA069CBL09USBCLNT	
R	2	Cable, D9F to D9F for ActiveSync only, 6' (Cradle use only) MX3XA070CBLD9RS232AS / Cradle MX3RA002DESKCRADLE	
R	3	Cable, USB Client D9F to USB, 6' (Endcap only) MX3XA071CBLD9USBTYPB	
R		Cable, 12 in., D9F / USB Type A Receptacle MX3XA068CBLD9USBHOST	

	Tethered Scanners	
R	Scanner, Powerscan SR, 8’ Cbl, WW	8300A326SCNRPWRSR8DA9F
	Scanner, Powerscan SR, 12’ Cbl, US	8300A327SCNRPWRSR12DA9F
R	Scanner, Powerscan LR, 8’ Cbl, WW	8310A326SCNRPWRLR8DA9F
R	Scanner, Powerscan LR, 12’ Cbl, US	8310A327SCNRPWRLR12DA9F
R	Scanner, Powerscan XLR, 8’ Cbl, WW	8320A326SCNRPWRXLR8DA9F
	Scanner, Powerscan XLR, 12’ Cbl, US	8320A327SCNRPWRXLR12DA9F
R	Scanner, LS3408ER, 9’ Cbl, US See Note	8520A326SCNRERDA9F
R	Scanner, LS3408FZ, Fuzzy Logic, 9’ Cbl, US See Note	8510A326SCNRFZYDA9F
	Holding Accessories	
R	Strap, Hand, Nylon	MX3RA497HANDSTRAP
R	MX3X Nylon Holster for use with Belt	MX3RA401HOLSTER
R	MX3X Nylon Hip Flip	9000A408HIPFLIP
R	Adjustable Belt for Hip Flip – Velcro ends	9200L67
R	Belt Strap with plastic scanner clip	9200L57
	MX3-RFID Nylon Case with Shoulder Strap [1]	MX3XA411RFIDCASE
R	MX3X Nylon Case with Shoulder Strap	9000A409CASE
R	Scanner Clip Strap (85XX scanners only)	9000A411SCNRSTRAP
	Bracket, Mounting LS300 Scanner, Tethered	8010A001BRKT
	Holster, Hood, Nylon, 5300IP Series Scanner, Tethered	8100A401HLSTRHOOD
*	*** **Voice Recognition and Headsets** ***	
R	MX3X Voice Case optional shoulder strap	9000A410SHOULDERSTRP
R	MX3X Nylon Case, Voice Recognition w/Belt	MX3XA410VOICECASE
R	MX3X to Headset adapter cable, 2.5mm	9000A076CBLHEADSET1
R	Single ear and headband, headset with microphone, 5 windscreens	HX1A501SNGBHEADSET
R	Single ear, dual headband, headset with microphone, 5 windscreens	HX1A502DUALBHEADSET
R	Dual ear, behind head, headset with microphone, 5 windscreens	HX1A503BTHHEADSET
R	Replacement foam block for dual headband	HX1A504AHSBLOCKFOAM
R	Replacement head yoke for dual headband	HX1A505DUALYOKE
R	Replacement head yoke for single headband	HX1A506SINGLEYOKE
R	Replacement windscreen for all microphones, 10 pack	HX1A508WINDSCREEN10
R	Replacement windscreen for all microphones, 50 pack	HX1A509WINDSCREEN50
R	Replacement foam ear piece cover for single/dual headsets, 10 pack	HX1A510FOAMEAR10
R	Replacement foam ear piece cover for single/dual headsets, 50 pack	HX1A511FOAMEAR50
*	*** Contact your LXE representative for availability. ***	
	Miscellaneous	
R	Stylus Kit includes stick-on clip, stylus and tether, 5 pack	9000A507STYLUS
R	MX3X SDK, CD (Windows CE .NET 4.2 only)	MX3XA504CENET42SDK
R	Windows CE 5.0 Pro SDK with English Font	Call LXE
R	Cover Plate, RS-232 Port, MX3/MX3-CE	MX3RA351RS232CVR
R	Touchscreen Protective Film, Monochrome Display	MX3XA502PROTFILMMONO
R	Touchscreen Protective Film, Color Display	MX3XA503PROTFILMCOLR
	Battery Chargers and Battery	
R	Battery Charger/Analyzer, US V1.01	9000A377CHGR5US
R	Battery Charger/Analyzer, WW	9000A377CHGR5WW
	Battery, Replacement, RFID Device	MX3A380RFIDBATT

[1] Accessories designed specifically for the MX3-RFID device are compatible with the MX3P device.

R	Battery, Li-Ion	MX3A378BATT
	Cradles and Power Supplies	
	MX3-RFID \ MX3P Passive Mounting Cradle	MX3XA001RFIDCRADLE
	MX3-RFID \ MX3P RAM Mounting Kit for Passive Cradle	9000A019RAMKIT
R	MX3X Desktop Cradle [2]	MX3RA002DESKCRADLE
R	MX3X Vehicle Mount Cradle [2]	MX3RA003VMCRADLE
R	MX3X Vehicle Mount Cradle, 19.2K baud rate	9000A005VMCRADLE19KB
	Power Supply, Vehicle Cradle, 9-30VDC	2381A054CRDLDCPWR30V
	Power Supply, Vehicle Cradle, 30-80VDC	2381A055CRDLDCPWR80V
R	AC Power Supply, External, US	9000A301PSACUS
R	AC Power Supply, External, AC, International	9000A302PSACWW
R	Power Cord, AC, US	9000A066CBLPWRAC
	P/S, External, Cigarette Lighter Adapter	9000A303PSCIGLTADPT
R	Power Adapter, Bare Wire 12 VDC	9000A079CBL12ML3
R	Power Adapter, 24-72 VDC, Bare Wire (Vehicle)	9000A316PS24V72VMX13
	Power Adapter, 110-240 VAC	1300A303PSACWW
	MX3P Power Cable, Bare Wire, 12 Ft, 12V, DC Jack	9000A060CBL12V
	MX3P Power Supply, Bare Wire input, MX3P output	9000A316PS24V72VMX3P
	Cables for Cradle and Endcap Serial Ports	
R	Cable, Null Modem, PC, D9F to D9F, 6’	9000A054CBL6D9D9
	Cable, Null Modem, Printer/PC, D9F to D25F, 6’	9000A053CBL6D9D25
R	Cable, USB D9F to USB Type A Receptacle	MX3XA068CBLD9USBHOST
R	Cable, USB D9F to USB Type A Plug	MX3XA069CBLD9USBCLNT
R	Cable, USB D9F to USB Type B Plug	MX3XA071CBLD9USBTYPEB
R	Cable, D9F to D9F for ActiveSync only, 6’ See Note	MX3XA070CBLD9RS232AS

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

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

Note: There may be different SDK kits for Windows CE .NET 4.2 and CE 5.0. Contact your LXE representative to order an LXE SDK CD.

[2] Power Adapter Required.

Chapter 2 Physical Description and Layout

Hardware Configuration

The MX3X and MX3P hardware configuration is shown in the following figure.

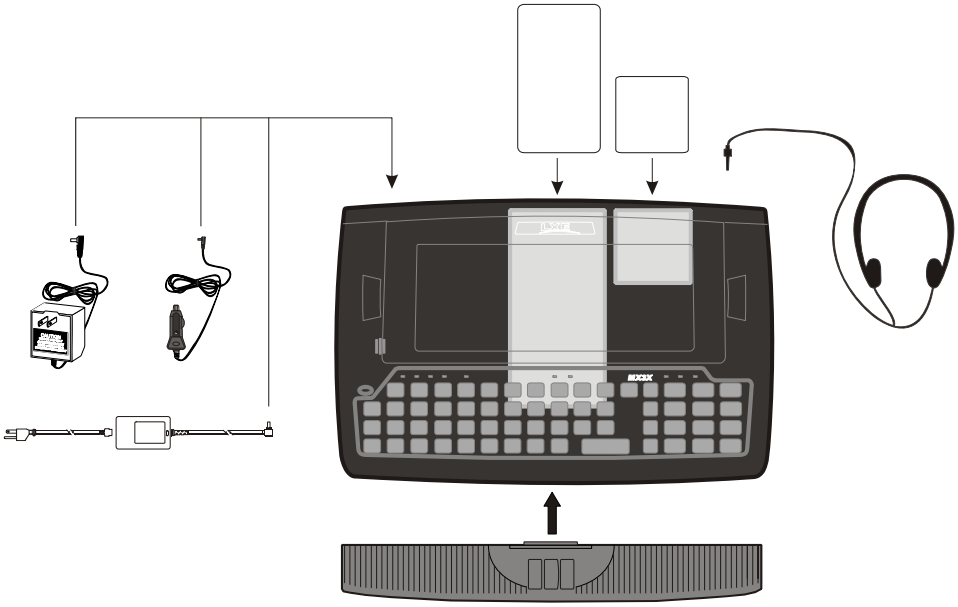


Figure 2-1 Hardware

Central Processing Unit

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

System Memory

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

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

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

Core Logic

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

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

Video Subsystem

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

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

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

See Section “Display” .

Power Supply

The mobile device uses two batteries for operation.

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

See “Power Supply”.

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

Audio Interface

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

PCMCIA Slots

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

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

Slot 0 – Network or SRAM Cards

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

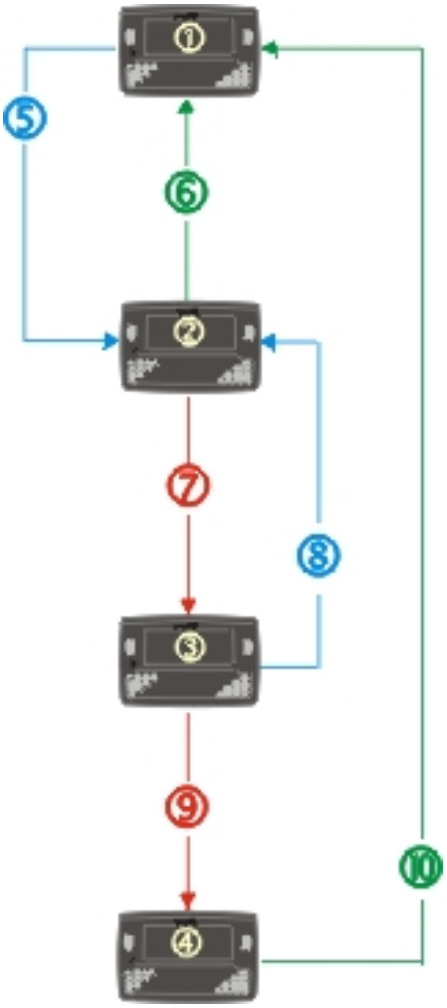
The mobile device has one internal PCMCIA slot that conforms electrically to PCMCIA 2.1 specifications. The PC Slot supplies 0.75 of an amp at 5Volts or 3.3Volts. Battery voltage is supplied through unused pin 35 to support a WAN client device in the slot.

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

Slot 1 – Compact Flash Card

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

Power Modes



1 – On

2 – Suspend

3 – Critical Suspend

4 – Off

5 – Power Button or Power Off Timer expires

6 – Primary Event

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

8 – Restoration of power.

9 – Backup battery and main battery dead

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

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

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

Primary Events Listing

Any key on the keypad	COM1 activity
Stylus touch on the touchscreen	COM2 activity (prior to July 2006 only)
Power button tap	COM3 activity
PC card activity	USB client connection
External power connection	Scanner activity

On Mode

The Display

When the display is On:

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

The Mobile Device

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

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

User Idle Mode

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

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

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

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

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

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

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

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

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

System Idle Mode

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

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

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

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

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

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

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

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

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

Suspend Mode

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

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

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

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

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

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

Critical Suspend Mode

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

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

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

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

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

Off Mode

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

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

Physical Controls

Power Button

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

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

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

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

Restart Sequence

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

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

Note: To reset to factory default values, please refer to Chapter 3 "System Configuration" section titled "Utilities".

Endcaps and COM Ports

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

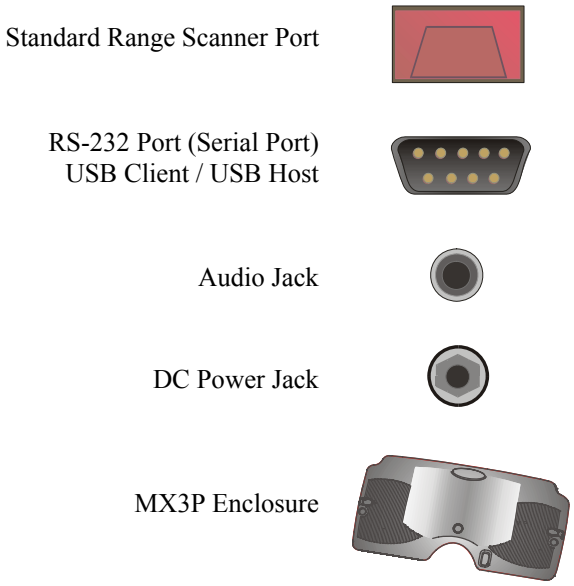


Figure 2-4 Endcap and COM Ports

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

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

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

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

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

Figure 2-5 Serial Ports and Cables

Endcap Combinations

Left Port	Right Port
Serial COM3	Serial COM1
Serial COM3	USB Client
USB Host	Serial COM1
USB Host	USB Client
Scanner*	Serial COM1
Scanner*	USB Client
Rear **IR Port** is COM2 Barcode scanners, tethered to the serial port on a cradle, send ASCII data to the MX3X in the cradle through the COM2 Port.	

Figure 2-6 Endcap Combinations

* The MX3P does not have an integrated scanner nor an RFID tag reader and antenna.

COM Port Switching

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

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

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

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

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

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

Note: If there is an integrated laser scanner, COM3 is greyed out – if there is no integrated laser scanner, Internal is greyed out.

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

See Also: Section titled “Tethered Scanners”.

Integrated Scanner Port

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

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

The mobile device has an SE923 or SE955 scanner engine.

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

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

Serial Port

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

Figure 2-7 RS-232 Port

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

Figure 2-8 9-Pin RS-232 Pinout

LXE Connection Cable Technical Specification

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

Serial cable:

9000A054CBL6D9D9

Pinout:

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

Figure 2-9 Pinout – Serial Cable for Synchronization

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

RTS/CTS Handshaking and the Serial Port

RTS	Ready to Send	CTS	Clear to Send
DTR	Data Terminal Ready	DSR	Data Set Ready
Remote Side	The device sending data to and receiving data from the MX3X through the LXE serial cable connected to the RS-232 ports on both devices.		
LXE Serial Cable	9000A054CBLD9D9		

The MX3X serial port supports four types of handshaking via the LXE serial cable: None, standard Xon/Xoff, standard DTR/DSR, and a form of RTS/CTS.

To use RTS/CTS, the remote side computer must clear the DTR line which sets the MX3X CTS line and allows the MX3X to send data to the remote side.

And then signals and data travel smoothly between both devices.

USB Host / Client Port

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

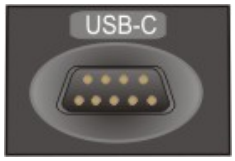
The optional LXE USB cable is required to adapt the connection to a standard USB connector. Please refer to section titled "Accessories" for the USB part number when ordering.

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

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

Figure 2-10 Endcap Ports

USB Host Cable



Port Label on Endcap

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

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

ActiveSync

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

USB Client Cable

Port Label on Endcap

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

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

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

Tethered Scanners

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

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

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

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

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

Programmable Scan Buttons

Figure 2-13 Programmable Buttons

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

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

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

The default setting for the right button for the MX3X and the MX3P is Enter. The default setting for the left button is Scan. When the device does *not* have an integrated scanner, both buttons default to Enter keys and the Scan selection is greyed out.

Each button can be setup as:

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

Field Exit Key Function (IBM 5250/TN5250 Only)

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

Scan Buttons and the SCNR LED

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

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

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

The Keypad

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

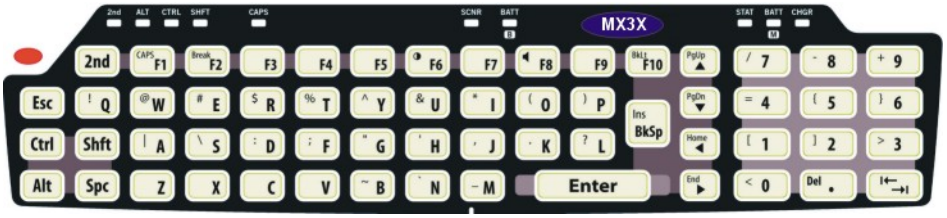


Figure 2-14 The QWERTY Keypad

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

Key Functions

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

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

Caps Key and CapsLock Mode

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

The CapsLock key sequence is 2nd + F1.

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

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

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

Keypress Sequences

See Appendix A for all key press sequences.

Custom Key Maps

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

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

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

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

LED Functions

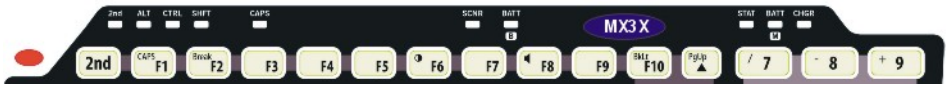


Figure 2-15 LED Functions

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

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

Display

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

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

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

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

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

Display and Display Backlight Timer

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

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

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

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

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

Touchscreen

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

Touchscreen operation is not affected by Display Backlighting.

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

Cleaning the Glass Display/Scanner Aperture

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

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

Applying the Protective Film to the Display

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

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

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

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

Speaker

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

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

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

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

Operational "beeps" are emitted from the speaker.

Infrared (IR) Port

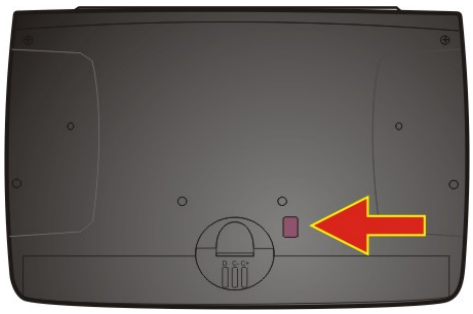


Figure 2-16 Infrared Port – COM2 Port

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

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

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

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

Power Supply

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

Note: LXE recommends the correct Desktop Cradle always be used to store / charge / communicate with the MX3X. The MX3X Desktop Cradle label is located on the bottom of the device. The MX3X Desktop cradle Product Number is ***MX3RA002DESKCRADLE****.*

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

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

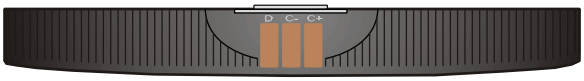


Figure 2-17 Main Battery

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

Check Battery Status

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

Handling Batteries Safely

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

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

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

Li-Ion Battery

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

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

Main Battery

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

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

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

Battery Hot-Swapping

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

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

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

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

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

Low Battery Warning

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

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

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

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

The Low Battery Warning will transition to Critical Suspend before the computer powers off.

Critical Suspend State

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

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

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

Backup Battery

The mobile device has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The need for recharging of the backup battery is automatically detected and controlled by the operating system. The energy needed to charge the backup battery comes from the main battery.

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

The backup battery is replaced by LXE.

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

Backup Battery Maintenance

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

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

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

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

Battery Chargers

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

MX3 Multi-Charger Plus

Figure 2-18 MX3 Multi-Charger Plus

The main battery can be charged in the MX3 Multi-Charger Plus. The main battery charges the backup battery using the mobile device's internal charging circuitry.

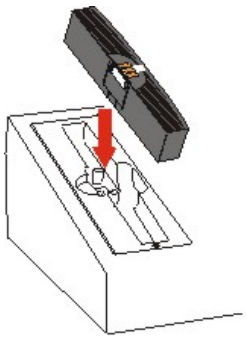


Figure 2-19 Insert Main Battery in Charge Pocket

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

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

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

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

Important Battery Charger Version Information

Battery Chargers Affected

MX3 Multi-Charger Plus
9000A377CHGR5

Use LXE V1.01 Upgrade Kit

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

Use LXE V1.20 Upgrade Kit

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

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

The mobile device device is designed to achieve 8+ hours of continuous operation.

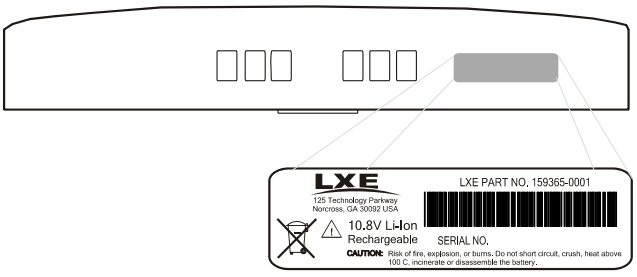
If the battery pack is inserted into a MX3 Multi-Charger Plus (*without the V1.01 upgrade*) bay, the battery may not become fully charged in the charger's 4 hour time limit and a red LED illuminates after 4 hours have elapsed indicating a Battery Problem.

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

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

Battery Label Location

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



External Power Supply (Optional)

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

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

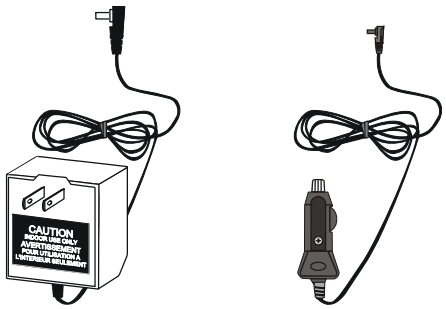


Figure 2-20 US AC/DC 12V Power Supply and Cigarette Lighter Adapter

Figure 2-21 International AC/DC 12V Power Supply

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

Note: The MX3P receives AC/DC power through the endcap power jack only. The passive vehicle cradle designed for these devices does not have power or communication capability. See "Accessories" for the MX3P passive vehicle cradle part number and description. The MX3P uses MX3P-specific cables.

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

Your MX3X operating system may be Windows CE .NET 4.2 or Windows CE 5.0. The MX3X 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 or Windows CE 5.0 user's guides or the Windows CE .NET on-line Help application installed in the mobile device.

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

Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX3X and it's 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 mobile 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 (was PocketWord in previous versions of Windows CE)
- Pocket Inbox
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer
- Scanner Wedge (LXE developed)
- ActiveSync
- Transcriber
- Media Player
- Internet Explorer

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

Optional

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.

AppLock (Option)

Installed by LXE. Applications are setup by the Administrator by tapping **Start | Settings | Control Panel | Administration**. 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.

See Chapter 6 "AppLock" for instruction.

Wavelink Avalanche Enabler (Option)

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

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

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

The MX3X has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. The designation of the mobile device to the Avalanche CE Manager is `LXE_MX3X`.

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).

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.

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

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

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

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

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

Desktop Icon	Function
My Computer (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 network card and Internet Service Provider – ISP enrollment is not available from LXE).
Wireless Client Setup Icon	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.

My Computer Folders (CE .NET 4.2)

Folder	Description	Preserved upon Reboot?
System	Internal ATA Card	Yes
Network	Mounted network drive	No
Storage Card	ATA Card in Compact Flash Slot 1	Yes
Windows	Operating System in ROM	No
Program Files	Applications	No
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Temp	Location for temporary files	No

Folders Copied at Startup

The following folders are copied on startup:

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

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

The following folders are *NOT* copied on startup:

Windows\AppMgr
Windows\Recent
Windows\Startup

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

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

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

My Device Folders (CE 5.0)

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downoaded 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 Program options 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: Start | Programs

Cisco	Set Cisco client / network parameters (See Chapter 5, "Wireless Network Configuration" for instruction.)
Communication	**Stores Network communication options**
ActiveSync	Transfer files between a mobile device and a desktop computer
Connect	Run this command after setting up a connection
Start/Stop FTP Server	Begin/end connection to FTP server
Diagnostics (optional)	**Diagnostic tests for the Mobile Device**
Registry Editor	Edit the mobile device registry (c a r e f u l l y)
Test Utility	Select a test to run e.g. Display, keyboard, audio.
Microsoft File Viewers	**View downloaded files** (see Note)
Excel Viewer	View Excel documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word and RTF files
Symbol	Tap the Network icon in the toolbar to set up the Symbol client (See Chapter 5, "Wireless Network Configuration" for instruction.)
Summit	Tap the Network icon in the toolbar to set up the Summit client network (See Chapter 5, "Wireless Network Configuration" for instruction.)
Command Prompt	The command line interface in a separate window
Inbox	Microsoft Outlook mail inbox.
Internet Explorer	Access web pages on the world wide internet
Java	Option
LXE RFTerm	Option. Terminal emulation application. RFTerm automatically opens as soon as a reboot is completed.
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server
Transcriber	Handwriting recognition program using an integrated dictionary
Wavelink Avalanche	Option. Remote management for networked devices.
Windows Explorer	File management program

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

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The RF client runs automatically during each reboot.

Communication

Access: **Start | Programs | Communication**

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

ActiveSync

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

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

Connect

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

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

The default connect setup is USB direct connect.

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

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

Start FTP Server / Stop FTP Server

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

Start | Programs | Communication | Start FTP Server

Start | Programs | Communication | Stop FTP Server

Command Prompt

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

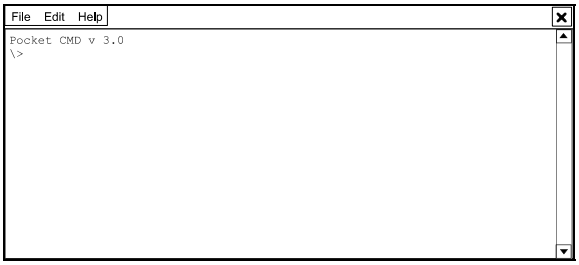


Figure 3-1 Pocket CMD Prompt Screen

Type help at the command prompt for a list of available commands.

Exit the Command Prompt by typing exit at the command prompt or select File | Close.

Inbox

Access: **Start | 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 mobile device inbox and a desktop inbox.

Internet Explorer

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

This option requires a network 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: **Start | 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.

Remote Desktop Connection

Access: **Start | Programs | 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.

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

Transcriber

Access: **Start | Programs | Transcriber**

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

Windows Explorer

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

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

Taskbar

Access: Start | Settings | Taskbar and Start Menu

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

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

There are a few changes in the CE 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.

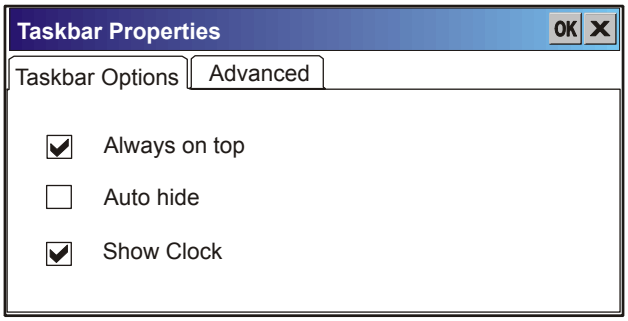


Figure 3-2 Taskbar Properties

Advanced Tab

Expand Control Panel

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

Clear Contents of Document Folder

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

Settings | Control Panel Options

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

or **My Computer icon | Control Panel (CE 4.2)**

or **My Device icon | Control Panel (CE 5.0)**

Getting Help

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

Option	Function
About	Displays software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility. See Chapter 6 for instruction.
Aironet Client Utility	Set the parameters for a Cisco client. (See Chapter 5, "Wireless Network Configuration" for instruction.)
Battery	View voltage and status of the main and backup batteries. Battery charge and discharge is performed using this option.
Bluetooth Device	Set the parameters for a Bluetooth radio. *Not available in this release.*
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings. Use Sync button to synchronize mobile device date and time with an internet time server.
Dialing	Set dialup properties for internal modems (modems are not supplied/supported by LXE).
Display	Set background graphic and color scheme. Set backlight properties and timers.
Input Panel	Select the current key / data input method.
Internet Options	*CE .NET 4.2* - Set General, Connection, Security and Advanced options for Internet connectivity. *CE 5.0* – Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.

Option	Function
Password	Set access password properties for signon and/or screen saver.
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.
PCMCIA	Network card in Slot 0, Internal ATA in Slot 2.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Select to remove specific user installed programs in their entirety. *Note: Programs listed in this location are deleted upon warm and cold boot processes.*
Scanner	Set scanner 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 "Determine Your Scanner Software Version".
Storage Manager	Manage storage devices, create partitions.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses	(*CE 5.0 only*) Select a server client license from a drop down list (Not available at this release).
Volume and Sounds	Enable/disable volume and sounds. Set volume parameters and assign sound wav files to CE events.

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

About

Access: Start | Settings | Control Panel | About

Displays hardware and software details.

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

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

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

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

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

Language and Fonts

The **Software** tab displays any fonts built into the OS image.

The fonts built into the OS image are noted in the Language section of this tab:

- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian fonts are ordered separately and built-in to the OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

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

Identifying Software Versions

The "Versions**"** tab displays the versions of many of the software programs installed. Not all installed software installed on the mobile device is included in this list and the list varies depending on the applications loaded on the MX3X. The LXE Image line displays the revision of the system software installed. Please refer to the last three digits to determine the revision level.

MAC Address

The "Network IP" tab displays the MAC address of the network card.

Accessibility

Access: Start | Settings | Control Panel | Accessibility

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sound 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 selected, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Administration – for AppLock

Access: Start | 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 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 as specified by the Administrator.

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

Battery

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

View the status of the Main and Backup batteries.

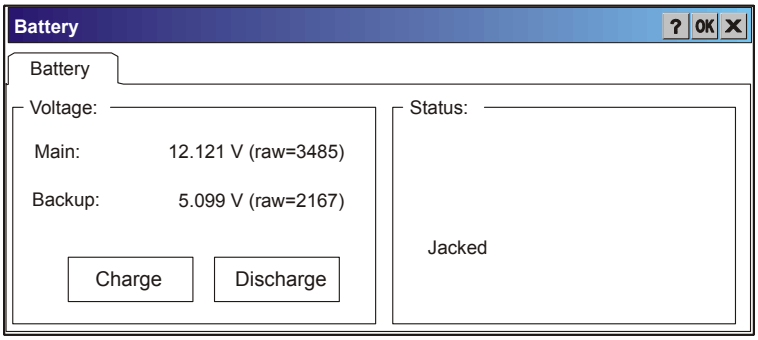


Figure 3-3 Battery

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

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

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

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

The Main Battery is charged only when an AC adapter is connected via the endcap, the MX3X is docked in a powered cradle or when the Main Battery is removed from the MX3X and placed in the MX3 Multi-charger.

Bluetooth Manager

Note: May or may not be available in every MX3X version.

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

Set the parameters for a Bluetooth radio. *Bluetooth Manager, Bluetooth service or options are not available for all MX3X devices or in all MX3X software releases.*

Factory Default Settings	
All Found Devices	Untrusted

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

Certificates

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

Manage digital certificates used for secure communication.

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

See Chapter 5 “Wireless Network Security” section titled “Certificates” for instruction.

Lists the Stored certificates trusted by the MX3X user. These values may change based on the type of network security resident in the client, access point or the host system.

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

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

Tap the **Remove** button to remove a highlighted certificate file.

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

See Also: Chapter 5 “Wireless Network Configuration” for instruction.

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

Date/Time

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

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

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

Note: (CE .NET 4.2 only) Date and time is reset to the factory default value each time the mobile device is cold booted.

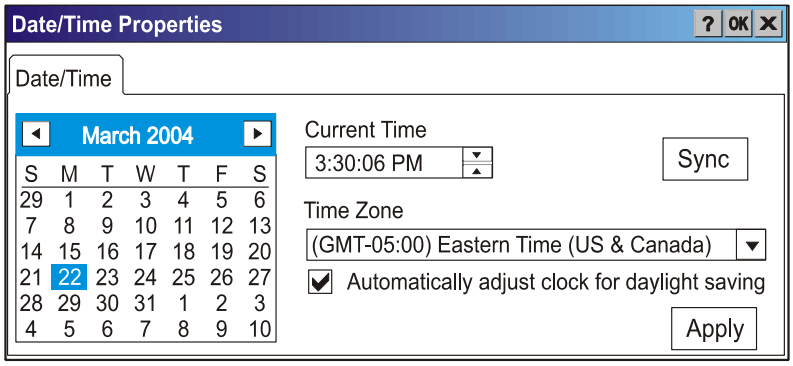


Figure 3-4 Date/Time Properties

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

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

The MX3X includes a **GrabTime** utility which can be configured to synchronize the time at each boot up. Please see “Enabling GrabTime”, in the “Utilities” section, for details.

Dialing

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

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

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

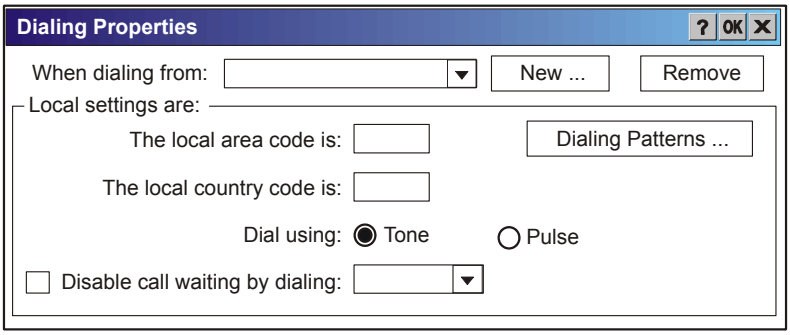


Figure 3-5 Dialing

Tap the "?" and follow the instructions in Help.

Display

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

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

Factory Default Settings	
Background	Windows CE or CE .NET
Tile	Disable
Appearance	
Scheme: Monochrome Color	 High Contrast White Windows Standard
Backlight	
Battery Power Auto Turn Off	Enabled
Idle Time	3 Seconds
External Power Auto Turn Off	Enabled
Idle Time	2 minutes

Background

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

Appearance

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

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

Backlight

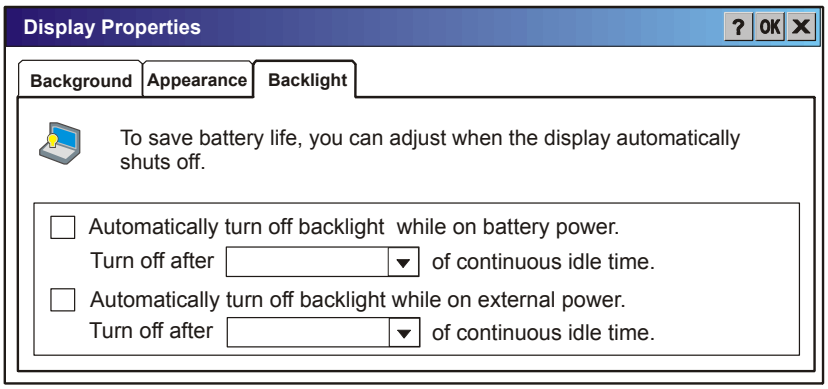


Figure 3-6 Display Properties / Backlight Tab

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

Input Panel

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

Select the current key / data input method.

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

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

Enable the input panel by checking "Allow applications to change the input panel's state". Then tap the OK button.

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

Tap the "OK" button to save any changes and exit, or tap the "X" button to exit without saving any changes. Tap the "?" button for Help. Warmboot the device to store the changed setting.

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

Internet Options

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

Windows CE .NET 4.2

Set General, Connection, Security and Advanced options for internet connectivity. Select a tab. Adjust the settings and tap the OK box to save the changes. Changes are saved from tab to tab. Tap the Clear Cache or Clear History buttons to clear files that have been downloaded to the mobile device during internet use. The changes take effect immediately. Help is not available for this option.

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

Factory Default Settings	
Enable web scripting	Enabled
Display script error note	Disabled
Underline links	Never

Windows CE 5.0

Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.

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

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
User Agent	Windows CE
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
Session cookies	Always allow
Advanced	
Stylesheets	Enable
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Keyboard

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

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

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key Map	0409 (CE .NET 4.2) Default (CE 5.0)

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

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

These values do not affect virtual keyboard taps.

Mixer

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

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

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

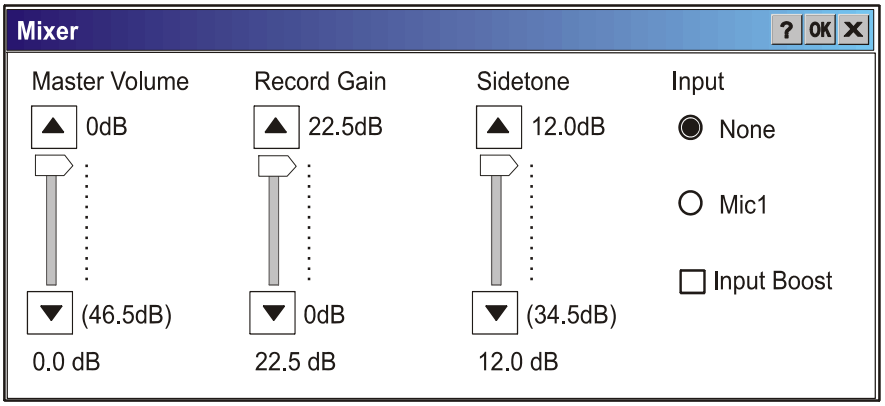


Figure 3-7 Mixer

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

Note: Set Input to "None" when using stereo headphones. Set Input to "Mic1" when using a mono headset with microphone.

Mouse

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

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

Network and Dialup Connections

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

Create a dialup, direct, or VPN connection on the mobile device. To configure the mobile device to use DHCP or a fixed IP address, select the desired connection. The default is to obtain an IP address via DHCP.

A static IP address can be assigned by tapping the **Specify an IP address** radio button and entering the desired IP address, subnet mask and gateway.

Create a Connection Option

1. On the mobile device, select **Start | Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the one you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (IR @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the Next button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the **Port Settings** tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off **Wait for dial tone**, since a direct connection will not have a dial tone. Set the timeout parameter (default is 90 seconds). Tap OK.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start | Settings | Control Panel | PC Connection** and tap the **Change** button.
11. Select the new connection. Tap OK twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. 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: **Start | Settings | Control Panel | Owner Icon**

Set mobile device owner details.

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

Enter the information and tap the OK box to save the changes. The changes take effect immediately.

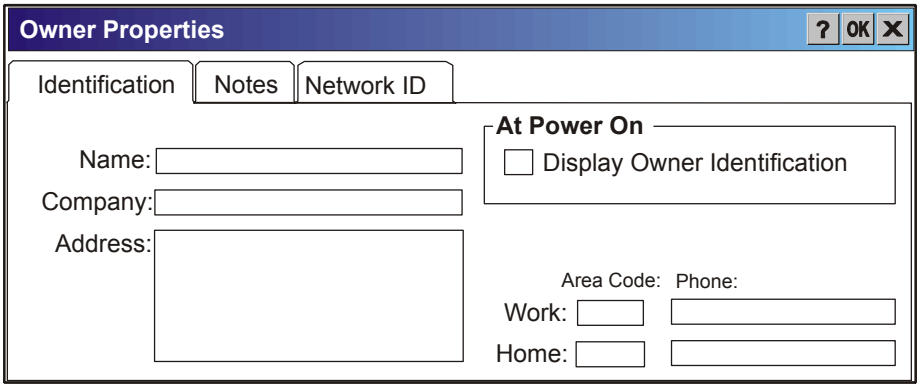


Figure 3-8 Owner Properties

Password

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

Set user access and power up password properties.

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

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

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

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

Tap the **Screen Saver** checkbox to set whether the user types a password to clear the screensaver. If there is no screensaver chosen, this checkbox is ignored. The screensaver password affects the Remote Desktop screensaver only.

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.

Note: Screensavers are not installed by LXE.

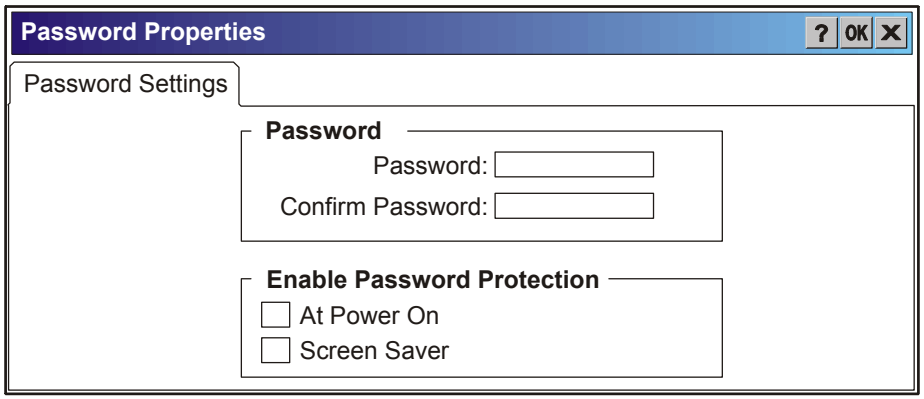


Figure 3-9 Password Properties

PC Connection

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

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

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

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

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

Change ….

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

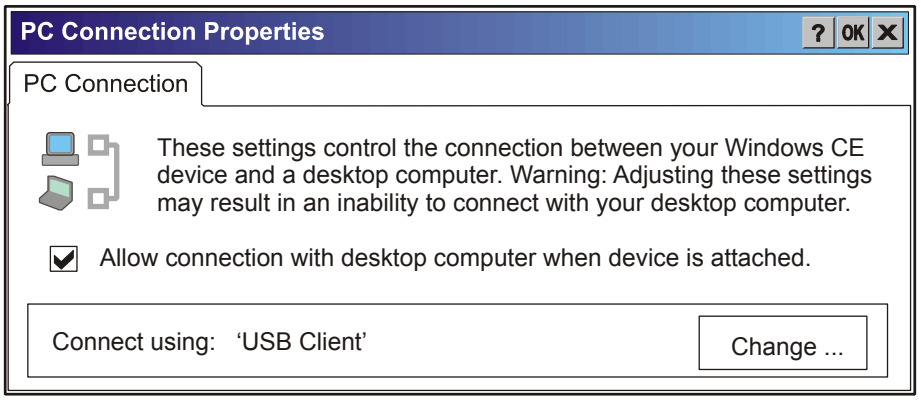


Figure 3-10 Communication / PC Connection Tab

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

PCMCIA

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

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

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

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

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

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

When there is no card in a slot, the options are dimmed.

Power

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

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

Note: Control Panel parameters established in Power Properties affect the mobile device operating system.

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

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

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

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

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

Battery

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

Schemes

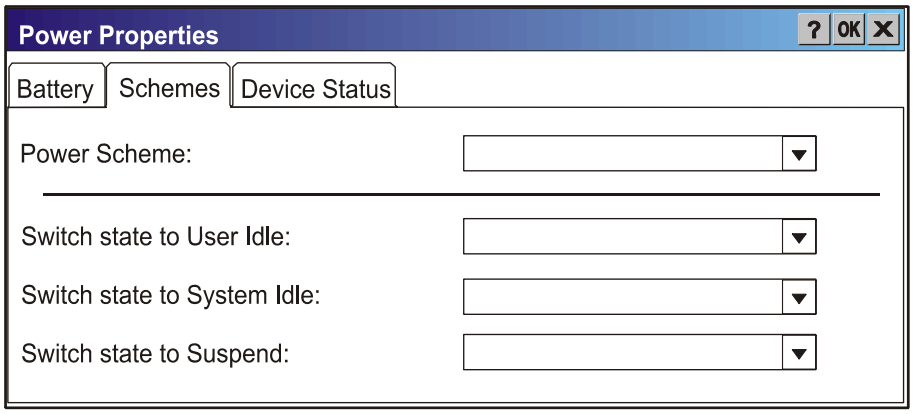


Figure 3-11 Power Schemes

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

Battery Power Scheme

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

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

AC Power Scheme

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

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

Device Status

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

Regional Settings

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

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

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

Options (and defaults) for the regional settings depend on the fonts included in the OS image. Please refer to the section on the **About** control panel earlier in this chapter for more details.

CE . NET 4.2 Default 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

CE 5.0 Default Settings

A language must be installed before it can be selected. After selecting a language to use, and after all changes are made, tap OK to save your changes then warmboot the device.

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

Tap the **Customize** button to set Number, Currency, Time and Date format for the selected Locale. User Interface Language determines the language used for the menus, dialogs and alerts. Select the Default Input Language to use when the device is rebooted.

Remove Programs

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

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

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

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

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

Scanner

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

Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Scanner parameters apply to the MX3X integrated scan engine *only*. Barcode manipulation parameters apply to barcodes scanned by the integrated scan 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 Scan LED is solid amber. The scanner is not operational during the configuration update.

	Please refer to the "MX3-RFID Reference Guide" when setting up scanner parameters for the MX3-RFID mobile device.

Determine Your Scanner Software Version

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX3X devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device. To identify the software version, tap the "About" icon in the Control Panel.

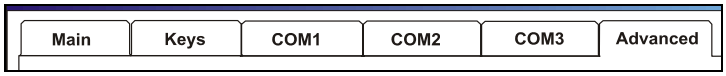
Scanner Control Menu Structure Versions Tabs	Go to . . . .
	This chapter, section titled "Scanner"
	Chapter 4 "Scanner", section titled "Advanced".
	Chapter 4 "Scanner", section titled "Barcode Manipulation".

Figure 3-12 Determine Your Scanner Software Version

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

Factory Default Settings

Factory Default Settings	
Main	
Port 1	Internal
Port 2	Disabled
Power Port 1 while asleep	Disabled
Send key messages WEDGE	Enabled
Keys	
Left	Scan
Right	Enter
COM Ports (COM1- COM2 – COM3)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	8

Notes:

- If the internal scanner has to be configured to operate at any communication settings other than 9600, N, 8, 1 and the computer either loses power or a cold boot command is entered, the Scanner applet must be reconfigured to match the scanner communication settings.
- When there is no internal scanner, Port 1 is disabled and the Left Scan button is an Enter key.
- ActiveSync will not work over a COM port if that COM port is enabled in the Scanner applet as a scanner input. For example, if COM 1 is being used by the scanner, COM 1 can't be used by any other program.
- When an RFID module is not installed, the RFID option on the Keys tab is greyed out. See the "MX3-RFID Reference Guide" for instruction when using the MX3-RFID.

Main

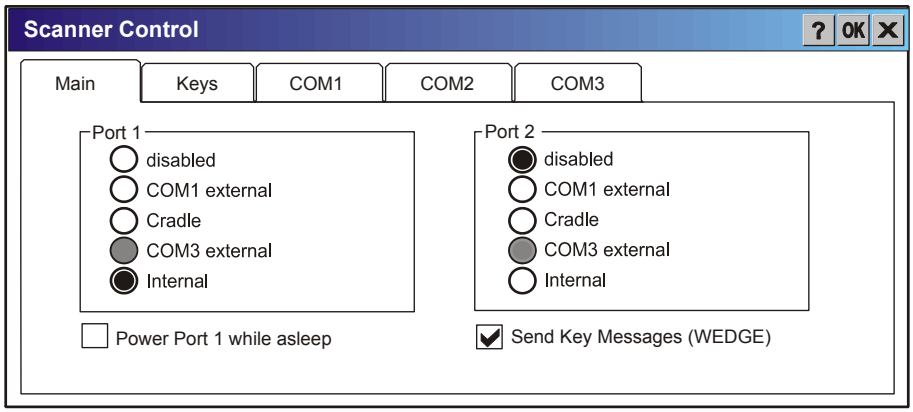


Figure 3-13 Scanner Properties / Main Tab

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

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

If "Send Key Messages …" is checked any data scan is converted to keystrokes and sent to the active window. When this box is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using "Wedge". Even if Send Key Messages is enabled ("key mode"), the data is still available using the scanner APIs ("block mode").

The Scan buttons have no effect on tethered external scanners connected to the RS-232 connector on the endcap.

Keys

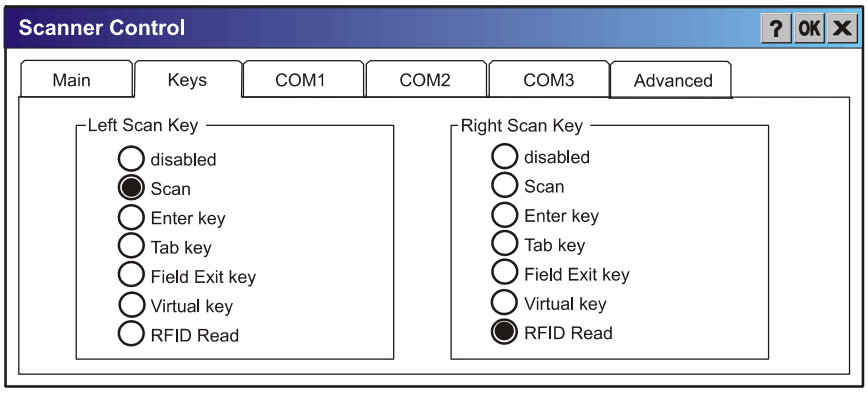


Figure 3-14 Scanner Properties / Keys Tab

See the "MX3-RFID Reference Guide" when using an MX3X with an RFID Module.

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

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

Change a Virtual Key (F20 or F21) Value

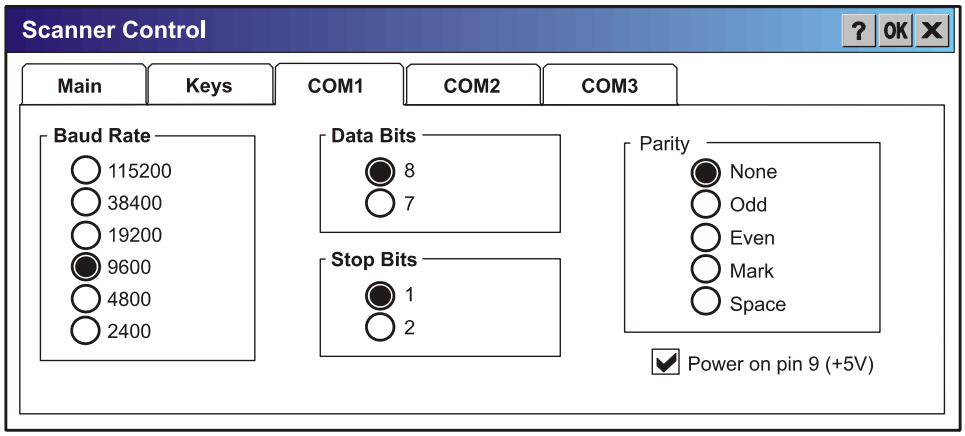
Modify the Registry using the Registry Editor (see section titled “Utilities”). LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

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

COM Ports

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



COM1, COM2 and COM3 Panel Options are Identical.

Figure 3-15 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.

“Power on Pin 9” on the COM2 panel is disabled.

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

See the “MX3-RFID Reference Guide” when using an MX3X with an RFID Module.

Storage Manager

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

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

On-line help is available for this option.

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

LXE recommends **caution** when formatting or dismounting storage devices and when creating new partitions or deleting partitions on the storage device. Using the storage manager to perform operations on the internal ATA is no longer available as of July 2006.

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

Stylus

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

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

Double Tap

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

Calibration

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.

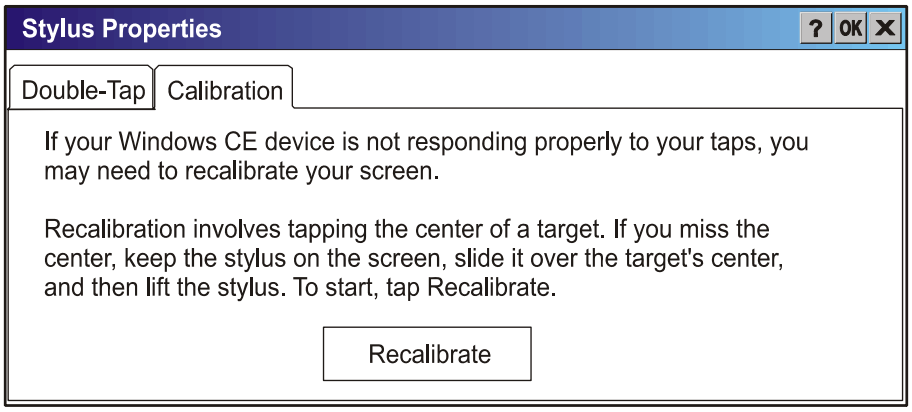


Figure 3-16 Stylus Properties / Recalibration Start

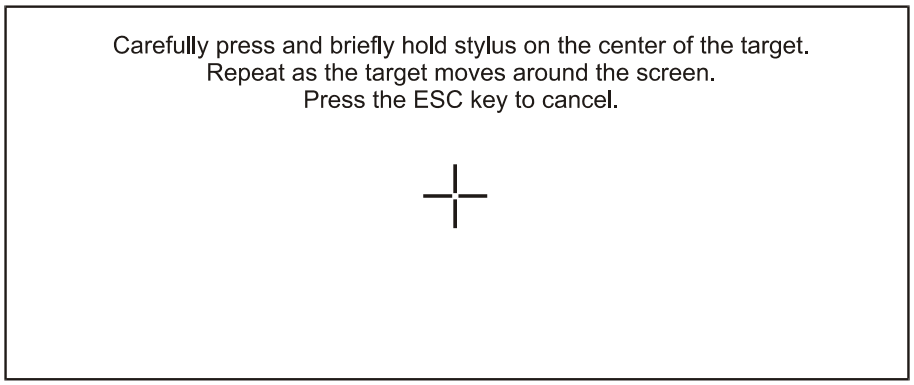


Figure 3-17 Stylus Properties / Recalibration

System

Access: Start | Settings | Control Panel | System Icon

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

Factory Default Settings	
General	N/A
Memory	1/3 storage, 2/3 programs.
Device Name	MX3X001
Device Description	LXE_MX3X
Copyrights	N/A

Persist RAM Base Files

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

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

General

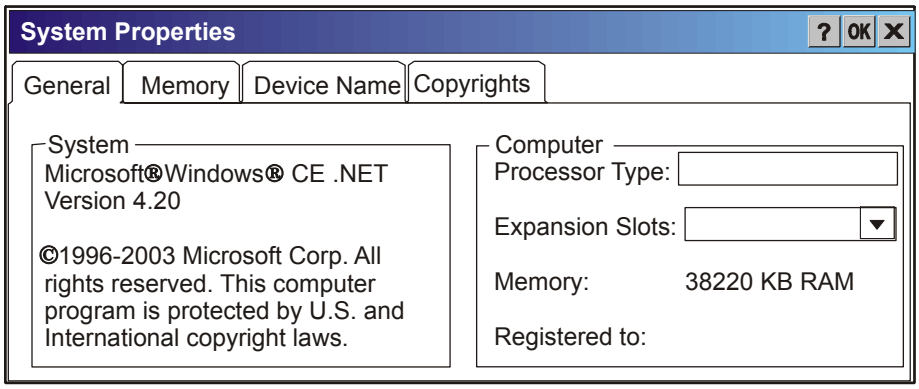


Figure 3-18 System / General tab

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

Computer: The processor type is listed. The type cannot be changed by the user. The name of the installed network 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 operating system. This is actual DRAM memory, and does not include internal flash or the internal ATA card used for storage.

Memory

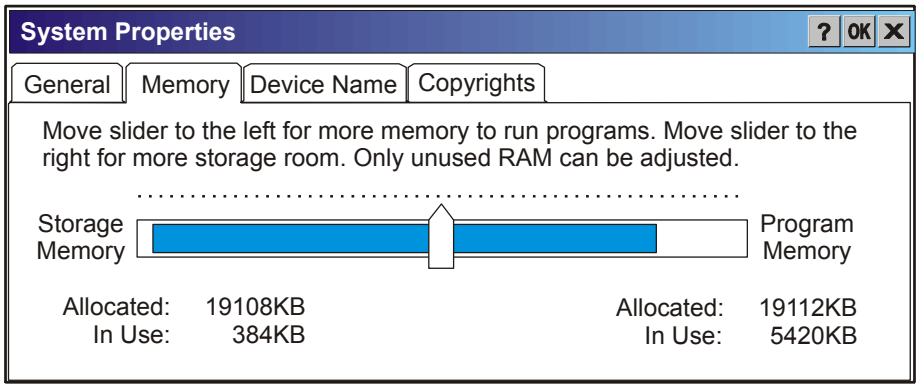


Figure 3-19 System / Memory

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

Device Name

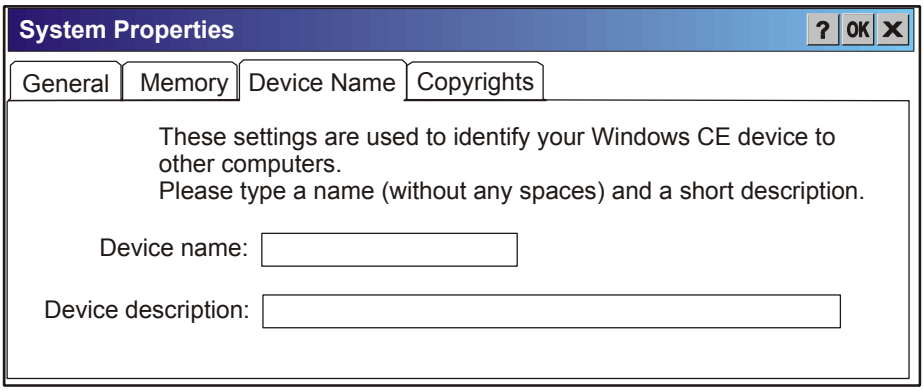


Figure 3-20 System / Device Name

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.

Terminal Server Client Licenses

(*CE 5.0 only*) Select a server client license from a drop down list

Not available at this release.

Volume and Sounds

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

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

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

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

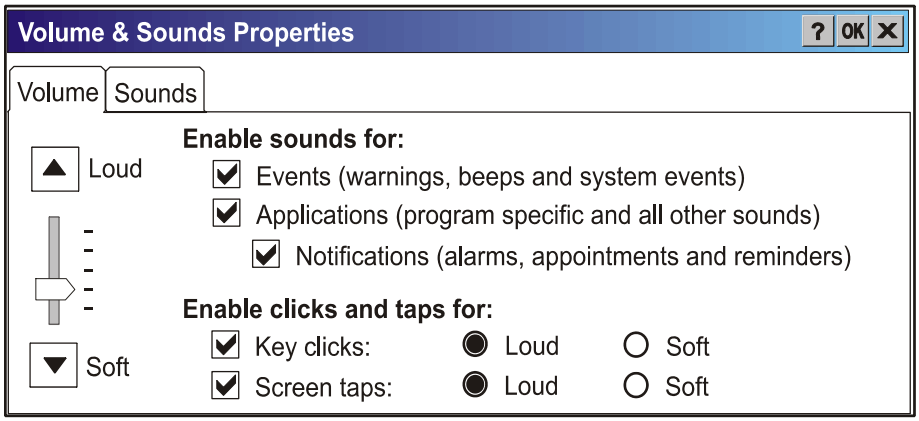


Figure 3-21 Volume and Sounds

Good Scan and Bad Scan Sounds

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

Note: 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 barcode processing causes a bad scan beep from the MX3X on the same data.

Utilities

These utilities are pre-loaded by LXE.

LAUNCH.EXE

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

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

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

FileName is the name of the CAB file, with the path (usually \System)
Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file
FileCheck is the name of a file to look for to determine if the CAB file is installed.

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

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

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

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

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

The **Order** field is used to force a sequence of events; **Order=0** is first, and **Order=99** is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence. Note: If the order of loading is not critical, it may be easier to use the \System\Startup folder instead; see below (only on **.01D** or newer images).

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

The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a wireless client driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the "Unidentified PCMCIA Slot" dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field

is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default wireless client drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.

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

Registry information is already in the default image for the following [3]:

```
        ; Summit client
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Summit Radio]
        "FileName"="\SYSTEM\SUMMIT.CAB"
        "Installed"=dword:1
        "FileCheck"="\WINDOWS\SDCCFG10G.DLL"
        "Order"=dword:02
        "Delay"=dword:0
        "PCMCIA"=dword:1

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

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

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

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

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

[3] CAB files for options not purchased are not loaded e.g. JAVA or RFID. If a CAB file is missing, please contact your LXE Representative.

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

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

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

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

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

        ; Avalanche (prior to October 2006)
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
        "FileName"="\SYSTEM\LXEAVA.CAB"
        "FileCheck"="\SYSTEM\AVALANCHE\MODEL.DAT"
        "Order"=dword:4
        "Installed"=dword:0
        "PCMCIA"=dword:0
        "Delay"=dword:0

        ; Avalanche (prior to October 2006)
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
        "FileName"="\SYSTEM\AVALANCHE\AVAINIT.EXE"
        "FileCheck"="dummy"
        “Order”=dword:5
        "Delay"=dword:0
        "PCMCIA"=dword:0
        "Installed"=dword:0
```

When you are installing your custom CAB file to the mobile device’s operating sytem, refer to the default image segments that are commented with “… RFTERM …” to see the expected Registry format.

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

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

To have files (CAB, EXE, REG, or WAV files) loaded on startup, when sequence of execution is not important, you can put these files in the \System\Startup folder (on the internal ATA card). This is parsed by the Launch utility, and these programs are started or executed. Note that this only works on images from **.01D** and newer.

REGEDIT.EXE

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

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

REGLOAD.EXE

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

WARMBOOT.EXE

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

WAVPLAY.EXE

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

Enabling GrabTime

The MX3X has a GrabTime utility which can automatically synchronize the MX3X with a time server (an active Internet connection is required) at boot up.

By default, using GrabTime for time synchronization at boot up is Off. Grabtime can be run at any time (even when Off at boot up) using the Sync button on the Date/Time control panel.

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

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

Disabling the Touchscreen

To disable the touchscreen, run \Windows\TouchDisable.reg and perform a warm reboot.

To enable the touchscreen, run \Windows\TouchEnable.reg and perform a warm reboot.

Note: These utilities affect the behavior of the touchscreen on warmboot. After a coldboot, the touchscreen is enabled. Enable this option with caution when switching from AppLock Administrator mode to AppLock User Mode.

Troubleshooting: Touchscreen is not accepting stylus taps or need recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and cursor keys to move the cursor from element to element.

Configuring CapsLock Behavior

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

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

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

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

Configuring IPv6

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

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

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

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

Command-line Utility

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

COLDBOOT.EXE

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

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

PrtScrn.EXE

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

API Calls

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

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

The APIs documented in the programming guide are included in the file LXEAPI.ZIP, which is in the LXE MX3X SDK kit. See "Accessories".

For ease of software development, the files LXEAPI.H and LXEAPI.LIB are available in the MX3X SDK, which are the include files and the link library for the DLL, respectively. Note that this DLL is installed in mobile device images with a version number of 1.2 or higher (as displayed on the screen during bootup).

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

Wavelink Avalanche Enabler Configuration

An MX3X 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.

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: LXE recommends serial communication with an MX3X be performed using the serial port on the MX3X endcap rather than using a docking cradle serial port.

Note: On LXE mobile devices with integrated scanners, the Scanner Wedge has primary control of the serial ports and must be configured properly to allow the Enabler to access the serial ports.

Enabler Install Process

- Doubletap the Avalanche Enabler CAB file in the System folder. The filename is LXE_MX3X_ENABLER.CAB.
- Warm boot the mobile device.

Enabler Uninstall Process

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

- Delete the Avalanche folder located in the System folder.
- Warm boot the mobile device.

The Avalanche folder cannot be deleted while the Enabler is running. See *Stop the Enabler Service*. If sharing errors occur while attempting to delete the Avalanche folder, warm boot the mobile device, immediately delete the Avalanche folder, and then perform another warm boot.

Orphaned Packages

To prevent the enabler from restoring parameters, delete orphaned packages through the 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_MX3X`.

The Enabler running on LXE Windows CE devices will attempt to access COM1, COM2, and COM3. "Agent not found" will be reported 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 setting are:

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

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

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

The designation of the mobile device to the Avalanche CE Manager is `LXE_MX3X`.

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.

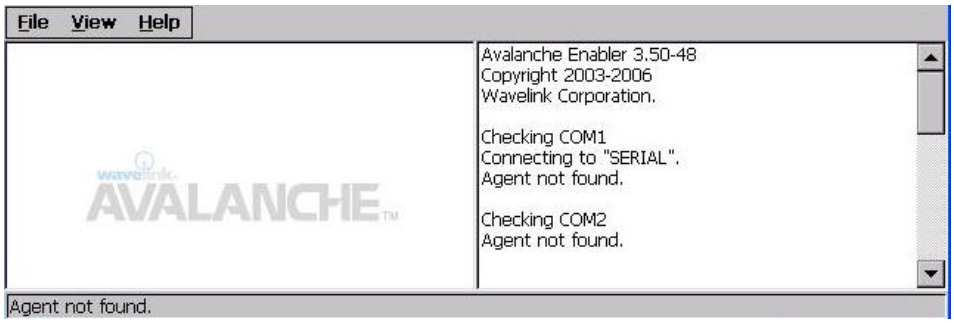


Figure 3-22 Avalanche Enabler Opening Screen

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	*Note: LXE does not support the Scan Configuration feature on Windows CE devices.* The Scan Config option under the File menu allows the user to configure Enabler settings using a special barcode that can be created using the Avalanche Management Console utilities. Refer to the *Wavelink Avalanche 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:  Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Avalanche Update Settings

Access: **Start | Avalanche | File | Settings**

Use these menu options to setup the Avalanche Enabler on the mobile device. LXE recommends changing and then saving the changes (reboot) before connecting to the network.

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

Menu Options

Settings Tab	Function
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

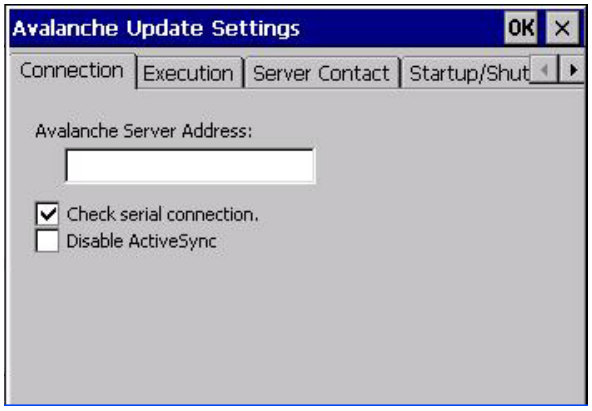


Figure 3-23 Connection Options

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.

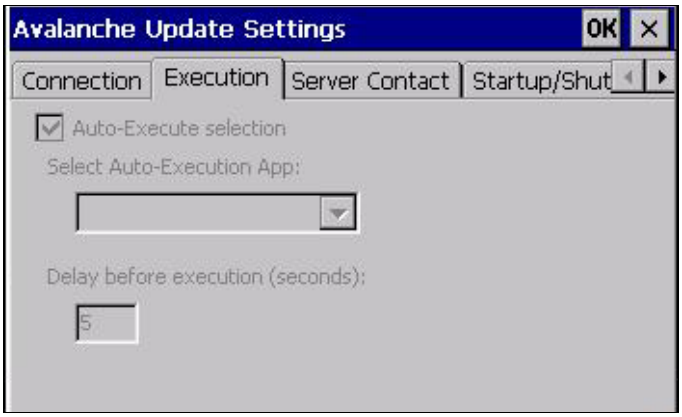


Figure 3-24 Execution Options (Dimmed)

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 3-25 Server Contact Options

Sync Clock	Reset the time on the 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.
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.

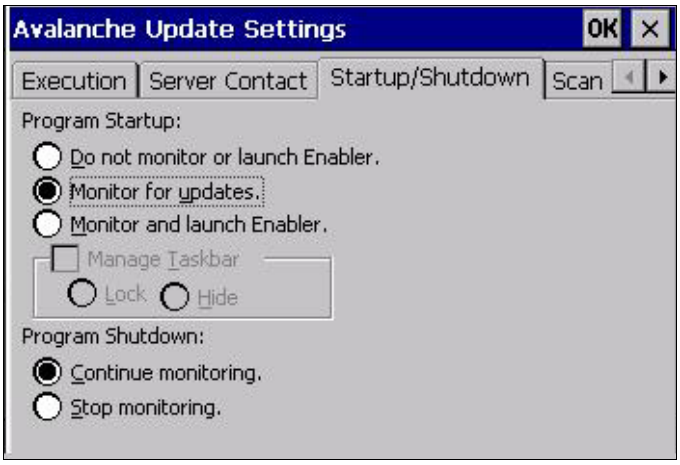
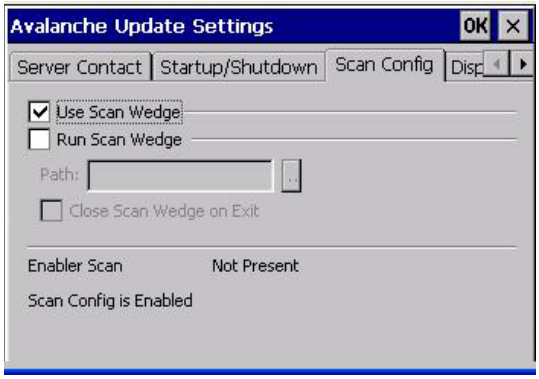


Figure 3-26 Startup / Shutdown Options

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 3-27 Scan Config Option

Display

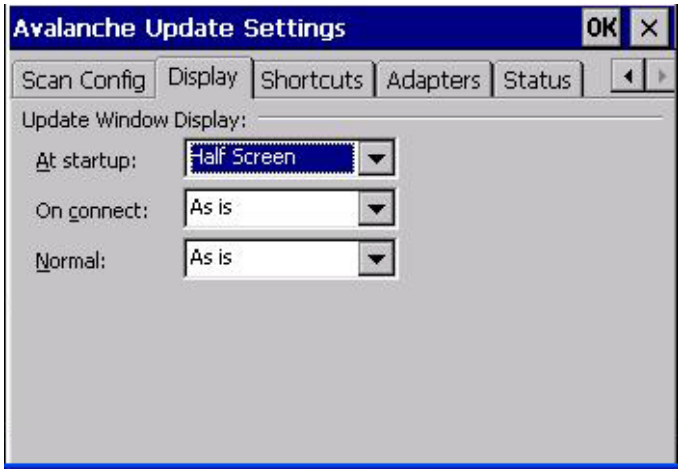


Figure 3-28 Window Display Options

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.

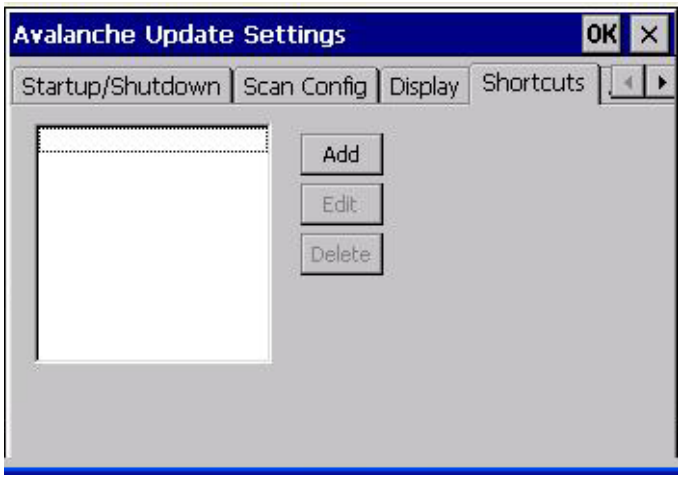


Figure 3-29 Application Shortcuts

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.

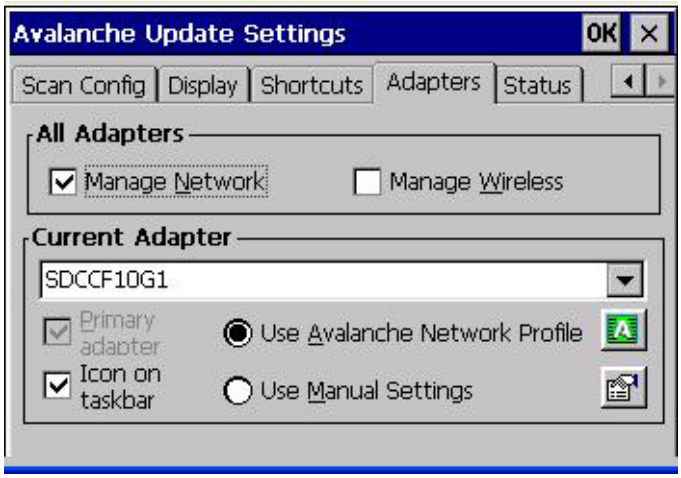
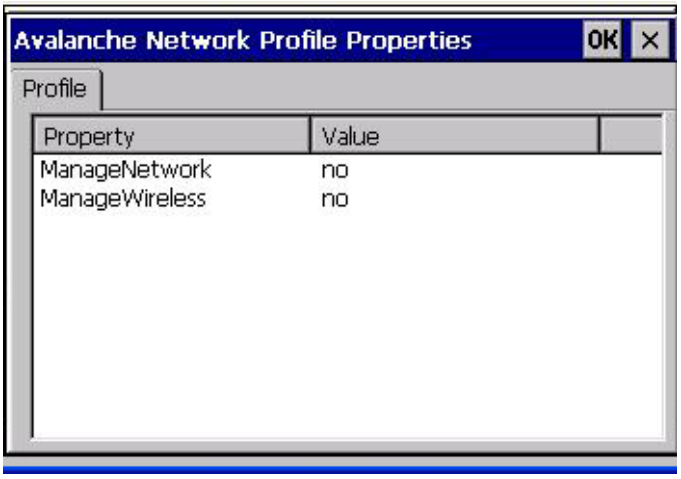


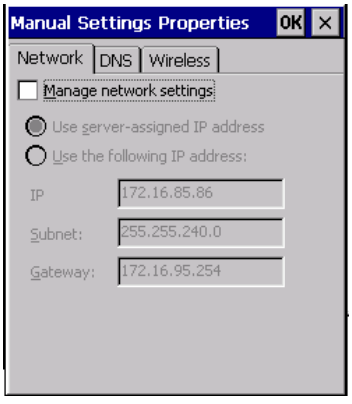
Figure 3-30 Adapters Options – Network

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 *only***.
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Management Console.

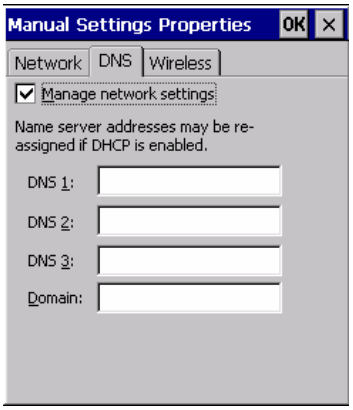
Avalanche Icon 	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.  **Figure 3-31 Avalanche Network Profile Displayed**
Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche Management Console and use only the network settings on the mobile device.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

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

Network



DNS



Wireless

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

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

Figure 3-32 Manual Settings Properties Panels

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global **Manage wireless settings** and **Manage network settings** options are enabled on the Adapters panel (see Figure titled *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..

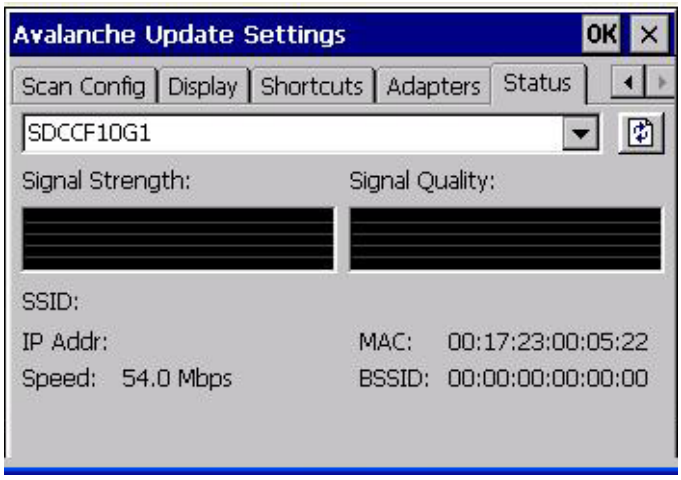


Figure 3-33 Status Display

Link speed indicates the speed at which the signal is being sent from the adapter to the mobile device. Speed is dependent on signal strength.

Troubleshooting

Cold Boot

If a device managed by Avalanche is cold-booted, a warmboot MUST be performed following the coldboot. Failure to perform the warmboot will leave the device in an undetermined configuration and it may not perform as expected. If the intention is to stop using Avalanche to manage the device configuration, please see “Enabler Uninstall Process” earlier in this section.

Reflash the Mobile Device

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

Caution 	Make sure the main battery has been fully charged before beginning the reflash procedure. Depleting the backup battery during the reflash process can result in corrupted files.

Requirement: A screwdriver (not supplied by LXE)

Preparation

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

How To : Reflash using Keypress Method

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

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

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

How To: Reflash using TAG file Method

1. Place the compact flash card with new image files on it in the right hand slot.
2. Double-tap **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Double-tap **\System** folder.
5. Select **Edit | Paste**. When asked "Overwrite ?", tap **Yes to All**.
6. Additionally a REFLASH.TAG file is needed to trigger the reflash. This file can be created on the MX3X or copied to it along with the system files. The contents of the file are unimportant; but the file must be named REFLASH.TAG and it must be in the **\System** folder with the new system load.
7. When the copy process finishes, remove the CF card.
8. Select **Start | Run** and type **Coldboot**.
9. When booting, the MX3X looks for a file named REFLASH.TAG in the \System folder.

   When REFLASH.TAG is encountered, the MX3X loads a new bootloader image (eboot.nb0) into the boot flash. The tag file is deleted and the MX3X is rebooted to begin using the new boot loader. If there is no .nb0 file it does not re-flash and deletes the REFLASH.TAG file to prevent an endless cycle.
10. The mobile device automatically reboots after flashing the bootloader. "Loading OS Image" is displayed on the screen and when the new OS finishes loading, all software upgrades are complete
11. Replace the endcap, being careful not to pinch any leads or cables. The touchscreen will need to be re-calibrated.

Clearing Persistent Storage

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

Important:

Contact LXE Customer Support prior to upgrading MX3X Windows CE .NET 4.2 to Windows CE 5.0.

Chapter 4 Scanner

Introduction

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

Set scanner keyboard wedge parameters, enable or disable symbologies from being scanned, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.

Determine Your Scanner Software Version

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

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX3X devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device. To identify the software version, tap the "About" icon in the Control Panel.

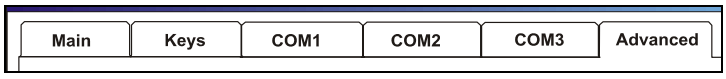
Scanner Control Menu Structure Versions Tabs	Go to . . . .
	Chapter 3, "System Configuration", section titled "Scanner"
	This chapter, section titled "Advanced".
	This chapter, section titled "Barcode Manipulation".

Figure 4-1 Determine Your Scanner Software Version

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.

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 Manipulation” section.

Barcode Manipulation

Access: Start | Settings | Control Panel | Scanner

If your scanner applet has an “Advanced” tab instead of a “Barcode” tab, please see section titled “Advanced” at the end of this chapter.

Factory Default Settings	
Main	
Port 1	COM1
Power Port 1 while asleep	Disabled
Enable Internal Scanner Sound	Enabled
Send Key Messages (WEDGE)	Enabled
Bluetooth	Disabled (Dimmed)
Output Enable	Disabled (Dimmed)
COM3	Disabled (Dimmed)
Port 2	Disabled
Enable Internal Scanner Sound	Enabled
Send key messages WEDGE	Enabled

Factory Default Settings	
Main	
Bluetooth	Disabled (Dimmed)
Output enable	Disabled (Dimmed)
COM3	Disabled (Dimmed)
Keys	
Left Scan key	Scan
Right Scan key	Enter key
COM Ports (COM1 - COM2 – COM3)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	8
Power on Pin 9 (+5v)	Disabled
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 MX3X either loses power or a cold boot command is entered, the Scanner applet must be reconfigured to match the scanner communication settings.
- 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.
- 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.
- The MX3P does not have an integrated scanner or RFID capability.

Main Tab

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

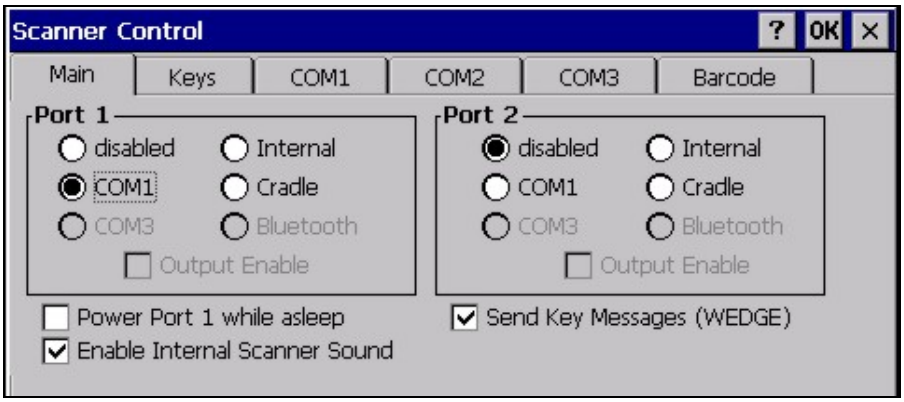


Figure 4-2 Scanner Control / Main Tab

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

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

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.

When **Enable Internal Scanner Sound** is checked, the functionality of the internal scanner driver engine includes audible tones on good scan (at the maximum db supported by the speaker) and failed scan. 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 MX3X on the same data.

Keys Tab

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

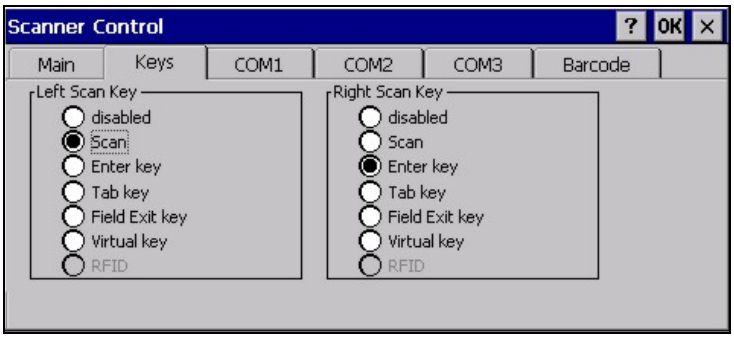


Figure 4-3 Scanner Control / Keys Tab

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.

Note: The left and right Scan buttons have no effect on tethered external scanners connected to an RS-232 connector on the endcap.

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

Change a Virtual Key (F20 or F21) Value

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

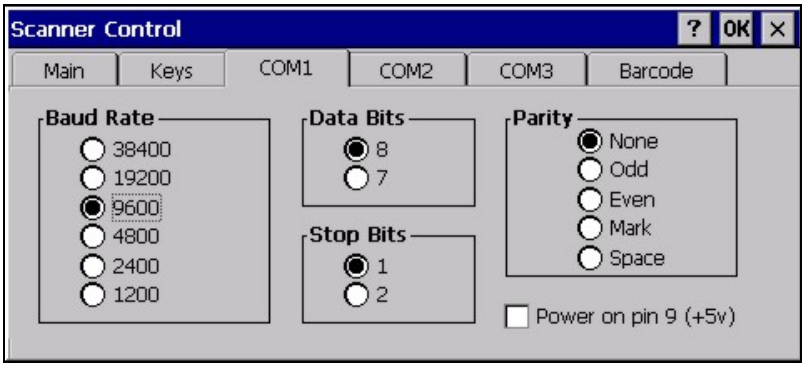
Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

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

COM Port Tabs

Access: **Start | Settings | Control Panel | Scanner | COM1 or COM2 or COM3**

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



COM1, COM2 and COM3 Panel Options are Identical.

Figure 4-4 Scanner Control / COM Port Tab

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. The COM 1 tab contains the same parameters as the COM 2 and COM 3 Tab. “Power on Pin 9” on the COM 2 panel is disabled. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Barcode Tab

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

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

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

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

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

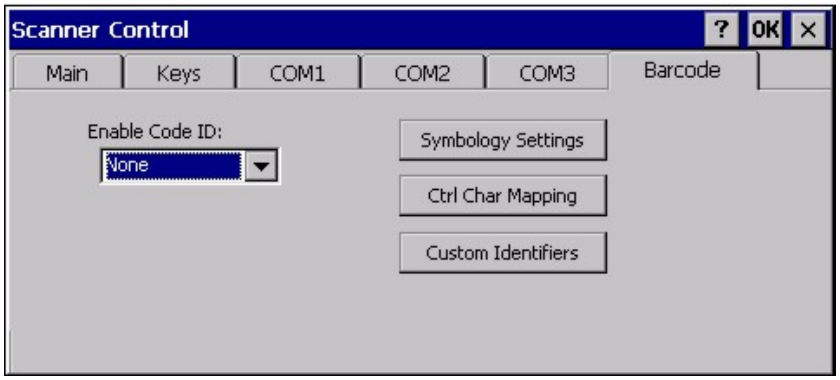


Figure 4-5 Scanner Control / Barcode tab

Buttons

Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

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

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 custom code ID string is stripped (i.e. treated as a Code ID).
- **UPC/EAN Codes only**: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to **AIM or Symbol,** Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to **Custom**, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to **Custom**, **AIM or Symbol Code IDs** must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 ']A1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID : `]A1AAA`.
- When Enable Code ID is set to **None**, Custom Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog. They are 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 MX3X scanner application; 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 MX3X emits 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 list contains all symbologies supported on the MX3X. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

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

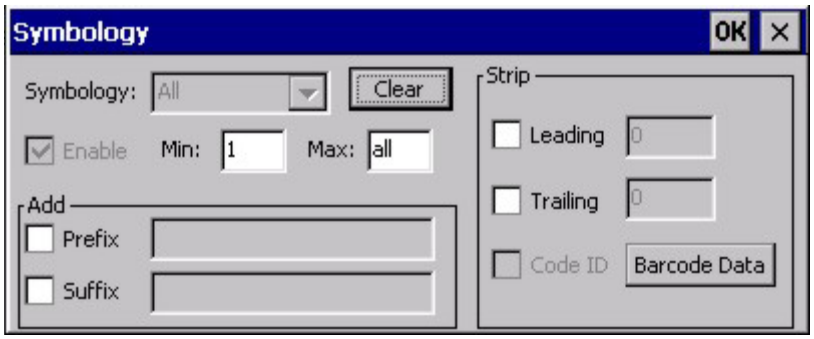


Figure 4-6 Barcode Tab – Symbology Settings

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

The order in which these settings are processed are:

- 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's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults. If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two. If a symbology has not been configured (does not have an * next to it) the settings for "All" are used which are not necessarily the defaults.

Parameters

Enable	This checkbox enables (checked) or disables (unchecked) the symbology field. The scanner driver searches the beginning of the barcode data for the type of ID specified in the Barcode tab – Enable Code ID field (AIM or Symbol) plus any custom identifiers. When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed. If the symbology is disabled, all other fields on this dialog are grayed. When there are ***no*** *customized settings*, and the Enable checkbox is unchecked (All is selected and no other settings are customized) a confirmation dialog is presented to the user "You are about to disable all scan input – Is this what you want to do?". Tap the Yes button or the No button. Tap the X button to close the dialog without making a decision. If there ***are*** *customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies except the customized ones.
Min	This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed. Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.
Max	This field specifies the maximum length that the barcode data (not including Code ID) can be to be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All. If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length will be used instead.

Strip Leading/Trailing Control

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.

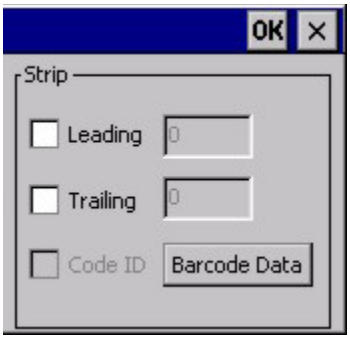


Figure 4-7 Strip Leading/Trailing Controls

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.

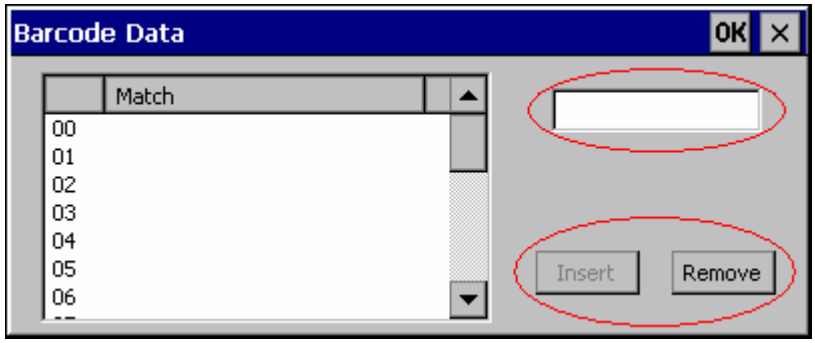


Figure 4-8 Barcode Data Match List

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.
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. It is valid to have more than one ***?*** in a string to match multiple characters.
- 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.

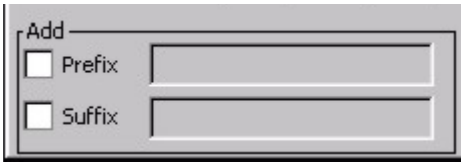


Figure 4-9 Add Prefix/Suffix Controls

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see the "Hat Encoding" section in Appendix B for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pulldown list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.

Add Suffix To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pulldown list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

See "Hat Encoding" and "Decimal-Hexadecimal Chart" in Appendix B "Technical Specifications".

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

Barcode – Ctrl Char Mapping

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

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

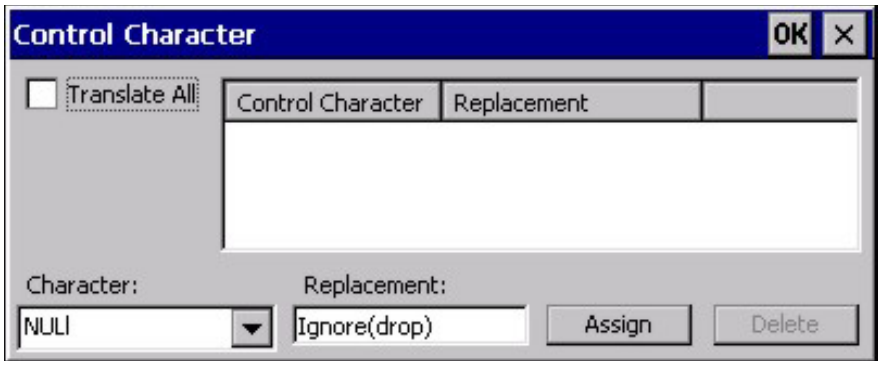


Figure 4-10 Barcode Tab – Ctrl Char Mapping

See "Hat Encoding" and "Decimal-Hexadecimal Chart" at the end of Appendix B "Technical Specifications".

Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Translate All	This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a keystroke equivalent is dropped.
Character	This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default Ignore (drop) in the Replacement edit control.

Replacement	The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button. For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a. The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.
List Box	The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.
Delete	This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Barcode – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard AIM or Symbol IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

These are called "custom" Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data. The dialog below allows the custom Code IDs to be configured.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if **Enable Code ID** is set to **AIM** or **Symbol**), or to replace the list of standard code IDs (if **Enable Code ID** is set to **Custom).**

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*

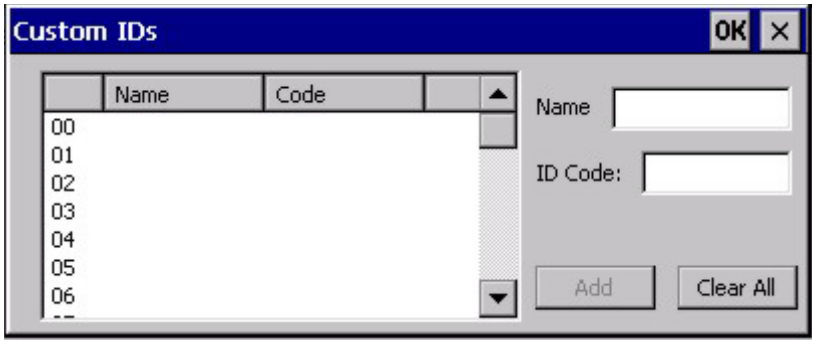


Figure 4-11 Barcode Tab – Custom Identifiers

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

Parameters

Name text box — Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the **Name** and **ID Code** may have the same value. **Name** is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box — ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both **Name** and **ID Code** must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

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

Control Code Replacement Examples

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

Barcode Processing Examples

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

	Symbology				
	All	EAN-128 (]C1)	EAN-13 (]E0)	Intrlv 2 of 5 (]IO)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

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

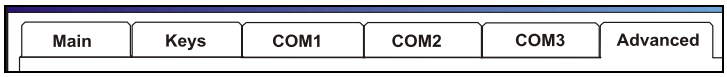
Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< ***rejected*** > *(too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< ***rejected*** > *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< ***rejected*** > *(disabled)*
Code-93	]G0444444	< ***rejected*** > *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< ***rejected*** > *(too short)*

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

Advanced

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

If your scanner applet has a "Barcode" tab instead of an "Advanced" tab, please see section titled "Barcode Manipulation" at the beginning of this chapter.



Factory Default Settings

Factory Default Settings	
Main	
Port 1	Internal
Port 2	Disabled
Power Port 1 while asleep	Disabled
Send key messages WEDGE	Enabled
Bluetooth	Disabled (Not supported)
Output enable	Disabled (dimmed)
Keys	
Left	Scan
Right	Enter
COM Ports (COM1- COM2 – COM3)	
Baud Rate	9600
Parity	None
Stop Bits	1
Data Bits	8
Advanced *or* **Barcode**	
Translate	Disabled
Strip Leading	0 characters
Strip Trailing	0 characters
Prefix	Disabled
Suffix	Disabled
Barcode	
Advanced Barcode Processing	Disabled

Notes:

- If the internal scanner has to be configured to operate at any communication settings other than 9600, N, 8, 1 and the MX3X 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.
- The MX3P does not have an integrated scanner or RFID capability.
- Bluetooth Manager, Bluetooth service or options are not available for all MX3X devices or in all MX3X software releases.

Main Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX3X devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

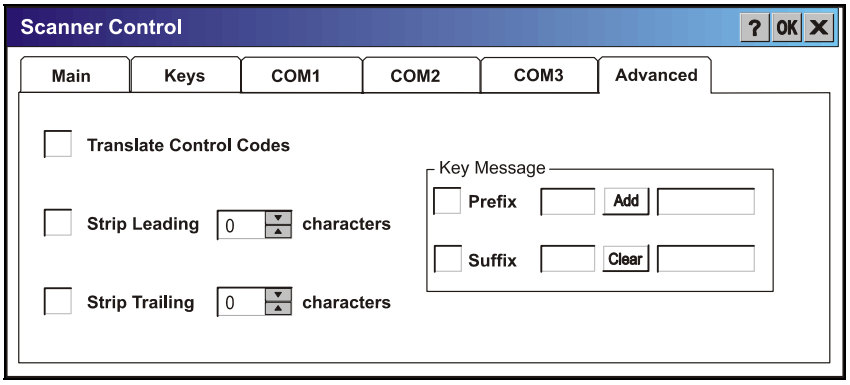


Figure 4-12 Advanced – Main Tab

Parameter	Default	Options
Port 1	Internal	Disabled, COM1, COM3, Internal, Cradle, Bluetooth, Output Enable.
Port 2	Disabled	Disabled, RFID Internal, COM3, Internal, Cradle, Bluetooth, Output Enable
Power Port 1 while Asleep	Disabled	Enabled, Disabled. If "Power Port 1 while asleep" is checked, whichever serial port is enabled as Port 1 will remain powered while the device is in Suspend, at the cost of reduced battery life. This allows a tethered scanner to wake the device by pressing the trigger on the scanner.
Send Key Messages	Enabled	Enabled, Disabled. 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".

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

The Scan buttons have no effect on tethered external scanners connected to the RS-232 connector on the endcap.

Keys Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX3X devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

Parameter	Default	Options
Left Scan Key	Scan	Disabled, Scan, Enter key, Tab key, Field Exit key, Virtual key, RFID (or RFID Read)
Right Scan Key	Enter key	Disabled, Scan, Enter key, Tab key, Field Exit key, Virtual key, RFID (or RFID Read)

- If there is no integrated scanner installed in the mobile device, the Left and Right Scan Keys default to Enter keys.
- On a 5250 device with an integrated scanner, the Left Scan key defaults to Scan and the Right Scan key defaults to Field Exit key.

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

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

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

Change a Virtual Key (F20 or F21) Value

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

Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

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

COM1, COM2, COM3 Tabs

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

COM	Default	Options
COM1	19200, 8 data bits, 1 stop bit, no parity Power on pin 9 (+5v) Enabled	Baud Rate – 115200 (115200 - RFID only), 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space
COM2	9600, 8 data bits, 1 stop bit, no parity Power on pin 9 (+5v) Disabled	Baud Rate – 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space
COM3	9600, 8 data bits, 1 stop bit, no parity Power on pin 9 (+5v) Disabled	Baud Rate – 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space

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

Advanced Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in MX3X devices. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

Translate Control Codes

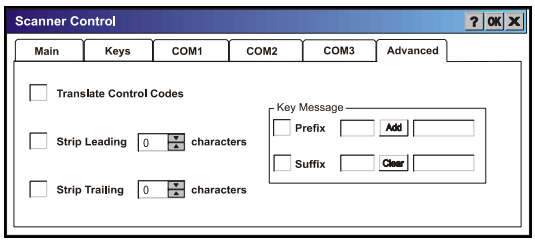


Figure 4-13 Advanced – Translate Control Codes

Note: If your Advanced tab scanner panel has four button choices, as shown above, then when the Prefix/Suffix button is tapped, CTRL codes are passed through in Block mode.

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

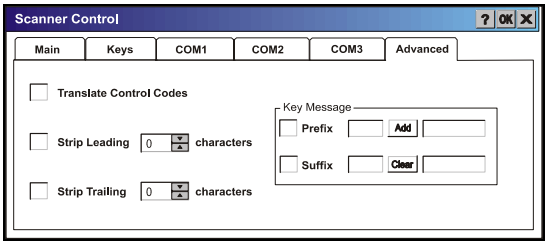


Figure 4-14 Advanced – Strip Leading/Trailing Characters

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 fetaures 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

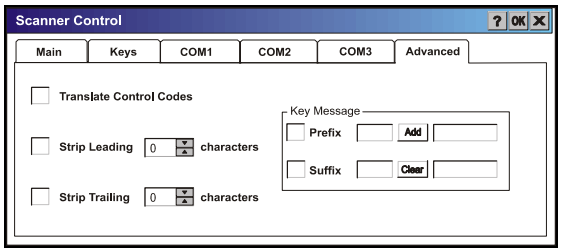


Figure 4-15 Advanced – Prefix/Suffix

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" at the end of Appendix B "Technical Specifications".

Barcode Tab

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

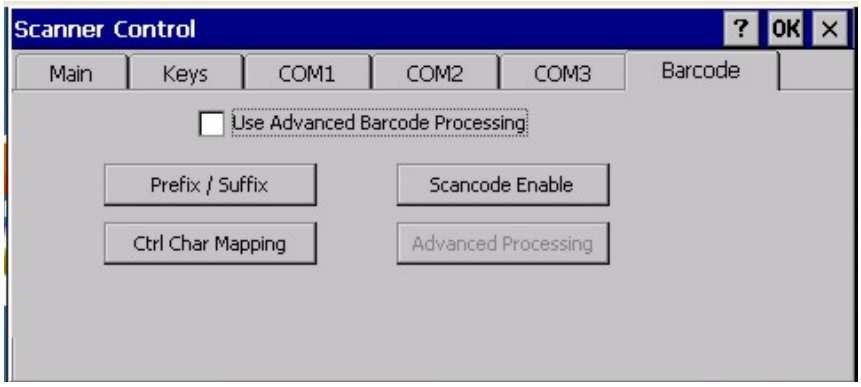


Figure 4-16 Barcode Tab

Prefix / Suffix

Note: Prefix / Suffix is only available when Use Advanced Barcode Processing is disabled.

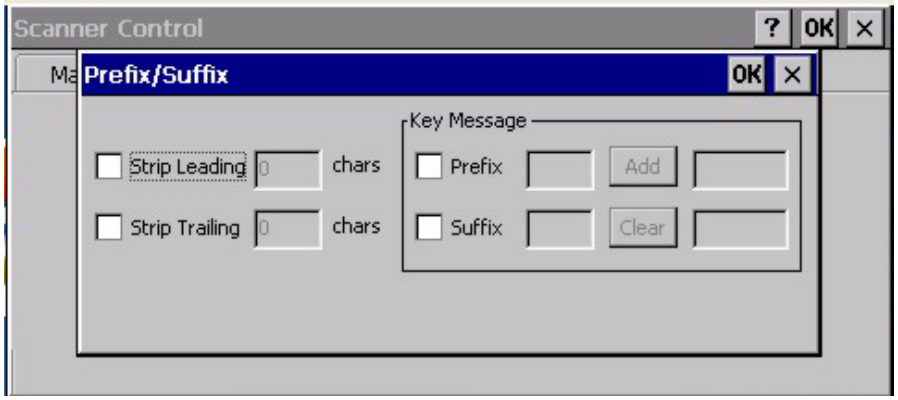


Figure 4-17 Barcode – Prefix / Suffix

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

Strip Leading / Strip Trailing Characters

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

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

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

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

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

Prefix / Suffix

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

The mode for Prefix/Suffix feature is determined by the "Send Key Messages (WEDGE)" setting in the Main tab. When checked (enabled), the prefix/suffix feature is in *Key Message mode*. Key message mode sends the prefix, barcode, and suffix to the application with the focus as keystrokes. In Key message mode all keys on the keypad can be entered.

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

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

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

Interaction between Strip Leading/Trailing and Prefix/Suffix Settings

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

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

   Group Separator is translated to 'GS'

   Strip Leading is set to 2

   In this case, the Group Separator is translated to 'GS' and then the 'GS' is stripped by the Strip Leading setting; rather than the Group Separator and 'A' being stripped.
3. If Translate All is enabled and replacements are assigned, the assigned replacements take precedence over the default one-to-one translation enabled by Translate all. For example if Translate All is enabled and Carriage Return is replaced by ^J, the value, 0x0d, in the barcode (prefix and suffix) are replaced with CTRL+Shift+J instead of CTRL+Shift+M keystrokes in Key Message mode.
4. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to 'Ignore (drop)' by the assigned replacements, it is discarded before the Translate All processing is performed and is therefore not translated.
5. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to text by the assigned replacements, the text is substituted for the control character. In this case, the control character would not be in the data processed by the Translate All feature.
6. If the application that is accessing the Barcode Wedge in Block mode, supports Hat encoded characters, like ^M, hat encoded characters can be assigned in the defined action and then interpreted by the receiving application by using the 'escape' format described above. The same is true for hex-encoded characters.

Ctrl Char Mapping

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

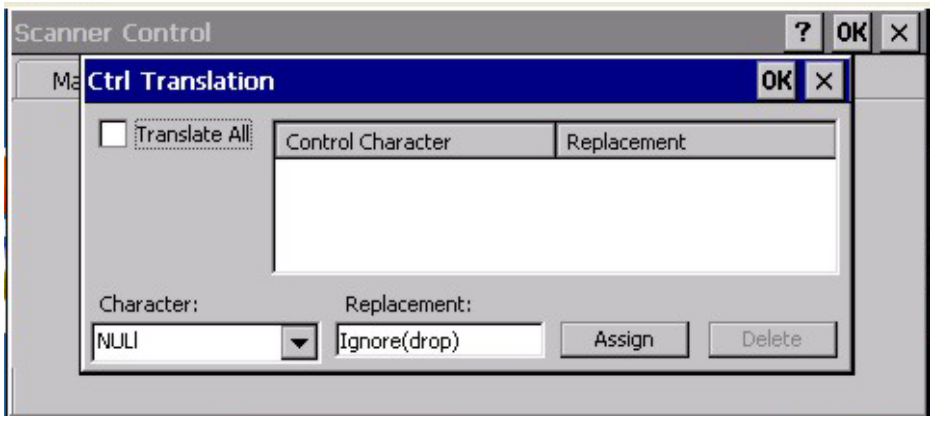


Figure 4-18 Barcode – Ctrl Translation

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

See "Hat Encoding" and "Decimal-Hexadecimal Chart" at the end of Appendix B "Technical Specifications".

Translate All

If "Translate All" is checked, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

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

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes in Key Message mode. If a control character is replaced by another control character, the replacement is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

Translate All	This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). It does not replace control characters in the prefix and suffix. The assignments provided by this enhancement allow the user to override the one-to-one translation provided by Translate All.

Character	This is a drop down combo box that contains the control character name. Refer to the table in “Assigned Replacements” for the list of control characters and their names. When a character name is selected from the combo box, the text ‘Ignore (drop)’ is shown and highlighted in the Replacement edit control. ‘Ignore (drop)’ is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types into the Replacement edit control, reselecting the character form Character combo box redisplays the ‘Ignore (drop)’ default in the Replacement edit control.
Replacement	The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character combo box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.
List Box	The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.
Delete	This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Scancode Enable

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

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

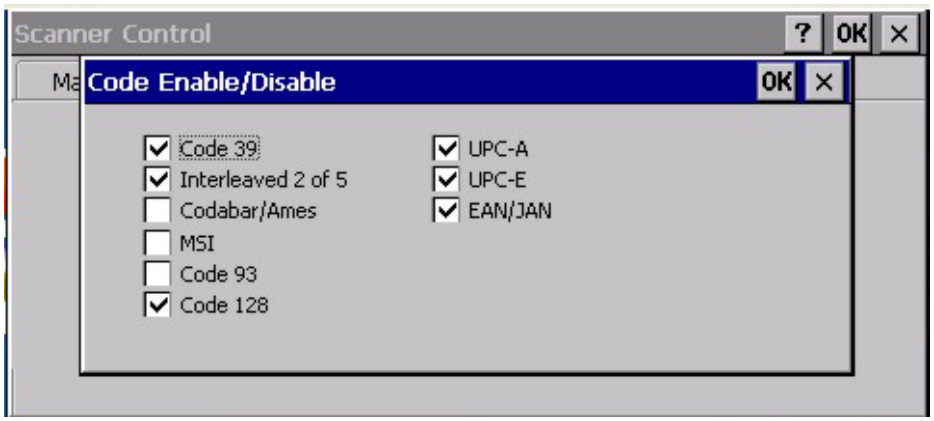


Figure 4-19 Barcode – Scancode Enable/Disable

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

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

Advanced Processing

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

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

See Also: The "Integrated Scanner Programming Guide", section titled "Data Options" for full details on AIM Code IDs and Symbol Code IDs.

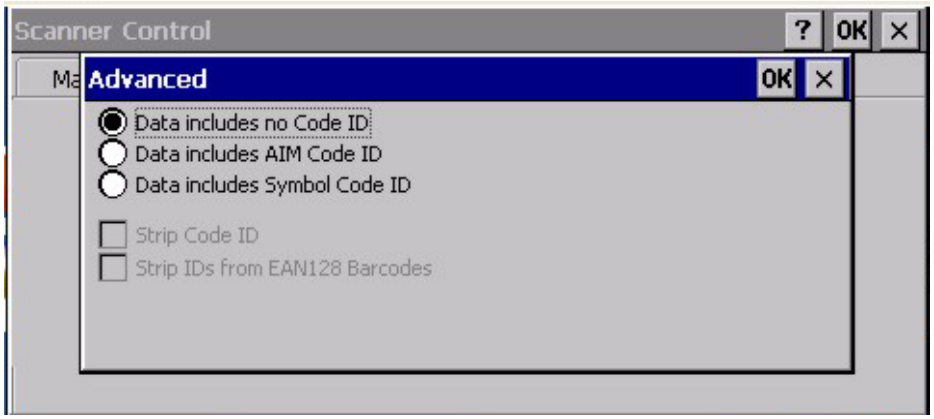


Figure 4-20 Barcode – Advanced Processing

No Code ID	Default. All symbology IDs are transmitted. This means that by default, all good scan barcodes are sent to the application just as they are received from the scanner, regardless of any possible symbology ID attached. The *Strip Code ID* radio button is unavailable when No Code ID is enabled.
AIM Code ID	Enabling the Strip Code ID checkbox ensures the 3-character AIM Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data inludes Symbol Code ID* if the AIM Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.
Symbol Code ID	Enabling Strip Code ID ensures the 1-character Symbol Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data includes AIM Code ID* if the Symbol Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.

Strip Code ID

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

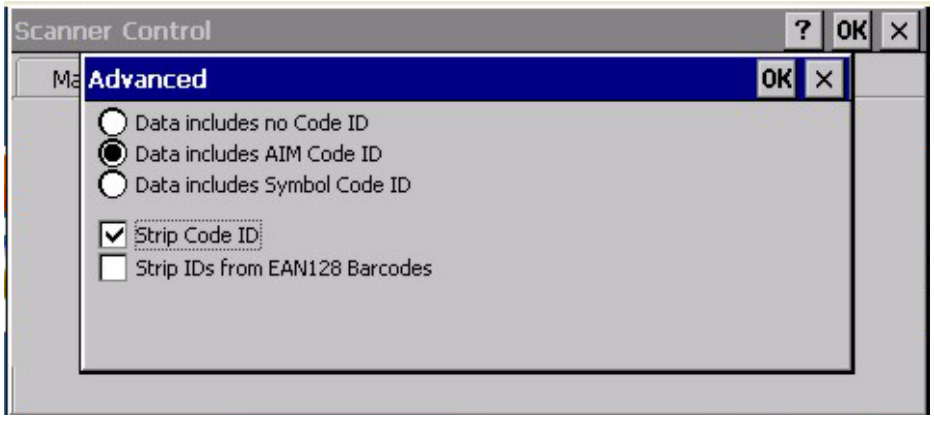


Figure 4-21 Barcode – Advanced Processing – Strip Code ID

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

Strip Identifiers from EAN128 Barcodes

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

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

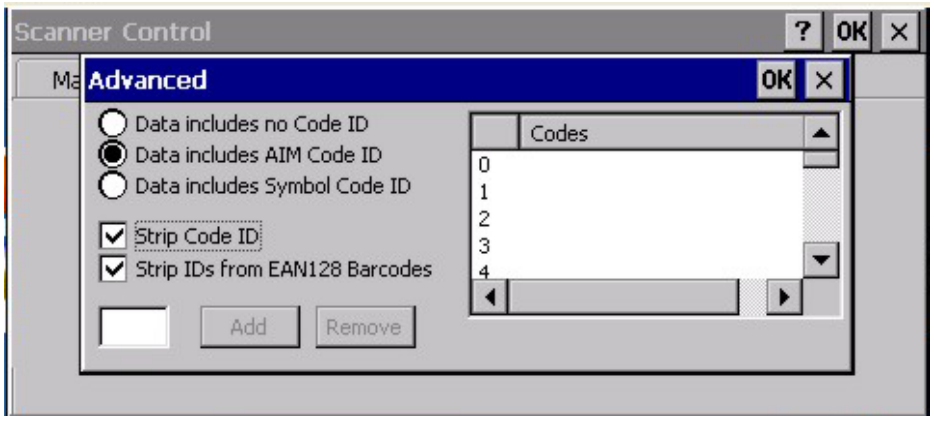


Figure 4-22 Barcode – Advanced Processing – EAN128 Barcodes

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

Adding Codes to the Match List for EAN128 Barcodes

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

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

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

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

Chapter 5 Wireless Network Configuration

Introduction

The MX3X mobile device offers a choice of Cisco, Symbol and Summit clients. The Summit client device is an 802.11g network card. The Cisco and Symbol client network cards are 802.11b clients. They can be configured for the security types listed below.

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

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

Security Options Supported	Type		
	Summit Client	Cisco Client	Symbol Client
None	Yes	Yes	Yes
EAP-FAST	Yes [4]	No	No
EAP-TLS	No*	Yes	No
LEAP	Yes	Yes	Yes
PEAP-GTC	Yes	Yes	No
PEAP-MSCHAP	Yes	Yes	No
WEP	Yes	Yes	Yes
WPA/LEAP	Yes	Yes	No
WPA-PSK	Yes	Yes	No

* Not available when this manual was published. Check with your LXE representative for current availability.

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys
- The Summit profile settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security option chosen.

	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for MX3X communication. It is available on the LXE Manuals CD and the LXE ServicePass website.
 Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
	It may be necessary to upgrade radio drivers in order to use certain Summit Client Utility (SCU) features described in this chapter. Please contact your LXE representative for details.

[4] EAP-FAST is supported only with automatic PAC provisioning.

Summit Client Configuration

The Summit client requires driver 1.2.1 SCU 1.2.4 or later. All MX3X's with a Summit wireless device ship with this software revision or greater. To identify the software version, tap the "About" icon in Start | Settings | Control Panel.

Summit Client Utility Icon

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

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

Summit Client Utility

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

Figure 5-1 Summit Client Utility

The **Main** tab provides information, admin login and active config (profile) selection.

Profile specific parameters are found on the **Config** 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 connection. *Diagnostics, 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** 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 that Wireless Zero Config application is enabled but the connection is inactive at this time (the MX3X 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 connect to your network. The Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

Select **ThirdPartyConfig** in the Active Config drop down list as the active profile. Warmboot the MX3X. The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, set up client and security settings. LXE does not recommend use of the Wireless Zero Configuration Utility for configuring the client device as it cannot be used to configure all supported security protocols.

To switch back to Summit client control, select any other profile in the SCU Active Config drop down list, except ThirdPartyConfig. Warmboot the MX3X. Wireless client control is passed to the SCU.

Main Tab

Factory Default Settings	
Admin Login	SUMMIT
Radio	Enabled
Active Config	Default

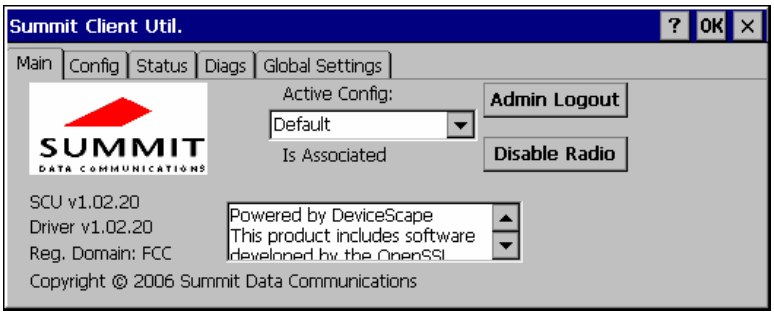


Figure 5-2 SCU – Main Tab

The Main tab displays information about the client device including:

- SCU (Summit Client Utility) version
- Driver version
- Regulatory Domain
- Copyright Info
- Active Config
- Status of the network device (Down, Associated, Authenticated, etc).

The **Active Config** (profile) can be switched without logging in to Administrator mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Administrator 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.

The **Admin Login** button provides access to editing client device parameters. Config and Global Settings may only be edited after entering the Admin Login password. The password is case-sensitive. Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Administrator Login

To login to Administrator mode, tap the Admin login button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the Admin Logout button, or a navigation button (X or OK), to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.

Figure 5-3 Admin Password Entry

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap OK. If the password is incorrect an error message is displayed.

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

The end user can:

- View the current parameter settings for the profiles on the Config tab.
- View the global parameter settings on the Global Settings tab.
- The current connection details on the Status tab.
- Radio status, software versions and regulatory domain on the Main tab.

After Admin login, the end user can also:

- Turn radio On/Off on the Main tab.
- Select active Config (Profile) on the Main tab.
- Create, edit, rename and delete profiles on the Config tab.
- Edit global parameters on the Global Setting tabs.
- Access additional troubleshooting features on the Diags tab.

Config Tab

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

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

Figure 5-4 SCU – Config Tab

When logged in as an Administrator (see "Administrator Login"), use the Config tab to manage profiles. When not logged in as an Administrator, the parameters can be viewed, and cannot be changed. The buttons on this tab are greyed out if the user is not logged in as an Administrator.

Buttons

Button	Function
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see "Config Parameters") and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
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.
WEP/PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: Unsaved Changes -- Newer versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the Config 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 Parameters

Parameter	Default	Explanation
Config	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Config or Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the network card connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking devices, e.g. Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 10mW or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the wireless network 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, or PEAP-GTC. *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, 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

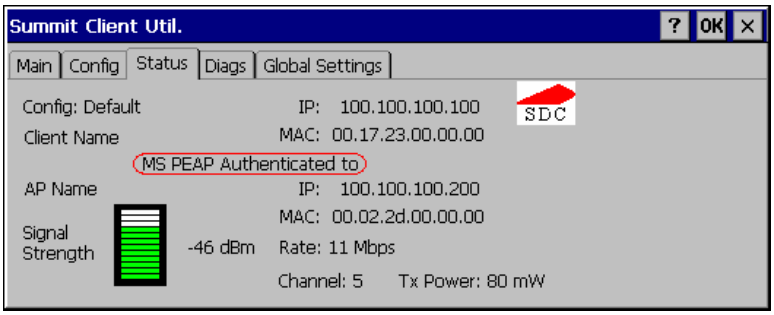


Figure 5-5 SCU – Status Tab

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

- The config profile being used
- The client name, IP address and MAC address
- The status of the network connection (down, associated, authenticated, etc.)
- The name, IP address and MAC address of the Access Point maintaining the connection to the network.
- Signal strength (changes with network activity).
- Channel currently being used for wireless traffic.
- Current transmit power in mW.
- Rate in Mbps.

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.

Administrator login is required for the (Re)connect button function.

Note: Diagnostics and Site Survey functions are not available in this release.

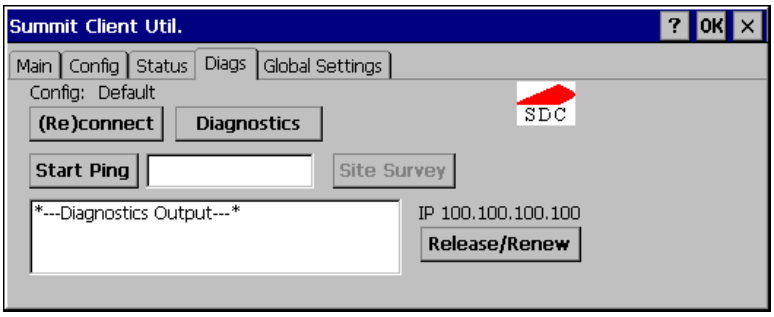


Figure 5-6 SCU – Diags Tab

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 Diagnotic Output text box on the lower part of the panel. Administrator login required for this function.
Diagnostics	Tapping this button begins an attempt to (re)connect to the wireless LAN. This option provides more data in the Diagnostics Output text box than the (Re)connect option. The data dump includes network card state, profile settings, global settings, and a list of access points by SSID broadcasting in the client's immediate area. *Not available in this release.*
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.
Release/Renew	Release the current IP address to obtain a new IP address. This option renews the IP address when applicable. Activity is logged in the Diagnostic Output text box. If a fixed IP address has been assigned to the client device, this is also noted in the Diagnostic Output box. The current IP address is displayed above the Release/Renew button.
Site Survey	*Not available in this release.*

Global Settings Tab

The parameters on the Global Settings panel can only be changed when an Administrator is logged in. No password is required to view the parameter settings.

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

Factory Default Settings	
RX Diversity	On-Start on Main
TX Diversity	On
Preamble	Auto
G Shorslot	Auto
Roam Trigger	-65 dBm
Roam Delta	10 dBm
Roam Period	10 sec.
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
Certs Path	System
CCX	Off
WMM	Off

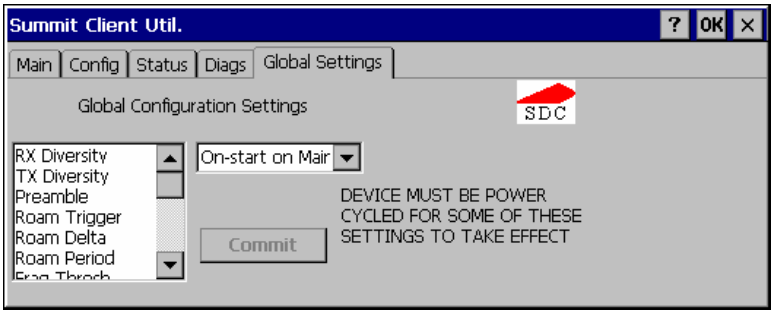


Figure 5-7 SCU – Global Settings Tab

Global Parameters

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.

Parameter	Default	Function
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).

Parameter	Default	Function
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).
Preamble	Auto	The type of client header, or preamble, for packets. Options are: Auto, Short, or Long.
G Short Slot	Auto	802.1x short slot timing mode. Options are: Auto, On, or Off. Note: The G Short Slot parameter has no effect on the Summit client device. This option is always set to On regardless of the parameter setting. 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 device looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, or -75 dBm.
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, or 35 dBm.
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, or 60 sec.
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.

Parameter	Default	Function
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 network card is not visible to the user when the network 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. Options are: none.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the 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. Options are: none. For example, when the valid certificate is stored as My Computer/System/*mycertificate.cer*, enter System in the Certs Path text box as the directory path.
CCX	Off	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: On, Off.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off.

Summit Wireless Security

Use the instructions in this section to complete the entries on the Config tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your System Administrator for complete information about your network and its wireless security requirements.

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

Default profile	LXE recommends editing the Default profile instead of creating new profiles. **Important**: Perform a soft reset (or Suspend/Resume) after changing parameters to save the changed parameters in the registry.
Switching profiles	Successfully connecting after switching from one profile to another may take up to 30 seconds from the moment the "Is not authenticated" or "Is not Associated" messages are displayed.
Adding, changing or renaming profiles	LXE recommends performing a Warmboot function (or Suspend/Resume) after tapping the Commit button.

Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP and PEAP/GTC

A sign-on screen is created by leaving the user name and password blank when configuring the credentials for LEAP, EAP-FAST, PEAP/MS-CHAP, PEAP/GTC. The sign-on screen is displayed upon each reboot function, and return from Suspend function, for the listed protocols.

Figure 5-8 Credential Sign-on Screen

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers two choices:

- The User name and Password may be entered on the Credentials screen. If this method is selected, anyone using the mobile device can access the network.
- The User name and Password are left blank on the Credentials screen. When this method is used and the mobile device attempts to connect to the network, a sign-on screen is displayed. The user must enter the User name and Password at that time to authenticate.

Enter the user name and password and tap OK.

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 for authentication.

No Security

Start the Summit Utility by tapping the Summit Client icon.

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

Tap the **Config** tab.

Figure 5-9 Summit Profile with No Security

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

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to None.

Tap the **Commit** button [5] to save the new profile configuration.

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

[5] LXE recommends performing a soft reset or Suspend/Resume function each time the Commit button is tapped.

WEP Keys

Please see your System Administrator for complete information about your network WEP key requirements.

To connect using WEP, use the following minimum required profile options..

- Auth Type = Open
- EAP Type = None
- Encryption = Manual WEP

Tap the **WEP/PSK** Keys button. The WEP Key Entry text entry box appears.

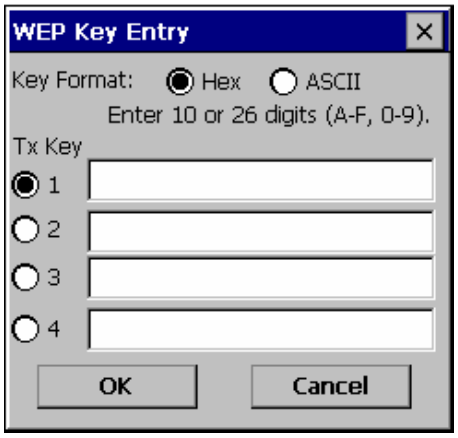


Figure 5-10 Summit WEP Keys

Enter the **WEP key**. If there are more than one set of keys, tap the radio button in front of the Key to be used.

WEP keys may be entered in Hex or ASCII format. For previous versions of the SCU, if the WEP key entry does not offer a choice between Hex and ASCII, the key must be in Hex (refer to the Hex Key Format segment that follows).

Once configured, tap **OK** then tap the **Commit** button. Ensure the correct Active Config is selected on the Main tab and warm boot. The SCU Main tab shows the device is associated after the radio connects to the network.

Hex Key Format

Valid keys are 10 (for 40 bit encryption) or 26 (for 128 bit encryption) hexadecimal characters (0-9, A-F). Enter the key(s) and tap **OK**.

ASCII Key Format

Valid keys are 5 (for 40 bit encryption) or 13 (for 128 bit encryption) alphanumeric characters. Enter the key(s) and tap **OK**.

LEAP w/o WPA Authentication

If the Cisco/CCX certified 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 Administrator **password** and tap OK.

Tap the **Config** tab.

Figure 5-11 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.

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.

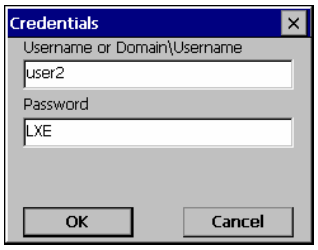


Figure 5-12 Summit LEAP Credentials

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** to connect using the new profile configuration.

Please see “WPA/LEAP Authentication” later in this section to configure the client for WPA LEAP.

Please see “Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP, and PEAP/GTC” earlier in this chapter if the username and password are left blank during setup.

EAP-FAST Authentication

Start the Summit Utility by tapping the Summit Client icon.

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

Tap the **Config** tab.

Figure 5-13 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.

The SCU only supports EAP-FAST with automatic PAC provisioning. The user credentials, whether entered on the saved credentials screen or the signon 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.

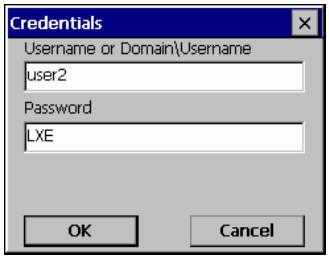


Figure 5-14 Summit EAP-FAST Credentials

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

Enter the **Password**, if desired. Tap **OK**. Tap the **Commit** button to save the new profile configuration.

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

Please see "Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP, and PEAP/GTC" earlier in this chapter if the username and password are left blank during setup.

PEAP/MSCHAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

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

Tap the **Config** tab.

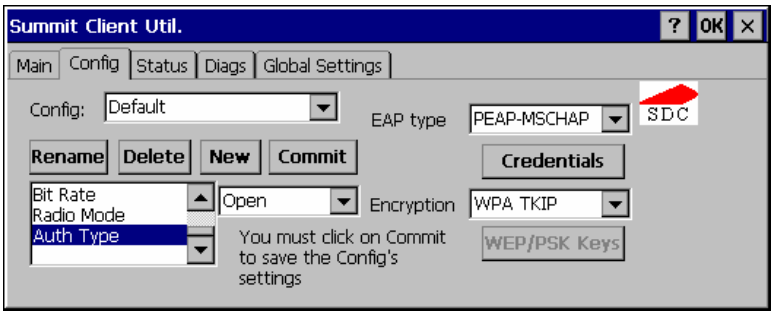


Figure 5-15 Summit Profile for PEAP/MSCHAP

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.

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.

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

Enter the **Password**, if desired.

Leave the CA Certificate Filename blank for now.

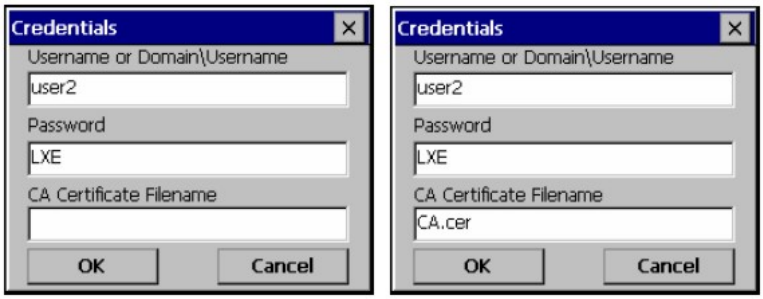


Figure 5-16 Summit PEAP/MSCHAP Credentials

Once successfully authenticated, copy the CA certificate into the \System directory of the device. Once the file is in the \System directory, enter the file name in the CA Certificate Filename text box.

Tap **OK** then tap the **Commit** button. Perform a warm reset function. [6]

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Please see "Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP, and PEAP/GTC" earlier in this chapter if the username and password are left blank during setup.

Note: The date must be properly set on the mobile device to authenticate a certificate.

[6] LXE recommends performing a soft reset or Suspend/Resume function each time the Commit button is tapped.

WPA/LEAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

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

Tap the **Config** tab.

Figure 5-17 Summit Profile with LEAP for WPA TKIP

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.

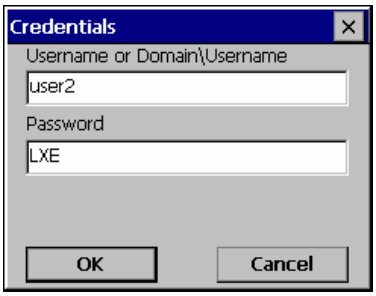


Figure 5-18 Summit WPA/LEAP Credentials

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** to connect using the new profile configuration.

Please see "LEAP w/o WPA" earlier in this section to configure the client for LEAP without WPA.

Please see "Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP, and PEAP/GTC" earlier in this chapter if the username and password are left blank during setup.

WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

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

Tap the **Config** tab.

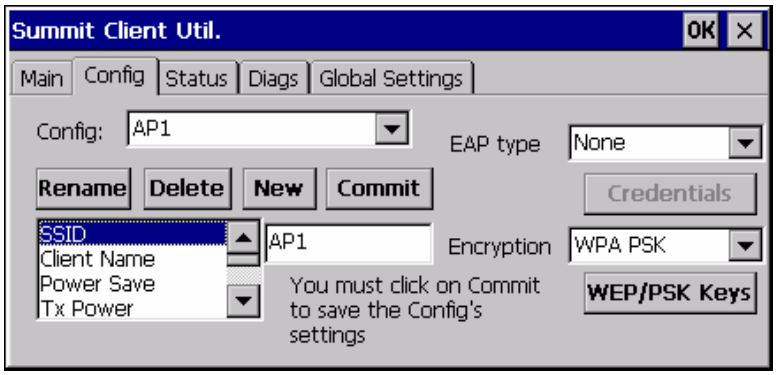


Figure 5-19 Summit Profile with WPA/PSK Encryption

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.

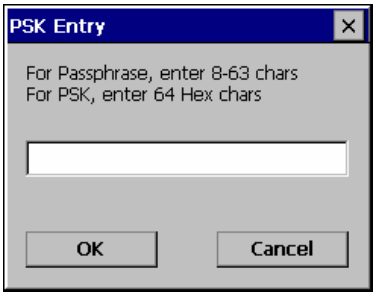


Figure 5-20 Summit PSK Entry

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** to connect using the new profile configuration.

Tap the **Main** tab. The screen shows the “WPA PSK” Active Config is **Associated** after the client connects to the network.

PEAP/GTC Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the main panel. Enter the Administrator **password** and tap OK.

Tap the **Config** tab.

Figure 5-21 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.

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.

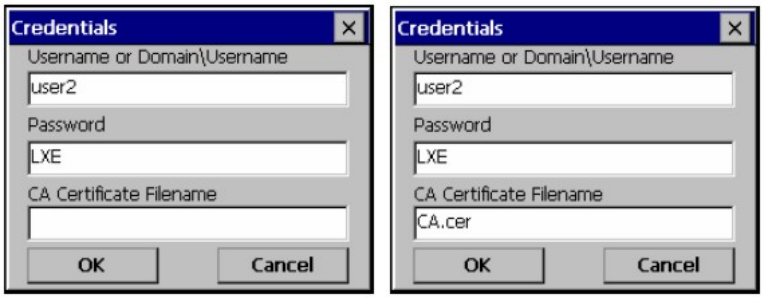


Figure 5-22 PEAP/GTC Credentials

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

Enter the **Password**, if desired. Leave the CA Certificate Filename blank for now.

Tap **OK**. Tap **Commit**.

Once successfully authenticated, copy the CA certificate into the System directory of the device. Once the certificate file is in the System directory, enter the filename in **CA Certificate Filename** on the popup Credentials data entry box.

Tap **OK**. Tap the **Commit** button to save the new profile configuration.

Perform a **Warm Reset** function to connect using the new profile configuration.

Please see "Sign-on Screen for LEAP, EAP-FAST, PEAP/MS-CHAP, and PEAP/GTC" earlier in this chapter if the username and password are left blank during setup.

Cisco Client Configuration

Prerequisites

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

Aironet Client Utility (ACU)

Access: Start | Aironet Client Utility *or* ACU Icon on Desktop

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards. Cisco options are available on the MX3X and MX3-RFID devices.

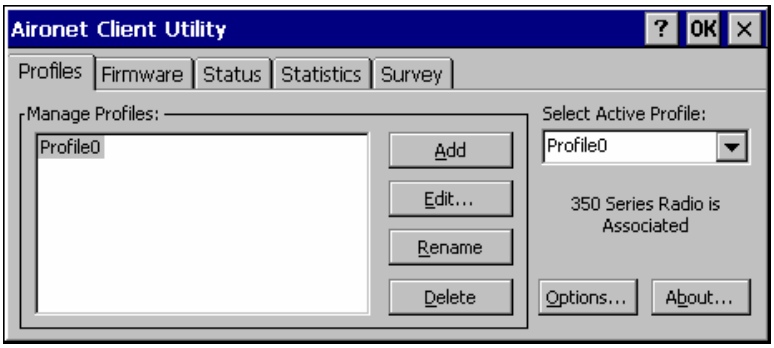


Figure 5-23 Cisco Aironet Client Utility

Note: To configure WPA, please see "Cisco Configuration", later in this chapter.

Profiles Tab	See the following "Profiles Tab" section for default profile parameter settings..
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.

Profile Parameters

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.

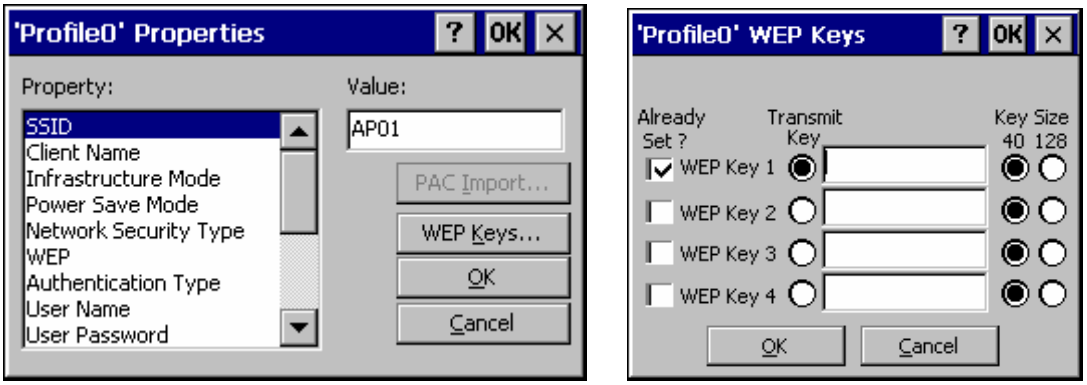


Figure 5-24 Cisco Profile Properties Screen

Tap the **WEP Keys** button to enter WEP information. If a key is already entered, the "Already set?" checkbox is checked. The previously entered key value is not displayed for security.

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, please tap the "About" icon in the Control Panel.

	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for Cisco client communication.

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

System Requirements

To support Wi-Fi Protected Access (WPA), the mobile device must be equipped as follows:

- Cisco 350 network card with driver release 2.60 (or later).

The LXE MX3X supports WPA and all authentications. The Microsoft supplicant and Cisco supplicants are used separately or together to provide support for the different authentications.

Most of the configuration is done with the Microsoft Wireless Configuration tool.

WPA/LEAP requires the Cisco supplicant and Cisco ACU configuration tool.

Installing Client Device Drivers

Which version of the Cisco client driver should be installed depends on which authentication protocol is to be configured.

- Cisco PEAP should not be installed if using PEAP/MSCHAP.
- Cisco PEAP must be installed if using PEAP/GTC.
- For all other authentications (LEAP, EAP-TLS, WPA-PSK) it does not matter if Cisco PEAP is installed or not.

To determine if Cisco PEAP is installed or to change the installation, refer to the instructions in the following sections.

Checking for the Cisco PEAP Supplicant

With a Cisco client installed, open the Wireless network properties as described in "Cisco Configuration", later in this section. With the Authentication tab selected check the text in the EAP type drop down box. Refer to the following figures to determine if Cisco PEAP is installed.

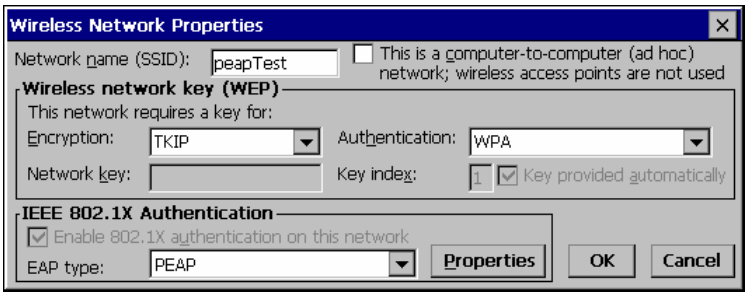


Figure 5-25 No Cisco PEAP

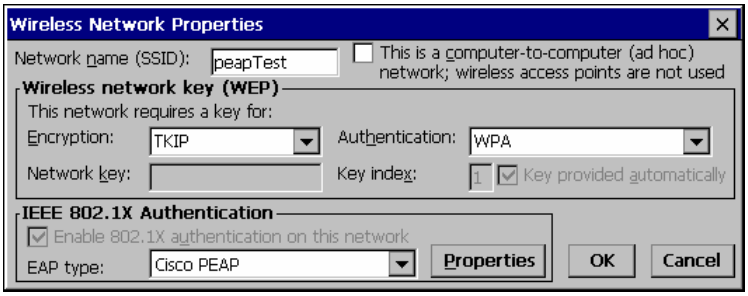


Figure 5-26 Cisco PEAP Installed

If the Cisco installation is correct, continue with the configuration. If it is not correct, follow the procedures below.

Note: Instructions are also included in the README file located in the \SYSTEM folder.

There are two Cisco CAB files in the \SYSTEM folder of the MX3X. The default files are:

CISCO.CAB CISCOPEAP.CAB

The default CISCO.CAB file provides for all authentications except Cisco PEAP. When the default CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the figure labeled "No Cisco PEAP", above.

If Cisco PEAP is desired:

1. Rename the CISCO.CAB file to CISCOMSCHAP.CAB.
2. Rename the CISCOPEAP.CAB file to CISCO.CAB.
3. Coldboot the mobile device to install the new driver with the registry.

The renamed CISCO.CAB file provides for Cisco PEAP and PEAP/GTC authentications. When the renamed CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the previous figure labeled "Cisco PEAP Installed".

If it becomes necessary to switch to a different authentication than Cisco PEAP or PEAP/GTC,

1. Rename the CISCO.CAB file to CISCOPEAP.CAB.
2. Rename the CISCOMSCHAP.CAB file to CISCO.CAB
3. Coldboot the mobile device to install the new driver with the registry.

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.

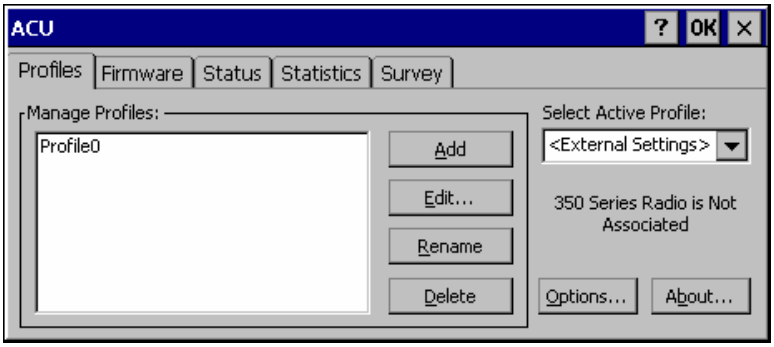


Figure 5-27 Cisco ACU Profile Selection

From the **Select Active Profile** pull down list, select <External Settings>.

Tap **OK** and warmboot.

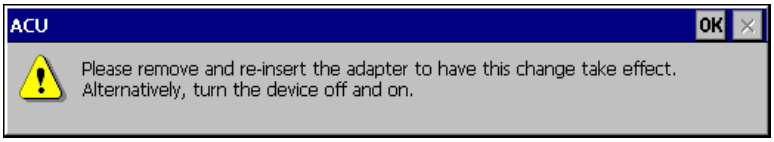


Figure 5-28 Cisco ACU Reboot Message

After booting up, the Microsoft Zero Config tool should start. If it does not, start configuring the wireless connection by tapping the icon on the task bar shown in below.

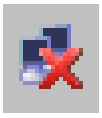


Figure 5-29 Microsoft Wireless Connection Icon

The Wireless Network Connection screen appears.

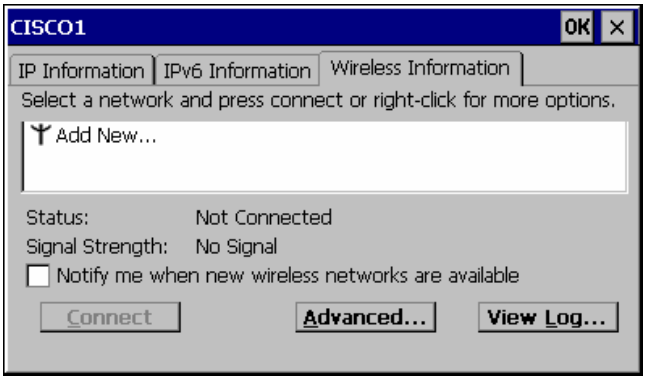


Figure 5-30 Wireless Information Screen

Make sure the "Notify me when new wireless networks are available" box is *not* checked..

Tap the **Advanced**… button.

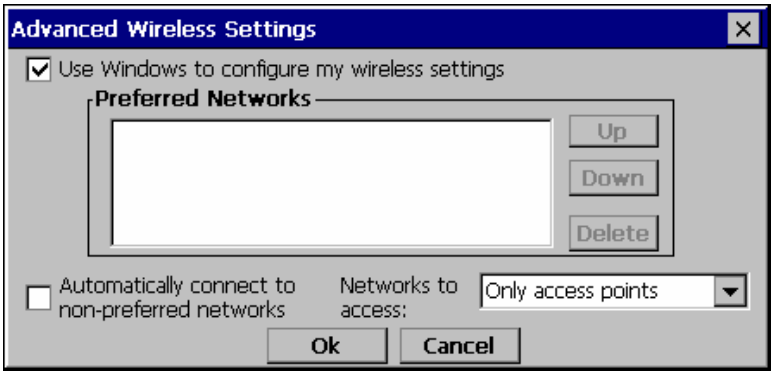


Figure 5-31 Advanced Wireless Settings

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.

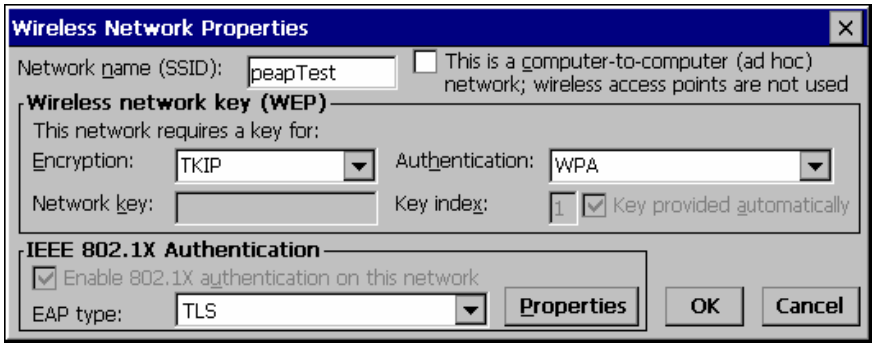


Figure 5-32 Wireless Network Properties

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 Client Device Drivers", earlier in this chapter, for more information.

Configuring the PEAP/MS-CHAP Supplicant

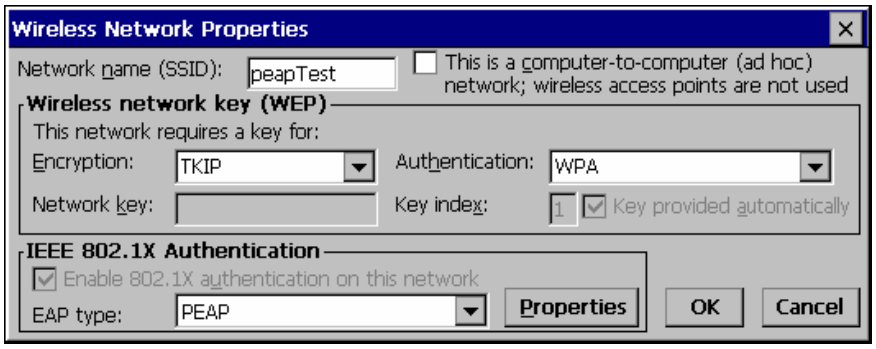


Figure 5-33 PEAP/MSCHAP Wireless Network Properties

With the client parameters configured set the **EAP type** to PEAP as shown above.

If the EAP type box text is not exactly as shown see "Installing Client Device Drivers" earlier in this chapter, to change the wireless CAB file.

Tap the **Properties** button.

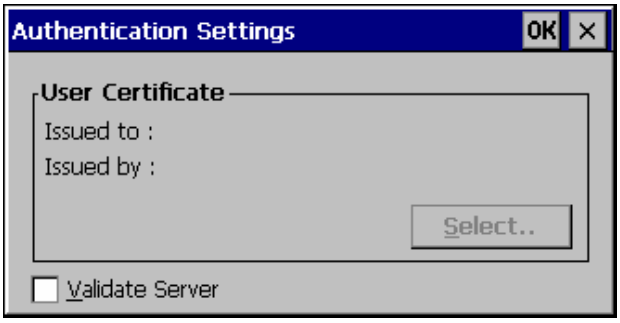


Figure 5-34 Authentication Settings

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.

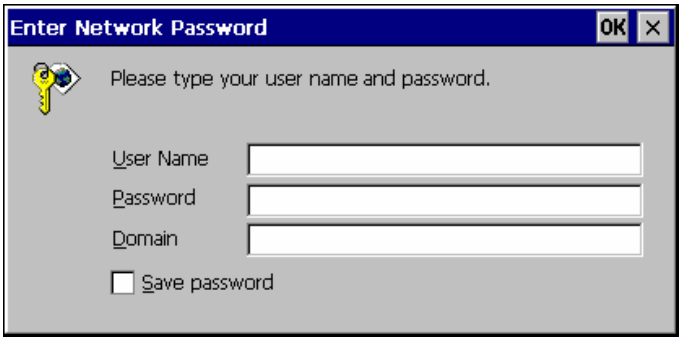


Figure 5-35 Wireless Network Login

Once authenticated, tap the **IP Information** tab.

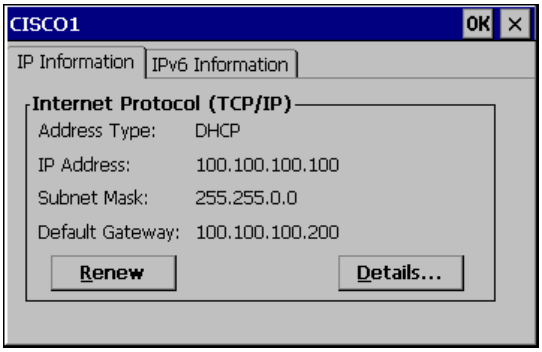


Figure 5-36 IP Information Tab

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", later in this chapter.

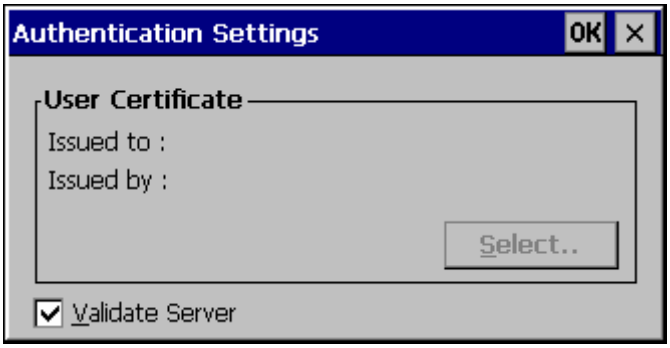


Figure 5-37 Authentication Settings, Validate Server

Navigate to the Wireless Network Properties configuration screen.

Tap the **Properties** button.

Check “Validate server” .

Tap **OK** to dismiss the configuration boxes.

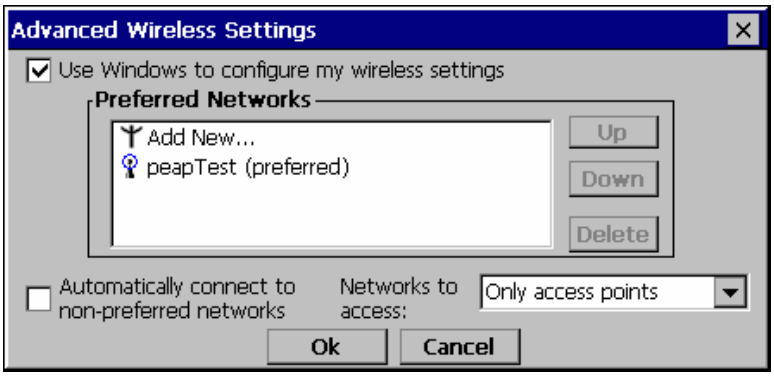


Figure 5-38 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Tap the IP Information tab and make sure there is a valid IP address as shown in the figure labeled “IP Information Tab”, earlier in this chapter.

PEAP/GTC Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/GTC protocol.

Configuring the PEAP/GTC Supplicant

With the client parameters configured set the EAP type to Cisco PEAP as shown below.

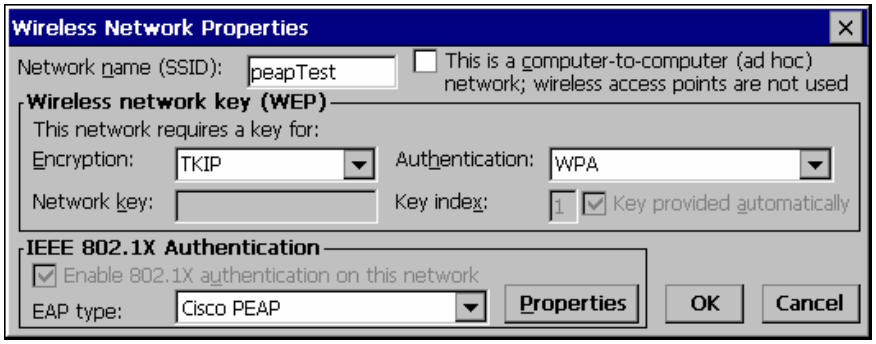


Figure 5-39 PEAP/GTC Wireless Network Properties

If the EAP type box text is not exactly as shown see “Installing Client Device Drivers”, earlier in this chapter, to change the client CAB file.

Click the **Properties** button.

Figure 5-40 PEAP Properties

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, return to this screen and validate the server certificate as shown later in this section.

Check the **Always try to resume secure session** box.

Note: This box must be checked for the LXE device to roam from one AP to another AP.

Tap the **OK** button.

The login screen appears for logging into the wireless network.

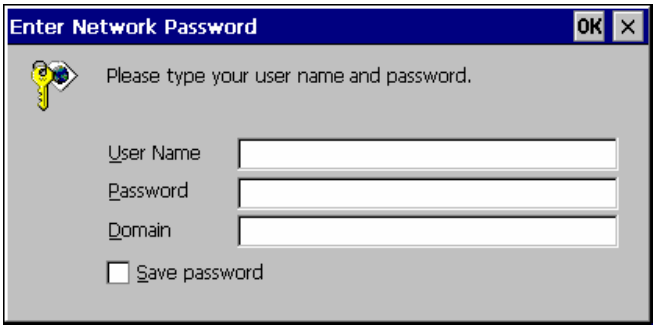


Figure 5-41 Login Screen

Enter valid user credentials.

Once authenticated tap the **IP Information** tab

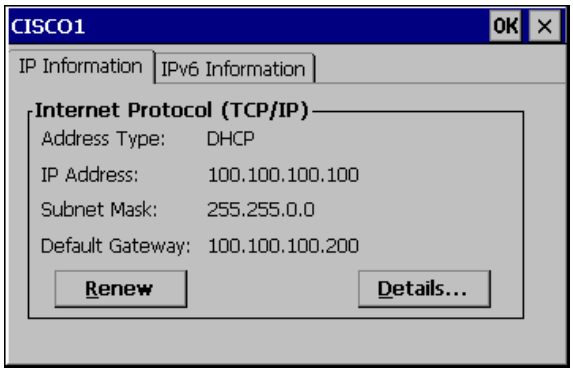


Figure 5-42 IP Information Tab

The .NET device displays the IP address given by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see "Root Certificates", earlier in this chapter.

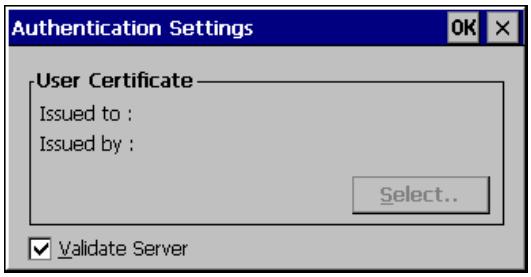


Figure 5-43 Authentication Settings, Validate Server

Navigate to the **Wireless Network Properties** configuration screen.

Tap the **Properties** button.

Check **Validate server** .

Tap **OK** to dismiss the configuration boxes.

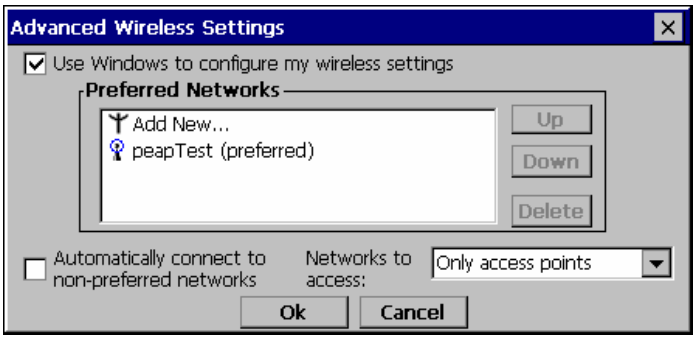


Figure 5-44 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Tap the IP Information tab and make sure there is a valid IP address as shown in the figure labeled "IP Information Tab", earlier in this chapter.

WPA/LEAP

LEAP is a Cisco proprietary authentication protocol and is not supported by the Microsoft supplicant. To configure the mobile device for WPA/LEAP, use the Cisco ACU installed during normal installation of the Cisco client driver.

Cisco ACU

Start the Cisco ACU by tapping the icon on the desktop or navigate to **Start | Programs | Cisco | ACU**.

Tap the Profile tab.

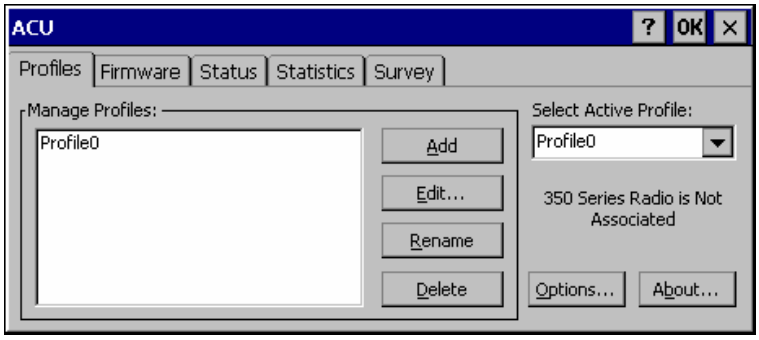


Figure 5-45 WPA/LEAP using ACU Profile Tab

Tap the **Rename** button.

Name the profile.

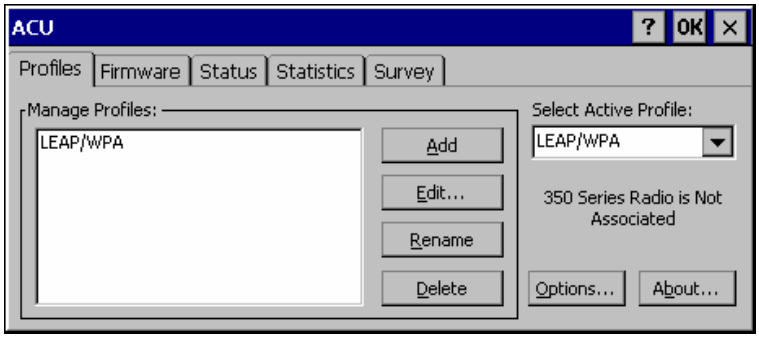


Figure 5-46 Renaming Profile

Tap the **Edit** . . . button.

The profile properties screen is displayed.

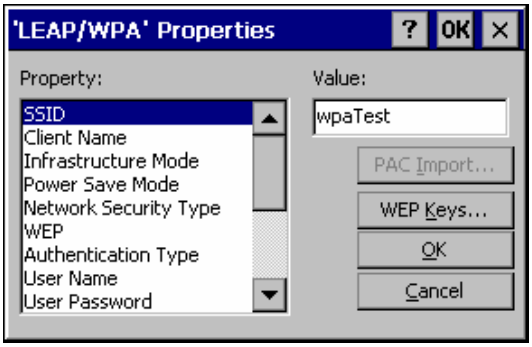


Figure 5-47 Profile Properties Screen

Enter the **SSID** and **Client Name** in the correct fields.

Set the **Network Security Type** to LEAP(WPA).

Tap the **OK** button.

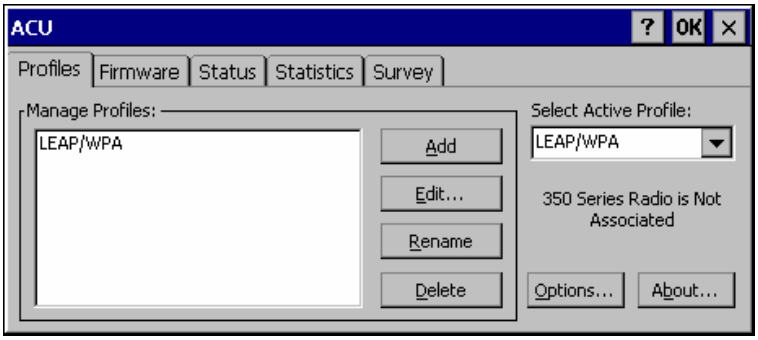


Figure 5-48 Select Profile

Use the drop down box to choose the profile just configured.

Tap **OK**.

The mobile device associates and displays the sign on screen.

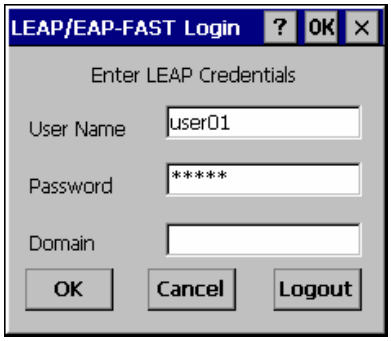


Figure 5-49 Login Screen

Tap the **Status** tab to display status.

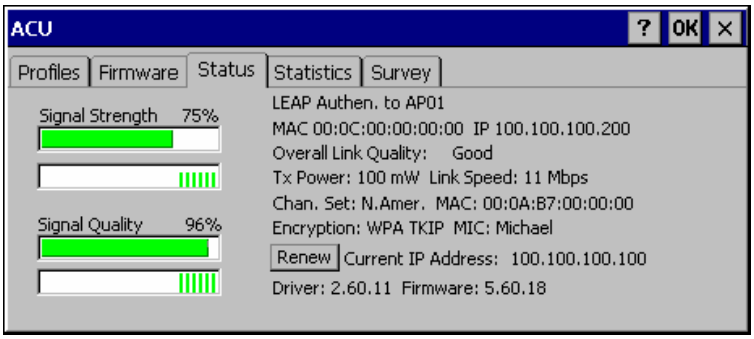


Figure 5-50 ACU Status Tab

EAP-TLS Authentication Configuration

To authenticate using the EAP-TLS protocol you need a user certificate file and a private key file. Once you have the user certificate files run the certificate installer from the Microsoft control panel. For EAP-TLS it does not matter which Cisco cab file is installed.

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

User Certificate

To check if a user certificate is installed navigate to **Start | Control Panel | Certificates**.

Set the drop down box to “My Certificates” as shown below.

The correct user certificate should be shown in the right pane.

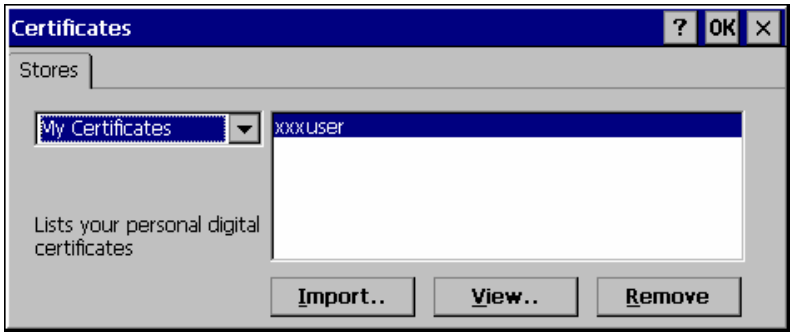


Figure 5-51 Certificate Stores

Tap the View . . . button.

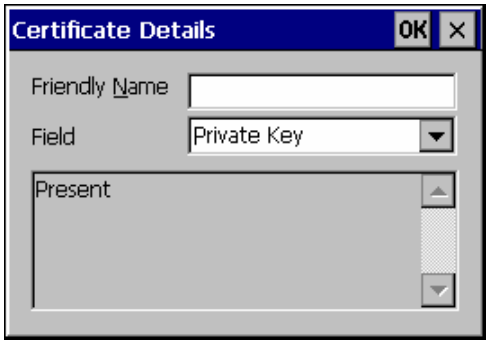


Figure 5-52 View Certificate Details

Set the **Field** to Private Key.

Make sure the private key is Present.

If it is not present, install the private key file.

If there is no user certificate refer to “User Certificates”, earlier in this chapter, to acquire a user certificate and private key file.

Setting EAP/TLS Parameters

With the client parameters configured set the EAP type to TLS as shown.

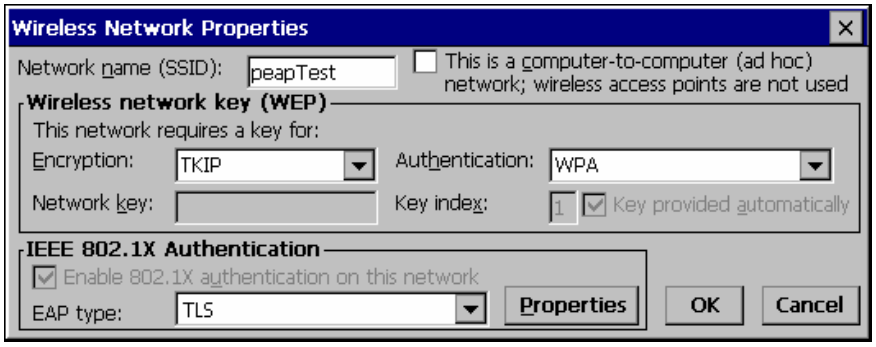


Figure 5-53 EAP/TLS Configuration

Tap the **Properties** button.

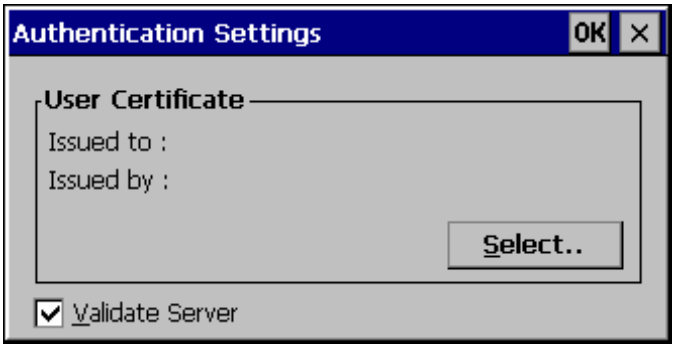


Figure 5-54 Authentication Settings

Tap the **Select** button to choose the user certificate.

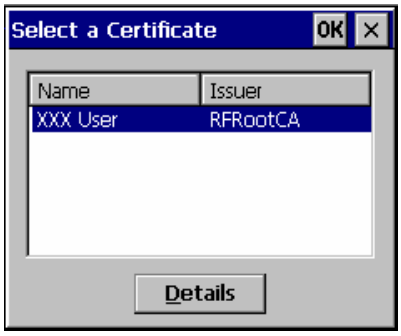


Figure 5-55 Select Certificate

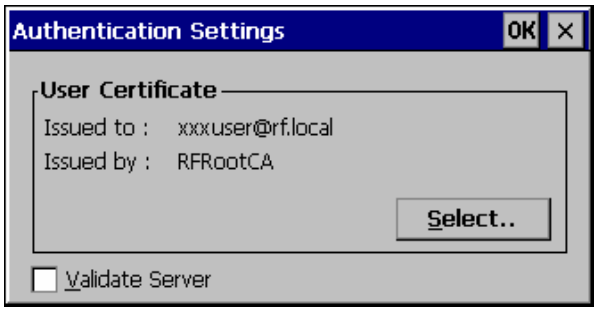


Figure 5-56 Authentication Settings, Certificate Details

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 device 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.

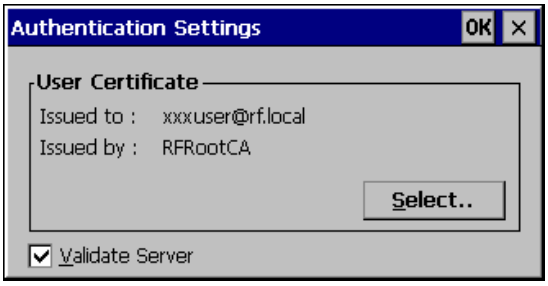


Figure 5-57 Validate Server

Tap OK to dismiss the configuration boxes.

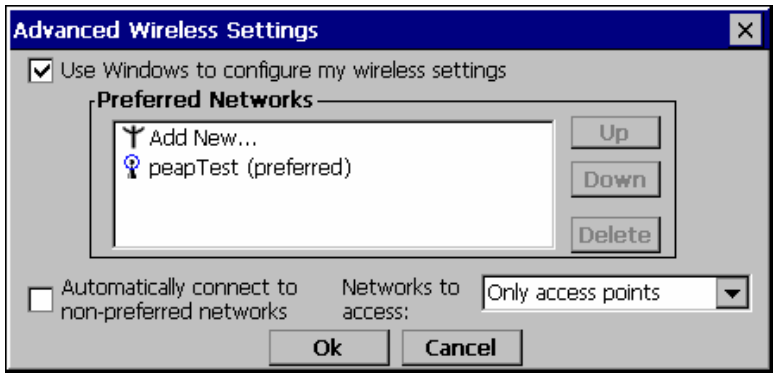


Figure 5-58 SSID Authenticated

Once the authentication completes the status changes to show the mobile device has authenticated to <SSID> as shown above.

WPA PSK Configuration

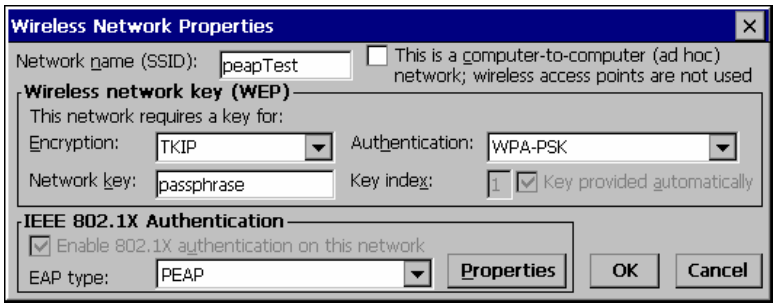


Figure 5-59 WPA PSK Configuration

Configure the Wireless Network Settings as described in "Wireless Security", earlier in this chapter.

Change the Network Authentication to **WPA-PSK**.

Enter an ASCII **network key** in the text field. Hex keys do not work in the Microsoft Zero Config utility at this time.

There is no server authentication when using WPA-PSK.

Tap the OK button to complete the configuration.

Symbol Client Configuration

Prerequisites

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

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards unless noted otherwise. Symbol options are available on an MX3X device only.

Access: Tap the Network Connected Icon in the Status Bar

Profile Parameters Menu

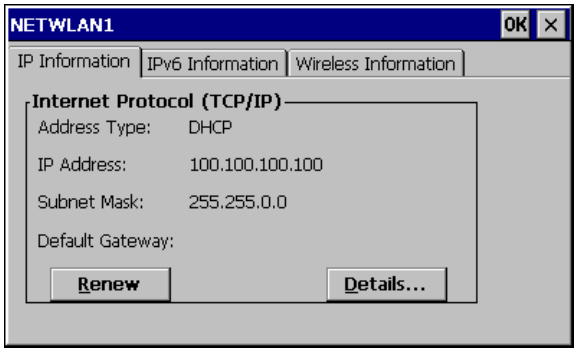


Figure 5-60 Symbol NETWLAN Screen

IP Information Tab	After the IP Address has been assigned to the mobile device, tap the **Renew** button to renew the IP address if necessary. Tap the **Details** button to view the Network Connection details.
IPv6 Information Tab	This is the TCP/IPv6 information screen. The contents cannot be edited by the user. **Configuring IPv6**: By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up. To disable IPv6, run \Windows\ipv6Disable.reg and perform a warmboot. To enable IPv6, run \Windows\ipv6Enable.reg and perform a warmboot. *Note: These utilities affect the behavior of the IPv6 on warmboot. After a coldboot, IPv6 is enabled.*
Wireless Information Tab	Setup Symbol client connection parameters: Encryption, authentication, WEP, WPA, EAP, etc.

Wireless Information Tab

Factory Default Settings	
Wireless Information	
Notify when new networks available	Enabled
Advanced Button	
Use Windows to configure wireless settings	Enabled
Automatically connect to non-preferred networks	Disabled
Networks to access (Only APs, Only comp-to-comp)	All available
Encryption (WEP, TKIP)	WEP
Authentication (WPA, Open, Shared, WPA-PSK)	WPA
Ad hoc network	Disabled
Key provided automatically	Enabled
Enable 802.1X authentication	Enabled
EAP Type (MDF-Challenge, PEAP, TLS)	TLS

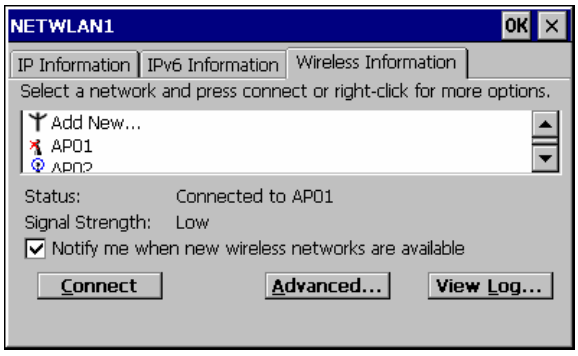


Figure 5-61 Symbol Wireless Information Tab

View Log

Displays the logon/connection data for the current network connection.

Add a new connection

Select **Add New**. Enter the ESSID in the **Network Name** text box.

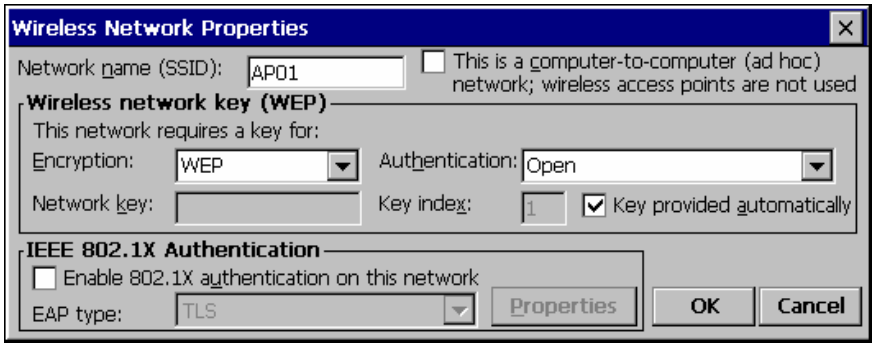


Figure 5-62 Symbol Wireless Network Properties

Disable WEP

- If WEP is to be disabled, tap the down arrow in the **Authentication** drop down box. Select **Open**.
- Tap the down arrow in the **Encryption** drop down box. Tap **Disabled** and WEP is disabled.
- Tap the **OK** button to return to the **Wireless Information** tab.

Enable WEP

- Tap the down arrow in the **Authentication** drop down box.
- Tap the **WEP Authentication** protocol.
- If the key is provided automatically by your network, check the "**Key provided automatically**" checkbox.
- If you wish to enter your Authentication key, uncheck the "**Key provided automatically**" checkbox and enter the Network Key in the **Network Key** text box.
- Tap the **OK** button to return to the **Wireless Information** tab.

Continue

Tap the **Advanced** … button. Make sure there is a checkmark in the "**Use Windows to configure my wireless settings**" checkbox. Make sure there is ***no*** checkmark in the "**Automatically connect to non-preferred networks**" checkbox. Tap the **Connect** button.

Tap **OK** to return to the **Wireless Information** tab.

Tap the **Connect** button.

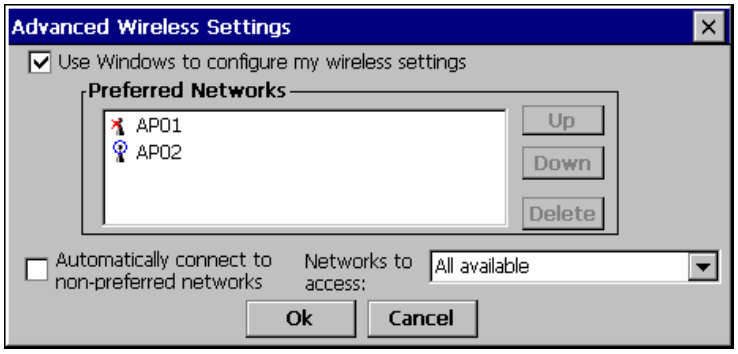


Figure 5-63 Symbol Advanced Wireless Settings

To access NETWLAN1 Properties again, tap the **Network Connected icon** in the Toolbar.

Select a User Certificate

1. Select **Wireless Information** Tab
2. Select a network by doubletapping the network name.
3. In the IEEE 802.1X Authentication box, enable **802.1X** authentication
4. Select an **EAP type.**
5. Tap the **Properties** button. Validate Server is enabled by default.
6. At the Authentication Settings display, tap the **Select** button to choose a User Certificate.

Certificates

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

Root Certificates

Generating a Root CA Certificate

Please refer to the “LXE Security Primer” for more information on obtaining and installing root certificates.

The easiest way to get the root CA certificate is to use a browser on a desktop PC to navigate to the CA (Certificate Authority). To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv

Sign into the CA with any valid username and password.

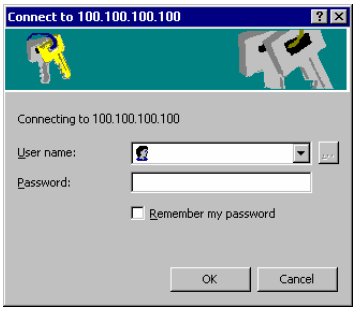


Figure 5-64 Logon to Certificate Authority

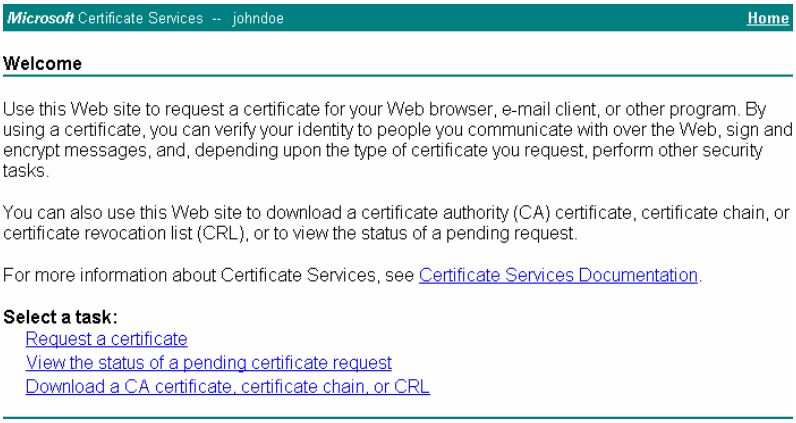


Figure 5-65 Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** task link.

Make sure the correct root **CA certificate** is selected in the list box.

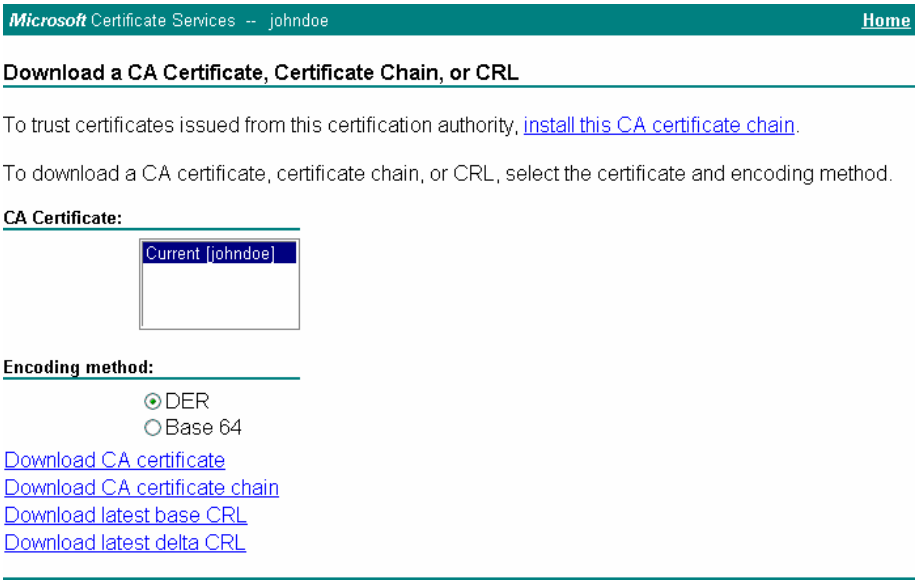


Figure 5-66 Download CA Certificate Screen

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.

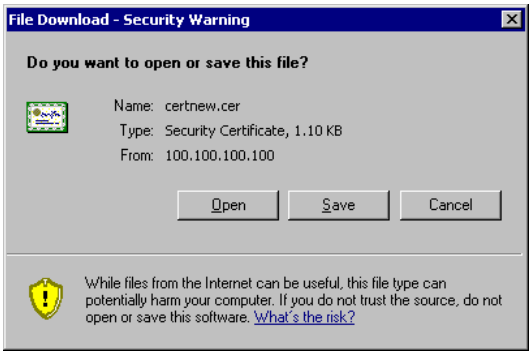


Figure 5-67 Download CA Certificate Screen

Click the **Save** button and save the certificate to the desktop PC. Keep track of the name and location of the certificate as the certificate file name and file location is required in later steps.

Installing a Root CA Certificate on the Mobile Device

Copy the certificate file from the desktop PC to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Figure 5-68 Certificates

Tap the "**Import**" button.

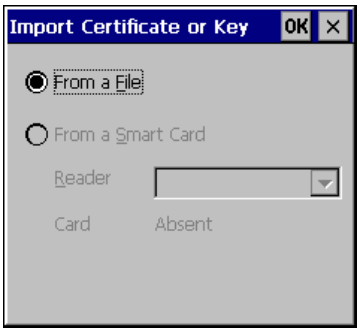


Figure 5-69 Import Certificate

Make sure "**From a File**" is selected and tap OK.

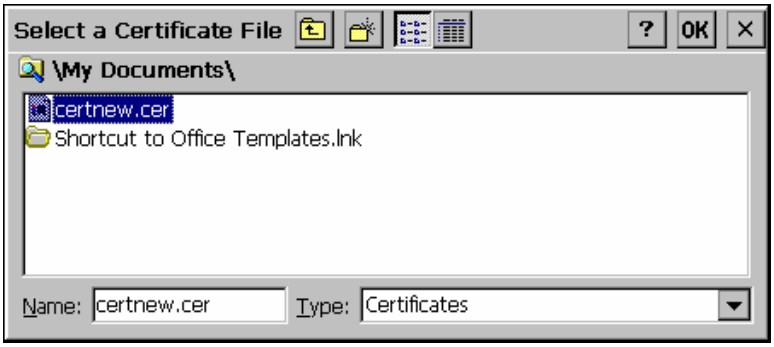


Figure 5-70 Browsing to Certificate Location

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

Figure 5-71 Certificate Import Confirmation

Tap **Yes** to import the certificate.

Once the certificate is installed, return to the proper authentication section, described later in this chapter.

User Certificates

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

Generating a User Certificate for the MX3X

Please refer to the "LXE Security Primer" for more information on obtaining and installing user certificates.

The easiest way to get the user certificate is to use a browser on a PC to navigate to the CA. To request the user certificate, open a browser to

http://<CA IP address>/certsrv

Sign into the CA with the username and password of the person who will be logging into the mobile device.

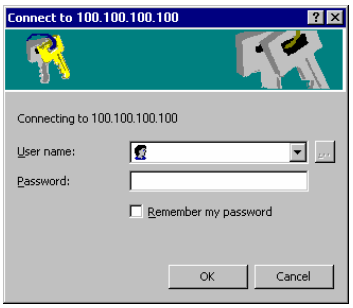


Figure 5-72 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. CE devices such as the MX3X require the private key to be saved as a separate file rather than including the private key in the user certificate.

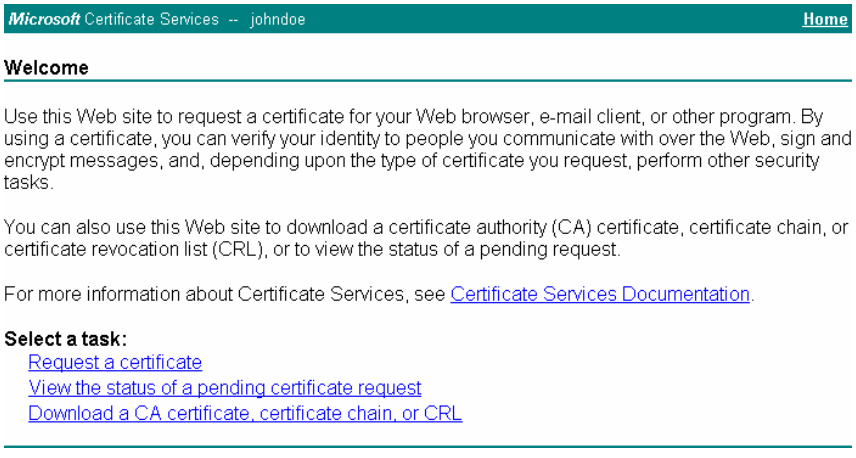


Figure 5-73 Certificate Services Welcome Screen

Click the "**Request a certificate"** task link.

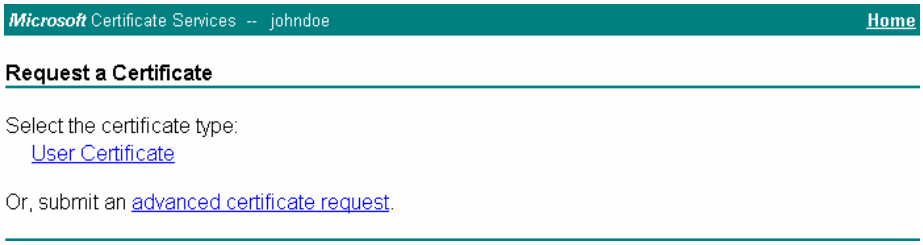


Figure 5-74 Request a Certificate Screen

Click on the "**advanced certificate request"** link.

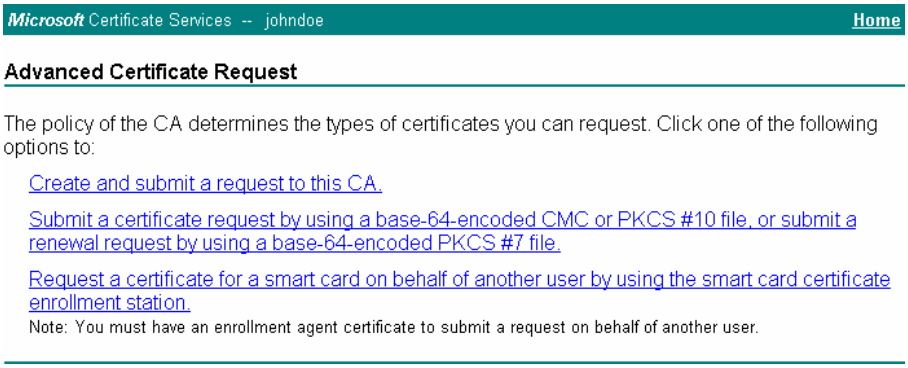


Figure 5-75 Advanced Certificate Request Screen

Click on the "**Create and submit a request to this CA"** link.

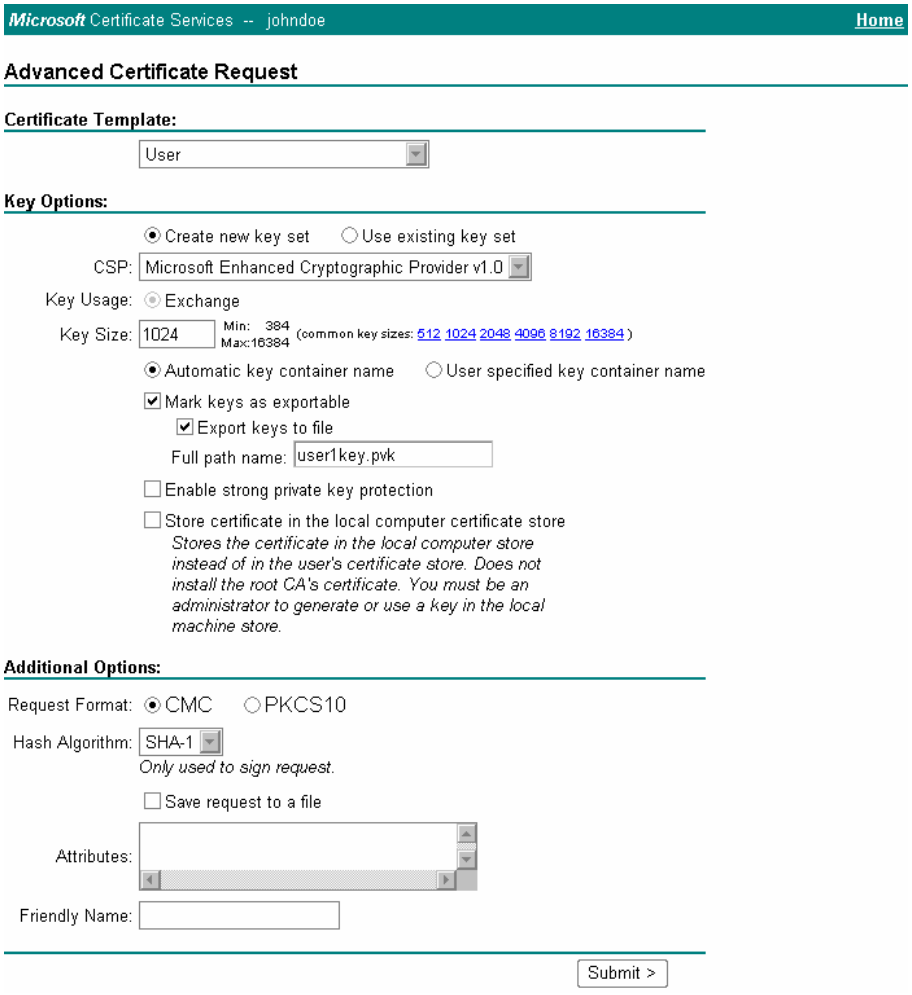


Figure 5-76 Advanced Certificate Details

For the Certificate Template, select “User”.

Check the “Mark keys as exportable” and the “Export keys to file” checkboxes.

Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

⚠	Be sure to note the name used for the private key file, for example MX3XUSER.PVK. The certificate file created later in this process must be given the same name, for example, MX3XUSER.CER.

DO NOT check “Enable strong private key protection”.

Make any other desired changes and click the “Submit” button.

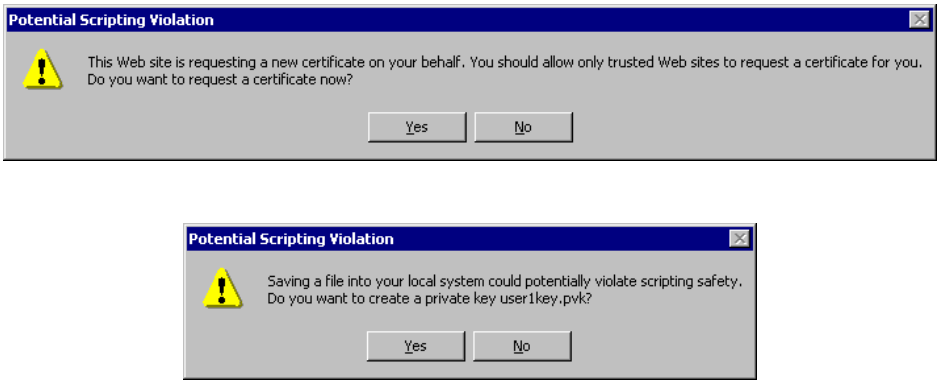


Figure 5-77 Script Warnings

If any script notifications occur, click the "Yes" button to continue the certificate request.

Figure 5-78 Script Warnings

When prompted for the private key password:

- Click "None" if you do not wish to use a password, *or*
- Enter and confirm your desired password then click "OK".

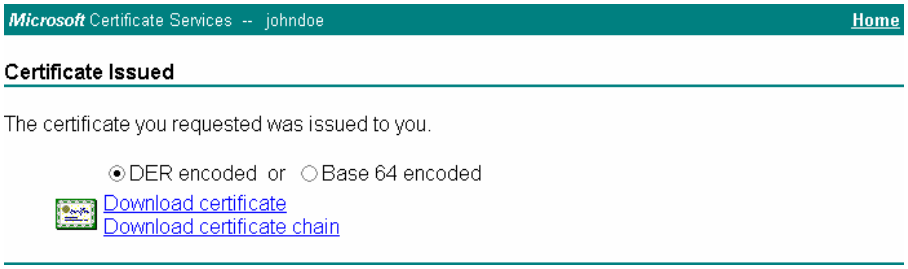


Figure 5-79 Certificate Issued

Click the **Download certificate** link.

Figure 5-80 Download Security Warning

Click **Save** to download and store the user certificate to the PC. Keep track of the name and location of the certificate as the file name and location is required in later steps. The private key file is also downloaded and saved during this process.

	Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as MX3XUSER.PVK then the certificate file created must be given the same name, for example, MX3XUSER.CER.

Installing a User Certificate on the MX3X (WPA-TLS Only)

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select “My Certificates” from the pull down list.

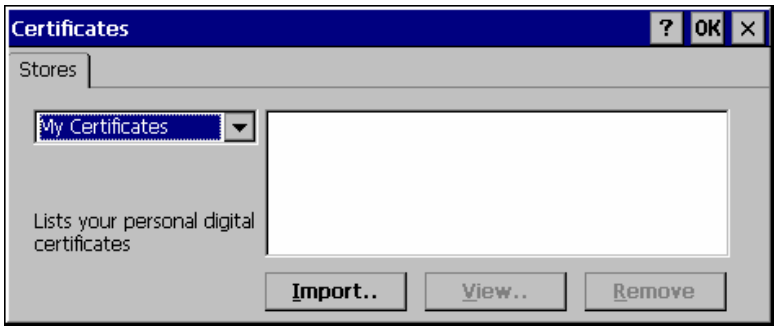


Figure 5-81 Certificates

Click the “Import” button.

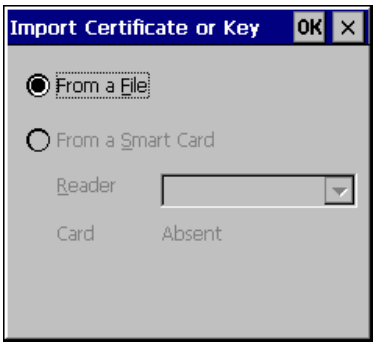


Figure 5-82 Import Certificate

Make sure “From a File” is selected and click OK.

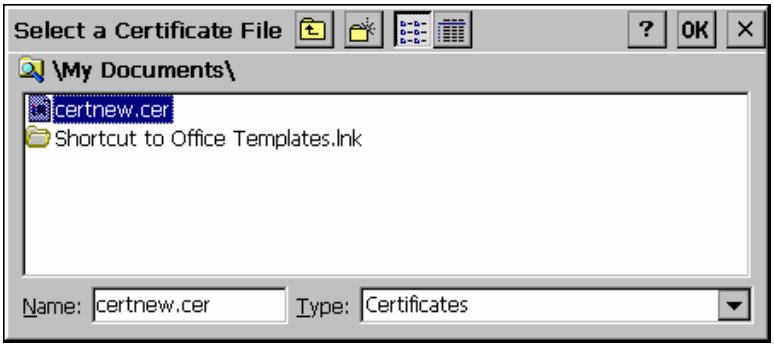


Figure 5-83 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

The certificate is now shown in the list.

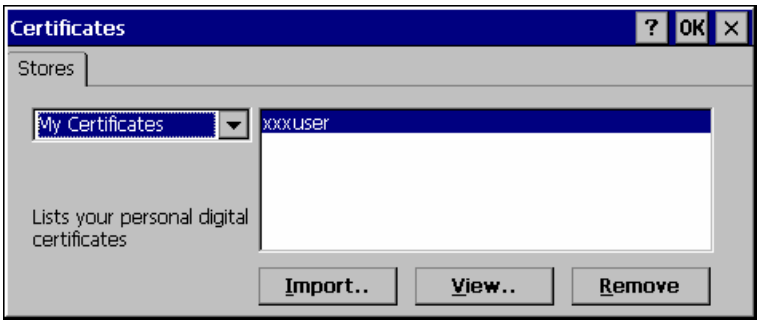


Figure 5-84 Certificate Listing

Highlight the certificate you just imported and tap the View. . button.

From the Field pull down menu, select “Private Key.

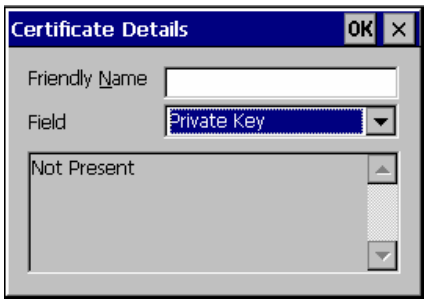


Figure 5-85 Private Key Not Present

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap OK to return to the Certificates screen.

Tap import.

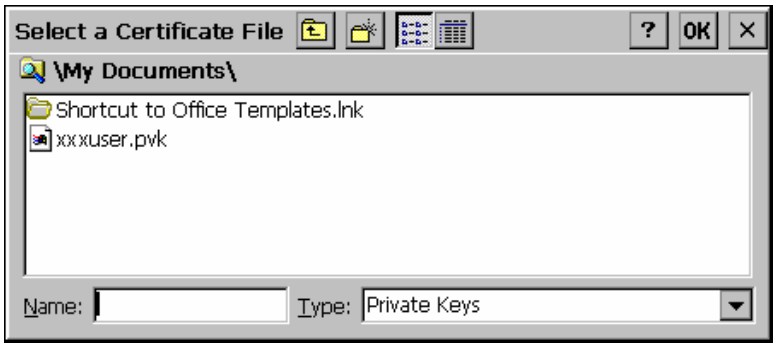


Figure 5-86 Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to "Private Keys", select the certificate desired and tap OK. Enter the password for the certificate if appropriate.

Tap View to see the certificate details again.

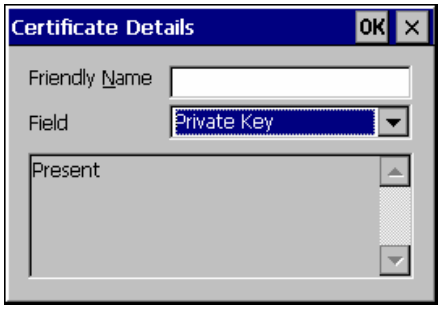


Figure 5-87 Private Key Present

The private key should now say "Present". If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example mx3xuser.cer for the certificate and mx3xuser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

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.

Sections in this chapter that are not specifically Multi-Application or Single Application are used/changed in the same way by both versions.

Note: To reset the device to factory default values, please refer to Chapter 3 "System Configuration" section titled "Utilities" and the RegClear, PSMFormat and ColdBoot executable files.

Setup a New Device

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies an application to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

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

Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.

Multi-Application Version

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

A mobile device running the Multi-Application version of AppLock becomes a dedicated, multiple application device. Only the applications or features specified in the AppLock configuration by the Administrator are available to the end-user. This version offers a user-mode taskbar icon allowing the end-user to switch between user applications.

See section titled *Multi-Application Configuration* for information and instruction. Note: only **two** applications can be specified at this release.

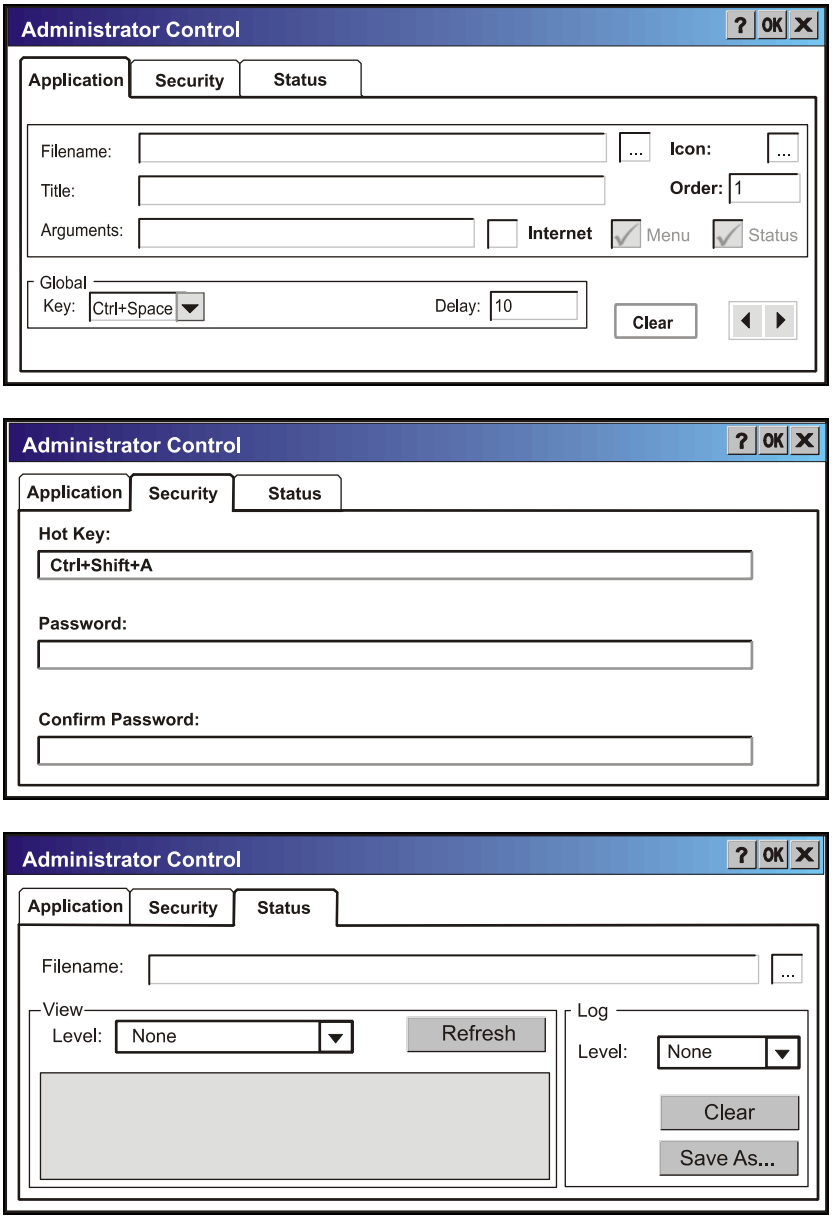


Figure 6-1 Administrator Control Panels – Multi-Application

Single Application Version

Access: **Start | 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.

See section titled *Single Application Configuration* for information and instruction.

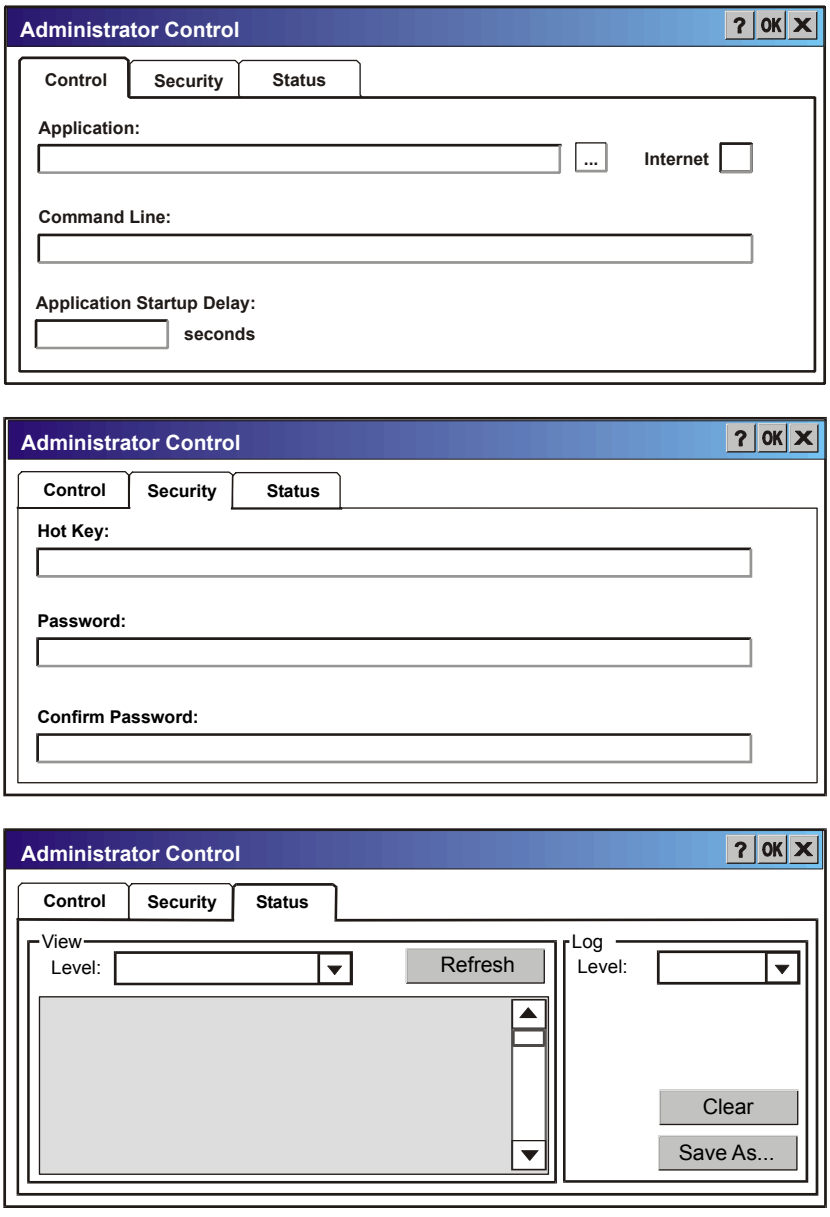


Figure 6-2 Administrator Control Panels – Single Application

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

1. Create/change the keystroke sequence to activate administrator access.
2. Create/change the password for administrator access.
3. Assign the name of the application, or applications, to lock.
4. Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	Shift+Ctrl+A
Password	none
Application path and name	none
Application command line	none

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user taps on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

1. If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
2. If the application name, which is mandatory for end-user mode, is missing in the configuration.
3. Invalid installation of AppLock (e.g. missing DLLs).
4. Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Troubleshooting

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

Multi-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.

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

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Note: AppLock cannot support multiple windows of some applications. Attempting to open multiple windows of RFTerm or Pocket Word will cause AppLock to switch to administration mode.

Application Panel

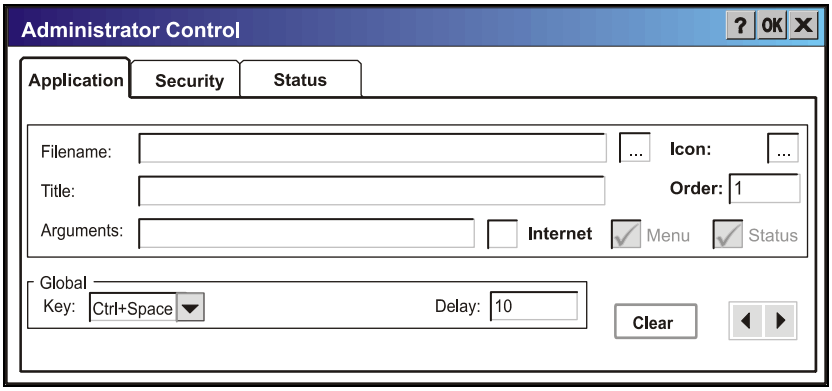


Figure 6-3 Application Panel – Multi-Application

Note: If your Application Panel does not look like the figure shown above, you may have the Single Application version.

Use the **Application** tab options to select the applications to launch when the device boots up in End User Mode.

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.

Enter the **Title** to be associated with the application's icon. The assumption is that multiple copies of the same application may need unique text for the icon in order to differentiate them in the application switcher panel.

Enter the command line parameters for the application in the **Arguments** text box.

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.

Enable the **Internet** checkbox to use the End User Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet **Menu** and Internet **Status** are available. See the section titled *End User Internet Explorer* for more details.

Select the **Global Key** key sequence the end user is to press when switching between applications. The Global Key default key sequence is **Ctrl+Spc**. The Global key is selected from a predefined list of Global hotkey combinations. The Global key is presented to the end-user as the *Activation* key.

Enter the number of seconds in **Global Delay** that both Applications must wait before starting to run upon reboot.

Tap the **Clear** button to clear all Application information that are currently displayed. The Global settings remain the same for both applications.

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.

If no application is specified when the Administrator Control applet is closed, the 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.

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's menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the **Status** checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel

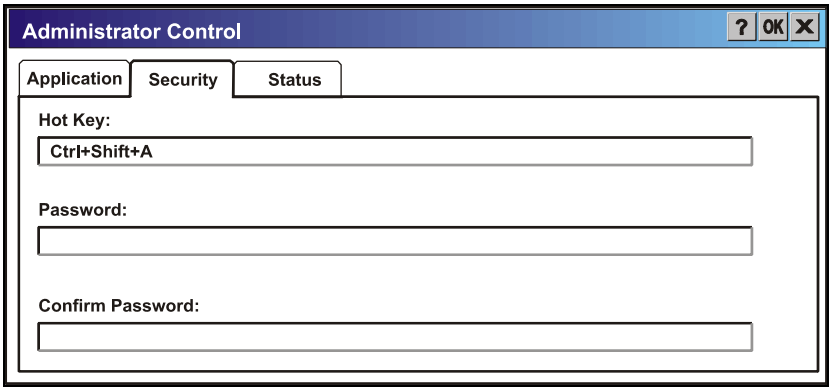


Figure 6-4 Security Panel – Multi-Application

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with “Shift”, “Alt”, and “Ctrl” text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the ‘Ctrl’ key is pressed followed by ‘A’, “Ctrl+A” is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: *Passwords* and *Troubleshooting Multi-Application AppLock*

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

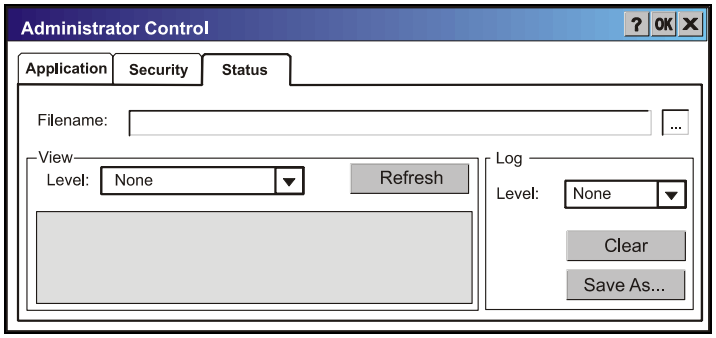


Figure 6-5 Status Panel – Multi-Application

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.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: ***If a level higher than Error is selected, the status should be cleared frequently by the administrator.***

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: *Error Messages*

End-User Switching Technique

Figure 6-6 End-User Multi-Application Touch Panel

Using a Stylus Tap

When the mobile device enters end-user mode, a taskbar icon is available to the user so they can switch between the locked applications. The touch screen must be enabled on the mobile device before the taskbar icon can be used. The taskbar is always visible on top of the application in focus.

When the taskbar icon is tapped, a menu is displayed showing the applications available to the user. The user then taps the 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.

The appearance of the taskbar is different on various mobile device platforms and may differ from the example shown above. This example is shown only to aid in describing how the user can switch between applications using a stylus. If RFTerm and Microsoft Word were the two applications locked, a switching icon showing both applications is displayed on the screen.

Using a Hotkey Sequence

One hotkey is defined for the end-user to key in 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 hotkey or hotkey 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 but end-user key presses affect the application in focus only.

Troubleshooting Multi-Application AppLock

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

> Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

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.

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

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Control Panel

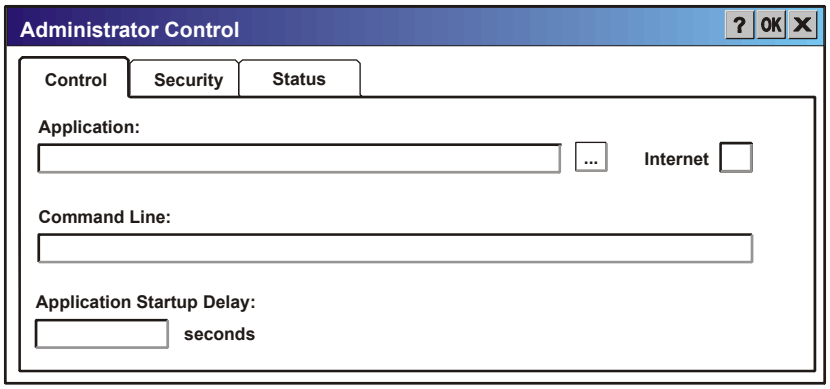


Figure 6-7 Administrator Control Panel

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 Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.

Enter the command line parameters for the application in the Command Line text box.

Enter the number of seconds the selected Application must wait before starting to run upon reboot.

If no application is specified when the Administrator Control panel is closed, the device reboots into Administrator mode. If a password has been set, but the application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

End User Internet Explorer

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode, End-user Internet Explorer (EUIE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by simply checking the "Internet" checkbox in the Control tab of the Administrator applet. The internet application should then be entered in the "Application" text box. If the standard Internet Explorer that is shipped with the device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel

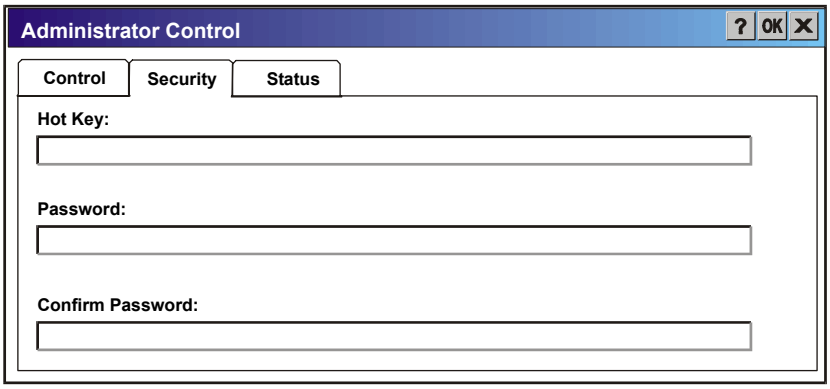


Figure 6-8 Administrator Security Panel

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Note: Some key combinations cannot be specified because they conflict with the key combinations used by other LXE applications. The message "Selected hotkey is not allowed, Please re-enter" is displayed. A different Hotkey must be entered.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with "Shift", "Alt", and "Ctrl" text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence.

For example, if the ‘Ctrl’ key is pressed followed by ‘A’, “Ctrl+A” is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords

Status Panel

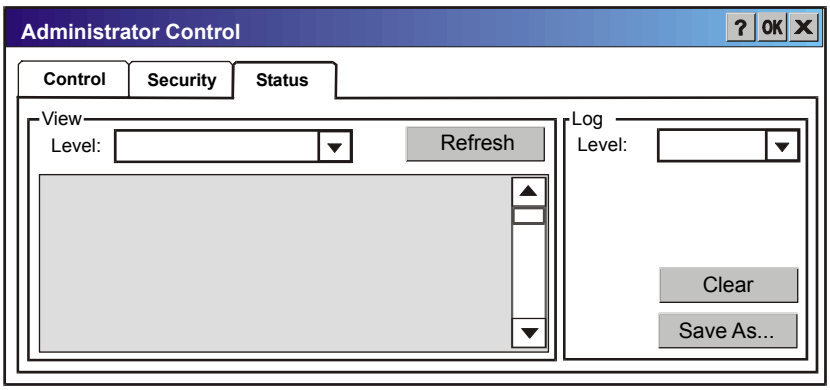


Figure 6-9 Administrator Status Panel

Use the Status panel to view the log of previous AppLock operation and to configure which messages are to be recorded during AppLock operation.

As the status information is stored in the registry and accumulates during AppLock configuration and operation, it is very important that the administrator periodically clear the status information to reduce the amount of registry space used. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Levels

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is Error Logging; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: Error Messages

Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	Applock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete applock.exe from the \Windows directory and reboot the unit. Deleting applock.exe triggers the applock system to reload.	LOG_ERROR

Message	Explanation and/or corrective action	Level
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
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

Message	Explanation and/or corrective action	Level
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

Message	Explanation and/or corrective action	Level
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
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

Message	Explanation and/or corrective action	Level
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

Message	Explanation and/or corrective action	Level
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	Applock is calling the keyboard hook initialization.	LOG_PROCESSING
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

Message	Explanation and/or corrective action	Level
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 the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Adminstration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so Applock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, Applock switches to admin mode. . If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	Applock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and Applock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR

Message	Explanation and/or corrective action	Level
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX
Term process restart –window not found	The locked application has been closed using a method that cannot be detected by AppLock. AppLock will restart the application.	LOG_ERROR

AppLock Registry Settings

This system application runs at startup via the "launch" feature of LXE Windows CE .NET devices. When the launch feature is installed on the device, the following registry settings are created. The launch feature registry settings are embedded in the mobile device OS image:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Filename=AppLock.exe
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Installed=
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\FileCheck=
```

AppLock registry settings identify the application that is going to be locked and any parameters that are needed by the application. These registry settings are as follows:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Administration\\AppName
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppCommandLine=
```

In addition to the registry settings needed to specify the application, additional registry settings are needed to store the configuration options for AppLock. These options include, among others, the administrator's password and hotkey.

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\HotKey=
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\EP=
```

Appendix A Key Maps

Keypad

Note: The key mapping in this appendix relates to the physical keypad. See section titled "Input Panel" for the Virtual (or Soft) Keypad used with the stylus.

Key Map 101-Key Equivalencies

Note: This key mapping is used on hand held computers that are NOT running an LXE Terminal Emulator.

When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.

Note: When the computer boots, the default condition of NumLock is On and the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with a 2nd+F1 key sequence. The CAPS LED is illuminated when CapsLock is On.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Contrast	x					F6
Volume	x					F8
Backlight	x					F10
2nd						2nd
Shift						Shft
Alt						Alt
Ctrl						Ctrl
Esc						Esc
Space						Spc
Enter						Enter
Scan [7]						Scan
CapsLock (Toggle)	x					F1
Back Space						BkSp
Tab						Tab
BackTab	x					Tab
Break	x					F2
Pause	x	x				F3
Up Arrow						Up Arrow
Down Arrow						Down Arrow
Right Arrow						Right Arrow

[7] Left Scan key default value is Scan. Right Scan key default value is Enter.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Left Arrow						Left Arrow
Insert	x					BkSp
Delete	x					DOT
Home	x					Left Arrow
End	x					Right Arrow
Page Up	x					Up Arrow
Page Down	x					Down Arrow
ScrollLock	x	x				F4
F1						F1
F2						F2
F3						F3
F4						F4
F5						F5
F6						F6
F7						F7
F8						F8
F9						F9
F10						F10
F11	x	x				F1
F12	x	x				F2
a					Off	A
b					Off	B
c					Off	C
d					Off	D
e					Off	E
f					Off	F
g					Off	G
h					Off	H
i					Off	I
j					Off	J
k					Off	K
l					Off	L
m					Off	M
n					Off	N
o					Off	O
p					Off	P

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
q					Off	Q
r					Off	R
s					Off	S
t					Off	T
u					Off	U
v					Off	V
w					Off	W
x					Off	X
y					Off	Y
z					Off	Z
A		x				A
B		x				B
C		x				C
D		x				D
E		x				E
F		x				F
G		x				G
H		x				H
I		x				I
J		x				J
K		x				K
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

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
1						1
2						2
3						3
4						4
5						5
6						6
7						7
8						8
9						9
0						0
DOT						DOT
<	x					0
[	x					1
]	x					2
>	x					3
=	x					4
{	x					5
}	x					6
/	x					7
-	x					8
+	x					9
*	x					I
: (colon)	x					D
; (semicolon)	x					F
?	x					L
`	x					N
_ (underscore)	x					M
, (comma)	x					J
‘ (apostrophe)	x					H
~ (tilde)	x					B
\	x					S
|	x					A
“	x					G
!	x					Q
@	x					W
#	x					E

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
$	x					R
%	x					T
^	x					Y
&	x					U
(	x					O
)	x					P

3270 Key Sequences

Legend	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
E-Inp	Erase Input	Ctrl + BkSp
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
PA1		Ctrl+F1
PA2		Ctrl+F2
PA3		Ctrl+F3
Rst	Reset	Ctrl + R
SysReq	System	Ctrl + S

Please refer to the “RFTerm Reference Guide” for further information about Terminal Emulation-specific key functions on the mobile device.

5250 Key Sequences

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 + BkSp
Field Exit	Enter	Enter
Fld –	Field Minus	Ctrl + M
Fld +	Field Plus	Ctrl + L
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
SysReq	System	Ctrl + S

Please refer to the “RFTerm Reference Guide” for further information about Terminal Emulation-specific key functions on the mobile device.

Creating Custom Key Maps

Prerequisite: LXE SDK CD

Note: There may be different SDK kits for Windows CE .NET 4.2 and CE 5.0. Contact your LXE representative to order an LXE SDK CD for your MX3X.

Introduction

A command-line compiler called KEYCOMP.EXE is provided on the SDK CD. Using this compiler, the System Administrator can convert a sample default key map text file into a custom key map text file which, when loaded onto the mobile device, can be chosen by the user to replace the default mobile device keymap and then switched back when they are finished using the customized keys. This custom key map file can be made to re-define the system return code for each of the 61 keys, key press or key press combinations. All keys, except the power key, can be re-mapped.

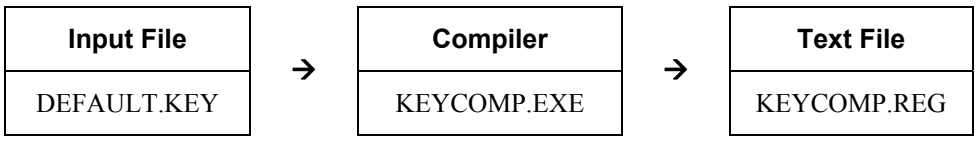
Custom keymaps for the mobile device are created on a desktop PC using the command line compiler KEYCOMP.EXE. Keycomp processes the input keymap source file and outputs a registry text file.

Note: Each VK_code has a numeric value (for example, VK_F20 = hex 83), these are documented in the SDK include file WINUSER.H (from Microsoft). The numeric value is what needs to go into the registry. Whether the value is hex or decimal depends on the registry editor being used - the one in the mobile device requires decimal, but the desktop one used over ActiveSync that a developer may use requires hex.

For Example
Default values: ScanCodeLeft = hex 83, decimal 131
ScanCodeRight = hex 84, decimal 132

Example:

KEYCOMP DEFAULT.KEY (writes KEYCOMP.REG to local directory)



This output file should be renamed to **xxx.REG** (the suffix must remain REG), then copied to the mobile device over ActiveSync. Once the file is loaded on the mobile device, double-tap the file from the Windows CE Explorer desktop. This will run the REGLOAD utility to put it into the registry, and save the registry to non-volatile flash. The keymap is now a permanent part of the mobile device, and the REG file is no longer needed unless it is necessary to perform a cold boot; this will return the registry to factory defaults, and it will be necessary to double-tap the REG file again.

Once the keymap has been added to the registry, it should appear in the Keyboard control panel as the name given in the MAPNAME field in the key file. To activate the keymap, select the keymap from the popup menu, and close the control panel with the OK button. To return to the default keymap, select **0409** from the keymap popup and tap OK.

The compiler has three functional stages:

- First, the input file is read and parsed for any syntax errors. The data read is stored in internal tables.

- Second, the data parsed from the input file is validated to see that all of the items required by the keyboard driver for normal operation are present.
- Third and finally, the KEYCOMP.REG file is written out in the format required by the REGLOAD utility on the Windows CE device.

Programmable Scan Buttons and Custom Key Mapping

The Left and Right Scan buttons can be reset using Custom Key Mapping. Custom keymapping changes the placement of the buttons (e.g., F1 can now be Scan Left).

The keycode that the Scan Left (or F1) button generates is then determined by the setting in the scanner control panel (See Chapter 3 "System Configuration", Control Panel", "Scanner" or Chapter 4 "Scanner".).

Remapping does not allow multiple entries. If the System Administrator uses Custom Key Mapping set a Scan button to ENTER, the original ENTER key must be redefined to something else. However, if the scanner control panel is used to change the Scan button to generate an ENTER, the original ENTER key is maintained as well.

Note: Tethered scanners are not activated/affected by the Scan buttons on the mobile device.

Keymap Source Format

The source file **DEFAULT.KEY** is supplied with the keymap compiler. This is the commented source for the default keymap **0409**. The comments in this file should make the majority of this document redundant. There is a copy of this file at the end of this section, in "Sample Input File**"**. This section should be read while referring to this sample source, for simplicity.

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

It is an important limitation that the keymap must have a 4, 5, or 6 digit numeric name; this is a limit of the Microsoft Windows CE layout manager.

The format of this file is familiar to anyone who has used .INI files under Windows. There is a section header in square brackets, followed by various values in the form *value=data*.

Lines beginning with a semicolon (;) or empty lines are ignored as comments. Spaces or tabs before or after the information are stripped off and ignored. Case is ignored in section names, value names, and value data.

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

COLxROWx Format

Note: There is no relationship between the physical layout COL/ROW of the keyboard / keypad and the COL/ROW listing in the key map file. The key map file represents the electrical layout not the physical layout.

All keys are specified in COLxROWx format. In this format, the first x is the 1 or 2 digit column in the keymap, and the second x is the 1 or 2 digit row in the keymap. All rows and columns are enumerated starting with zero (0).

In the **MAP** section, the **COLxROWx** is the value name, and the values must be less than the **MAPROWS** and **MAPCOLS** specified in the **GENERAL** section.

In the **SPECIAL** section, the **COLxROWx** is the value data, and the values given can be outside the normal key map limits.

GENERAL Section

The first section is the **GENERAL** section. This contains the keymap name (all numerics), as well as the number of rows and columns in the keymap, and the algorithm for converting rows and columns to a data byte to go into the keymap table.

```
.
[General]
MAPNAME=0409
MAPCNT=4
.
```

MAPNAME	Name of this map. This is what appears in the popup menu in the keyboard control panel.
MAPCNT	Gives the number of MAP sections (and hence keymap tables) in this source file.
MAPCOLS	Number of columns in each keymap table. This is defined by the hardware keyboard.
MAPROWS	Number of rows in each keymap table. This is defined by the hardware keyboard.
ALGOR	Defines the algorithm for converting row/column to internal scan code. Current values are: MX3X scancode = ((column << 3) + row)

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

SPECIAL Section

```
.
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
.
```

The second section is the **SPECIAL** section, which contains the row and column definitions for certain modifier keys which must be processed independent of the overall keymap. Currently, these are only modifier keys.

The only recognized names are: **KEYSHIFT**, **KEYALT**, **KEY2ND**, and **KEYCONTROL**, and these specify the row and column of these 4 specific modifier keys, in COLxROWx format. Note the row and column for these keys can be outside the keymap limits specified in the **GENERAL** section, since these are not loaded as part of the keymap proper.

MAP Section

```
.
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
.
```

There will be several (4 to 7) **MAP** sections, each defining the keymap for a given combination of modifier keys. The keyboard driver requires keymaps for normal (no modifiers), SHIFT only, 2ND only, and 2ND-SHIFT combined.

The CTRL modifier and ALT modifier do not have individual keymaps; the keystrokes are passed to the operating system, which is allowed to parse these keys according to Microsoft specifications (for example, ALT-keys are defined to only pulldown menus, with no other function).

The only recognized value names are **MAP** and **COLxROWx** (defining a key code). The only valid values for **MAP** are:

MAP_NORMAL	no modifier keys
MAP_2ND	2nd modifier only
MAP_SHIFT	shift modifier only
MAP_2NDSHF (or) MAP_2NDSHIFT	2nd and shift modifiers together

In addition, certain keymaps are used for special adjustment functions within the keyboard driver, via the **CHANGE+mapname** specification:

MAP_VOLUM (or) MAP_VOLUME	special keymap for volume adjustment
MAP_CONTR (or) MAP_CONTRAST	special keymap for contrast adjustment
MAP_BRITE (or) MAP_BRIGHT	special keymap for brightness adjustment

When these maps are selected, the keyboard driver handles the up arrow and down arrow as adjusting the particular parameter up and down, and any other key exits the adjustment state. Keys in these modes are handled completely inside the keyboard driver, and are not propagated to the operating system.

Key codes are defined by **COLxROWx=scancode**. **Scancode** has a number of options, as follows:

VK_code	any valid Windows VK code (see below for valid codes)
'x'	a single ASCII character ('A','b','1','@',' ', etc.)
SHIFT+VK_code	for a shifted VK code (see below for valid codes)
SHIFT+'x'	for a shifted ASCII character (should not be needed)
ACTION+code	special function key (valid codes listed below)
CHANGE+mapname	for modifier keys, change keymaps to mapname, as specified above
OPEN	an unused key position, does nothing when pressed

Valid **ACTION** codes are as follows:

SCAN1	Scan key 1 (left side of screen on mobile device)
SCAN2	Scan key 2 (right side of screen on mobile device)
SCAN3	Handle trigger button (unused on mobile device, but specified)
POWER	power button
BACKLIGHT	backlight on/off function

Note that specifying the power button in a different location will affect suspend/resume functions. The "15-second hold to force reboot" function is controlled by hardware, and will only work with the default power button.

Keycomp Error Messages

Most error messages will specify the line within the keymap source file where the error occurred.

Duplicate key

A COLxROWx code was found in a MAP table, but that COL/ROW already has a value assigned.

GENERAL section must come before MAP

The GENERAL section must come first, or at least before any MAP sections. The GENERAL section defines parameters which are needed to process Maps

Header line missing close bracket

The section header line must have square brackets before and after the section name

Header line missing open bracket

The section header line must have square brackets before and after the section name

Invalid ACTION code %s

The key scan code is specified as ACTION+code, but the ACTION code parsed is not recognized. The following values are valid: SCAN1, SCAN2, SCAN3, POWER, or BACKLIGHT.

Invalid keycode %s

The keycode parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A' or '#').
- OPEN for unused entries (will not do anything when pressed)

Invalid MAP value %s

The MAP value parsed is not one the following list: MAP_NORMAL, MAP_2ND, MAP_SHIFT, MAP_2NDSHF, MAP_2NDSHIFT, MAP_VOLUM, MAP_VOLUME, MAP_CONTR, MAP_CONTRAST, MAP_BRITE, or MAP_BRIGHT.

Invalid MAPCNT (1-%d valid)

The specified MAPCNT exceeds the limits of the KEYCOMP compiler.

Invalid MAPCOLS (1-%d valid)

The specified MAPCOLS exceeds the limits of the KEYCOMP compiler.

Invalid MAPROWS (1-%d valid)

The specified MAPROWS exceeds the limits of the KEYCOMP compiler.

Invalid ROWCOL format

A COLxROWx was expected, but the format was not correct. The only valid formats are: COLxROWx, COLxxROWx, COLxROWxx, or COLxxROWxx, where xx are decimal numeric digits (0-9).

Invalid scan code

The scan code parsed is not recognized. The scan code can take one of the following formats:

- VK_code
- 'x'
- SHIFT+VK_code
- SHIFT+'x'
- ACTION+code
- CHANGE+mapname
- OPEN

Invalid section name %s

The section name parsed is invalid. The only recognized names are: GENERAL, SPECIAL, or MAP

Invalid SHIFT code %s

The key scan code is specified as SHIFT+code, but the SHIFT code parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A', '3', or '#').

Invalid value %s in GENERAL section

The value name parsed is invalid for the GENERAL section. The recognized names are: MAPNAME, MAPCNT, MAPCOLS, MAPROWS, or ALGOR

Invalid value %s in MAP section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: MAP and COLxxx.

Invalid value %s in SPECIAL section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: KEYSHIFT, KEYALT, KEY2ND, and KEYCONTROL.

Invalid VK_ code %s

The VK code parsed is not recognized. See the VK Code Table (below) for valid values.

Map ended without MAP value

The MAP section must contain a MAP value, so the data fields can be parsed.

MAPNAME must be all numerics

Because of limitations in Microsoft Layout Manager, the map name must be all numeric (4, 5, or 6 digits). The name parsed did not fit this limitation.

No definition for map MAP_2ND

There is no 2nd keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_2NDSHIFT

There is no 2nd-SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_NORMAL

There is no Normal keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_SHIFT

There is no SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.key2nd

No 2ND modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyalt

No ALT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keycontrol

No CTRL modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keydnarrow

No down arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keypower

No power key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan1

No Scan Key 1 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan2

No Scan Key 2 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan3

No Trigger Button definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyshift

No SHIFT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyuparrow

No up arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No equal in value line

A value line must be of the form *value=data*. A value line was expected, but there was no equal in it. *(or)* A comment line did not begin with a semicolon (;).

No MAPNAME defined

There is no map name defined. The keyboard driver requires this name to be able to load the keymap tables. This message comes from the post-parse validation, so no line # is specified.

Scan code algorithm required

A COLxROWx data value was found before any ALGOR statement. ALGOR algorithm is parsed to decide how to encode COLxROWx into a keymap value.

Too many maps for specified MAPCNT

There are more MAP sections defined that the MAPCNT field specified.

Unknown scan code algorithm

The ALGOR algorithm specified is not one that KEYCOMP understands.

Unrecognized scancode algorithm %s

The ALGOR algorithm specified is not one that KEYCOMP understands.

Value outside of section

A value (defined as *value=data*) is only valid within a section (defined as *[section]*). A value line was found when a section header line was expected.

Sample Input File

```
;;-----------------------------------------------------
;; keymap file for MX3X default keyboard
;;-----------------------------------------------------

;;-----------------------------------------------------
;; general parms give the size of arrays
;; all numeric values are decimal
;; these numbers are validated with the data below
;; at compile time
;; MAPNAME must be all numerics
;;-----------------------------------------------------
[General]
MAPNAME=0409
MAPCNT=4
MAPCOLS=8
MAPROWS=8
ALGOR=MX3X

;;-----------------------------------------------------
;; special keys are accessed outside the map
;; this specifies the row and column
;; these should not need to change, but...
;;-----------------------------------------------------
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
KEY2ND=COL10ROW0
KEYCONTROL=COL11ROW0

;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with no modifier
;;-----------------------------------------------------
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=VK_F7
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0='Q'
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3='T'
COL1ROW4='U'
COL1ROW5='4'
COL1ROW6='O'
```

```
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0='A'
COL2ROW1=open
COL2ROW2='D'
COL2ROW3='G'
COL2ROW4='J'
COL2ROW5='1'
COL2ROW6='L'
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=' '
COL3ROW1=open
COL3ROW2='X'
COL3ROW3='V'
COL3ROW4='N'
COL3ROW5='0'
COL3ROW6=VK_LEFT
COL3ROW7=VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=VK_F9
COL4ROW1='S'
COL4ROW2=VK_RIGHT
COL4ROW3='F'
COL4ROW4='H'
COL4ROW5='K'
COL4ROW6='2'
COL4ROW7=VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1='Z'
COL5ROW2=VK_BACK
COL5ROW3='C'
COL5ROW4='B'
COL5ROW5='M'
COL5ROW6=VK_PERIOD
COL5ROW7=VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=VK_F10
COL6ROW1='W'
COL6ROW2=VK_RETURN
COL6ROW3='R'
COL6ROW4='Y'
COL6ROW5='I'
COL6ROW6='5'
COL6ROW7='P'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0='E'
COL7ROW1=open
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4=VK_F6
COL7ROW5='7'
COL7ROW6=VK_F8
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only 2ND
;;-----------------------------------------------------
[Map]
MAP=MAP_2ND
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_CAPITAL
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_PAUSE
COL0ROW4=open
COL0ROW5=open
COL0ROW6=VK_HYPHEN
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'1'
COL1ROW1=SHIFT+VK_EQUAL
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'5'
COL1ROW4=SHIFT+'7'
COL1ROW5=VK_EQUAL
COL1ROW6=SHIFT+'9'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+VK_BACKSLASH
COL2ROW1=open
COL2ROW2=SHIFT+VK_SEMICOLON
COL2ROW3=SHIFT+VK_APOSTROPHE
COL2ROW4=VK_COMMA
COL2ROW5=VK_LBRACKET
COL2ROW6=SHIFT+VK_SLASH
COL2ROW7=SHIFT+VK_PERIOD
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=VK_BACKQUOTE
COL3ROW5=SHIFT+VK_COMMA
COL3ROW6=VK_HOME
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=VK_BACKSLASH
COL4ROW2=VK_END
COL4ROW3=VK_SEMICOLON
COL4ROW4=VK_APOSTROPHE
COL4ROW5=VK_PERIOD
COL4ROW6=VK_RBRACKET
COL4ROW7=VK_PRIOR
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+VK_RBRACKET
COL5ROW1=open
```

```
COL5ROW2=VK_INSERT
COL5ROW3=open
COL5ROW4=SHIFT+VK_BACKQUOTE
COL5ROW5=SHIFT+VK_HYPHEN
COL5ROW6=VK_DELETE
COL5ROW7=VK_NEXT
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=ACTION+BACKLIGHT
COL6ROW1=SHIFT+'2'
COL6ROW2=open
COL6ROW3=SHIFT+'4'
COL6ROW4=SHIFT+'6'
COL6ROW5=SHIFT+'8'
COL6ROW6=SHIFT+VK_LBRACKET
COL6ROW7=SHIFT+'0'
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'3'
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=CHANGE+MAP_CONTRAST
COL7ROW5=VK_SLASH
COL7ROW6=CHANGE+MAP_VOLUME
COL7ROW7=open

;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with 2ND and SHIFT
;;-----------------------------------------------------
[Map]
MAP=MAP_2NDSHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=open
COL0ROW5=open
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=open
COL1ROW4=open
COL1ROW5='4'
COL1ROW6=open
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=open
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=open
```

```
COL2ROW5='1'
COL2ROW6=open
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5='0'
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=open
COL4ROW3=open
COL4ROW4=open
COL4ROW5=open
COL4ROW6='2'
COL4ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1=open
COL6ROW2=open
COL6ROW3=open
COL6ROW4=open
COL6ROW5=open
COL6ROW6='5'
COL6ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=VK_PAUSE
COL7ROW3=VK_SCROLL
COL7ROW4=VK_SNAPSHOT
COL7ROW5='7'
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only SHIFT
;;-----------------------------------------------------
[Map]
MAP=MAP_SHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=SHIFT+VK_ESCAPE
COL0ROW1=SHIFT+VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_F2
COL0ROW4=SHIFT+VK_F5
COL0ROW5=SHIFT+VK_F7
COL0ROW6=SHIFT+'8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'Q'
COL1ROW1=SHIFT+'9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'T'
COL1ROW4=SHIFT+'U'
COL1ROW5=SHIFT+'4'
COL1ROW6=SHIFT+'O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+'A'
COL2ROW1=open
COL2ROW2=SHIFT+'D'
COL2ROW3=SHIFT+'G'
COL2ROW4=SHIFT+'J'
COL2ROW5=SHIFT+'1'
COL2ROW6=SHIFT+'L'
COL2ROW7=SHIFT+'3'
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=SHIFT+' '
COL3ROW1=open
COL3ROW2=SHIFT+'X'
COL3ROW3=SHIFT+'V'
COL3ROW4=SHIFT+'N'
COL3ROW5=SHIFT+'0'
COL3ROW6=SHIFT+VK_LEFT
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=SHIFT+VK_F9
COL4ROW1=SHIFT+'S'
COL4ROW2=SHIFT+VK_RIGHT
COL4ROW3=SHIFT+'F'
COL4ROW4=SHIFT+'H'
COL4ROW5=SHIFT+'K'
COL4ROW6=SHIFT+'2'
COL4ROW7=SHIFT+VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+'6'
COL5ROW1=SHIFT+'Z'
```

```
COL5ROW2=SHIFT+VK_BACK
COL5ROW3=SHIFT+'C'
COL5ROW4=SHIFT+'B'
COL5ROW5=SHIFT+'M'
COL5ROW6=SHIFT+VK_PERIOD
COL5ROW7=SHIFT+VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=SHIFT+VK_F10
COL6ROW1=SHIFT+'W'
COL6ROW2=SHIFT+VK_RETURN
COL6ROW3=SHIFT+'R'
COL6ROW4=SHIFT+'Y'
COL6ROW5=SHIFT+'I'
COL6ROW6=SHIFT+'5'
COL6ROW7=SHIFT+'P'
;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'E'
COL7ROW1=open
COL7ROW2=SHIFT+VK_F3
COL7ROW3=SHIFT+VK_F4
COL7ROW4=SHIFT+VK_F6
COL7ROW5=SHIFT+'7'
COL7ROW6=SHIFT+VK_F8
COL7ROW7=open
```

Sample Output File

```
[HKEY_CURRENT_USER\Keyboard Layout\0409]
;; header limits and special keys
;;  MAPCNT
;;  MAPCOLS
;;  MAPROWS
;;  # of keys in each map
;;  (unused)
;;  (unused)
;;  scancode value for power key
;;  scancode value for up arrow
;;  scancode value for down arrow
;;  scancode value for scan key 1
;;  scancode value for scan key 2
;;  scancode value for trigger button
;;  scancode value for SHIFT
;;  scancode value for ALT
;;  scancode value for 2ND
;;  scancode value for CTRL key
"Head"=hex: 04,08,08,40,00,00,02,27,2F,07,0F,0A,40,48,50,58

;; Map0 is the scancode values for the NORMAL key map
"Map0"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag0 is the shift codes for the NORMAL key map
"Flag0"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map1 is the scancode values for the 2ND key map
"Map1"=hex:\
    00,14,DF,13,00,00,BD,87,31,BB,89,35,37,BB,39,88,\
    DC,00,BA,DE,BC,DB,BF,BE,00,00,00,00,C0,BC,24,09,\
    00,DC,23,BA,DE,BE,DD,21,DD,00,2D,00,C0,BD,2E,22,\
    8A,32,00,34,36,38,DB,30,33,00,00,00,00,BF,00,00

;; Flag1 is the shift codes for the 2ND key map
"Flag1"=hex:\
    00,00,A0,10,00,86,00,A0,10,10,A0,10,10,00,10,A0,\
    10,00,10,10,00,00,10,10,00,00,00,00,00,10,00,10,\
    00,00,00,00,00,00,00,00,10,00,00,00,10,10,00,00,\
    A0,10,00,10,10,10,10,10,10,00,00,00,85,00,84,00

;; Map2 is the scancode values for the 2ND-SHIFT key map
"Map2"=hex:\
    00,7A,DF,7B,00,00,38,87,00,39,89,00,00,34,00,88,\
    00,00,00,00,00,31,00,33,00,00,00,00,00,30,00,00,\
    00,00,00,00,00,00,32,00,36,00,00,00,00,00,00,00,\
```

```
    00,00,00,00,00,00,35,00,00,00,13,91,2C,37,00,00

;; Flag2 is the shift codes for the 2ND-SHIFT key map
"Flag2"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map3 is the scancode values for the SHIFT key map
"Map3"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag3 is the shift codes for the SHIFT key map
"Flag3"=hex:\
    10,10,A0,10,10,10,10,A0,10,10,A0,10,10,10,10,A0,\
    10,00,10,10,10,10,10,10,10,00,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,00,10,10,10,10,10,00
```

List of Valid VK Codes for CE .NET and 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 .NET and CE.

Note: There may be different VK Codes for Windows CE .NET 4.2 and CE 5.0. Check with your LXE representative before using VK Codes for your MX3X.

VK_ADD	VK_F3	VK_NUMPAD9
VK_APOSTROPHE	VK_F4	VK_OEM_CLEAR
VK_APPS	VK_F5	VK_OFF
VK_ATTN	VK_F6	VK_PA1
VK_BACK	VK_F7	VK_PAUSE
VK_BACKQUOTE	VK_F8	VK_PERIOD
VK_BACKSLASH	VK_F9	VK_PLAY
VK_BROWSER_BACK	VK_FINAL	VK_PRINT
VK_BROWSER_FAVORITES	VK_HANGUL	VK_PRIOR
VK_BROWSER_FORWARD	VK_HANJA	VK_RBRACKET
VK_BROWSER_HOME	VK_HELP	VK_RBUTTON
VK_BROWSER_REFRESH	VK_HOME	VK_RCONTROL
VK_BROWSER_SEARCH	VK_HYPHEN	VK_RETURN
VK_BROWSER_STOP	VK_INSERT	VK_RIGHT
VK_CANCEL	VK_JUNJA	VK_RMENU
VK_CAPITAL	VK_KANA	VK_RSHIFT
VK_CLEAR	VK_KANJI	VK_RWIN
VK_COMMA	VK_LAUNCH_APP1	VK_SCROLL
VK_CONTROL	VK_LAUNCH_APP2	VK_SELECT
VK_CONVERT	VK_LAUNCH_MAIL	VK_SEMICOLON
VK_CRSEL	VK_LAUNCH_MEDIA_SELECT	VK_SEPARATOR
VK_DECIMAL	VK_LBRACKET	VK_SHIFT
VK_DELETE	VK_LBUTTON	VK_SLASH
VK_DIVIDE	VK_LCONTROL	VK_SLEEP
VK_DOWN	VK_LEFT	VK_SNAPSHOT
VK_END	VK_LMENU	VK_SPACE
VK_EQUAL	VK_LSHIFT	VK_SUBTRACT
VK_EREOF	VK_LWIN	VK_TAB
VK_ESCAPE	VK_MBUTTON	VK_UP
VK_EXECUTE	VK_MEDIA_NEXT_TRACK	VK_VOLUME_DOWN
VK_EXSEL	VK_MEDIA_PLAY_PAUSE	VK_VOLUME_MUTE
VK_F1	VK_MEDIA_PREV_TRACK	VK_VOLUME_UP
VK_F10	VK_MEDIA_STOP	VK_ZOOM
VK_F11	VK_MENU	
VK_F12	VK_MULTIPLY	
VK_F13	VK_NEXT	
VK_F14	VK_NOCONVERT	
VK_F15	VK_NONAME	
VK_F16	VK_NUMLOCK	
VK_F17	VK_NUMPAD0	
VK_F18	VK_NUMPAD1	
VK_F19	VK_NUMPAD2	
VK_F2	VK_NUMPAD3	
VK_F20	VK_NUMPAD4	
VK_F21	VK_NUMPAD5	
VK_F22	VK_NUMPAD6	
VK_F23	VK_NUMPAD7	
VK_F24	VK_NUMPAD8	

Appendix B Technical Specifications

Physical Specifications

Features		Specifications	Comments	
CPU		Xscale PXA255 CPU operating at 400 MHz. Turbo mode switching is supported.	32 bit CPU (with on-chip cache)	
Compact Flash (Internal)		Supports an ATA interface only.	3.3v ATA flash card. Inaccessible by customer.	
Memory	ROM RAM	64 MB Flash 64 or 128MB of SDRAM	 System Memory	
Display	LCD	Monochrome Transflective Transmissive Color	Transflective LCD with touchscreen. Customer Configurable Backlighting	
Mass Storage	Removable PC Card	SRAM or Flash PCMCIA Type I or II PC Cards (Various Sizes) Compact Flash Card	Bootable SRAM PC Card, ATA Flash PC Card, or ATA Hard Drive PC Card (Customer Installable)	
PCMCIA Interface		Slot 0 accepts Type I and II Slot 1 accepts Type I and II CF+	Compatible with the PCMCIA version 2.1 standard.	
Weights		Unit with radio, battery and scanner endcap	Less than 30 oz	<850g
		Battery	5.6 oz	157g
		Network Card - 2.4GHz Type II	1.0 oz 1.6 oz	28g 45g
		SRAM Card	1 oz	28g
External Connectors/Interface USB Host / Client Ports		IrDA Connector (COM 2) bi-directional half-duplex	Supports 115k baud	
		Endcap - Dual Serial, DA-9 or DB-9 Connector (COM 1 and COM 3)	9 Pin “D” (male) Connector. Provides connection to external devices such as a printer.	
		Endcap - incl Scanner (COM 3), DA-9 or DB-9 Connector (COM 1)	9 Pin “D” (male) Connector. Provides connection to external devices such as a printer.	
		Endcap – incl Scanner (COM 3), DA-9 (COM 1)	Scanner – SE923 or SE955 Symbol engine	
Power Connector		8.5V - 15 VDC Input Power	External Battery Charger Contacts	
		10.8 - 16VDC Input Power	Power Jack	

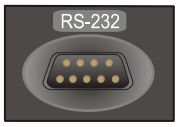
Features		Specifications	Comments	
Audio Connector			Audio Jack	
Dimensions w/Endcap		Length	6”	15 cm
		Width	8”	20 cm
		Depth (No RFID)	1.44”	3.66 cm
		Depth (With RFID Module)	1.88”	4.77 cm
Batteries	Main	1900 mAh 10.8V, 3 cell, Li-Ion battery pack	In-Unit Chargeable or Externally Chargeable	
	Backup (CMOS)	Internal Nickel-Cadmium (NiCd) 5.7V max.	Automatically charges from main battery during normal operation Memory operational for 5 minutes when main battery is depleted	

Display Specifications

Type	LCD - Transflective Monochrome, Transmissive Color Electroluminescent Backlighting
Resolution	640x240 pixels
Size	½ VGA landscape
Diagonal Viewing Area	5.92 in (150.4mm)
Dot Pitch	0.22mm
Dot Size	0.20mm x 0.20mm
Color Scale	Monochrome - 16 Shades of Gray Transmissive – 256 colors

Cable Specifications

Caution: Do Not Use this Port for Cables with USB Plugs/Receptacles:



Caution: Do Not Use these Labeled Ports for Tethered Scanners:

Cable Ends

Receptacle	Plug	Receptacle	Plug
 USB A	 USB A	 RS232	 RS232
 USB B	 USB B		

Cable Pinouts and Diagrams

MX3X068CBLD9USBHOST – CBL, USB D9F to USB Type A Receptacle

ActiveSync: Connect from mobile device USB-C port to USB Type A Host. E.g. laptop/desktop PC.

Mobile Device Client End	Goes To	USB Type A Plug End
1	Host Detect	1
2	Not Used	
3	D+	3
4	Not Used	
5	GND	4
6	Not Used	
7	D-	2
8	Not Used	
9	Not Used	

MX3XA069CBLD9USBCLNT – CBL, USB D9F to USB Type B Plug

Connect from MX3X USB-H port to USB Type B device. e.g. Hub, camera, other client device, etc.

Mobile Device Host port End	Goes To	USB Type B Plug End
1	Not Used	
2	Not Used	
3	D+	3
4	Not Used	
5	GND	4
6	Not Used	
7	D-	2
8	Not Used	
9	PWR	1

MX3XA070CBLD9RS232AS - Cable, RS232 (D9F) / RS232 (D9F) 	*ActiveSync*: Connect from desk cradle male serial port to a D9 male serial port on a PC / Laptop. Cable used for serial ActiveSync. 
MX3XA068CBLD9USBHOST – CBL, USB D9F to USB Type A Plug  Connect from mobile device USB-H to a USB device with a cable that has a Type A plug end. e.g. USB mouse, USB keyboard, etc. 	Mobile Device Host port End — Goes To — USB Type A Receptacle End 1 ..... Not Used 2 ..... Not Used 3 ..... D+ ..... 3 4 ..... Not Used 5 ..... GND ..... 4 6 ..... Not Used 7 ..... D- ..... 2 8 ..... Not Used 9 ..... PWR 1
9000A054CBL6D9D9 - Cable, RS232 (D9F) / RS232 (D9F)	D9 Female — D9 Female 1 ..... 7 2 ..... 3 3 ..... 2 4 ..... 6,8 5 ..... 5 6,8 ..... 4 7 ..... 1 9 ..... Not Used
Tethered Scanner: Connect to MX3X powered Cradle D9F Serial port. 	RS232 Tethered Scanner Serial Port on Cradle  **Do Not Use these Endcap Labeled Ports for Tethered Scanners:** 

Environmental Specifications

Mobile Device and Endcaps

Operating Temperature	-4°F to 122°F (-20°C to 50°C) monochrome 32°F to 122°F (0°C to 50°C) color
Storage Temperature	-22°F to 158°F (-30°C to 70°C)
Water and Dust	IEC IP66
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Ambient Light – ranging from total darkness to direct sunlight	Display readable (with backlight on) for <= two hours Keypad readable (after previous exposure to a 60W bulb for 30 minutes) for <= 15 minutes.
Contamination	Resistant to exposure to skin oil and other lubricants.
Vibration	Based on MIL Std 810F
ESD	8 KV air, 4kV direct contact
Shock, MX3X	Multiple 4 foot drops to concrete. 6 foot with protective cover/boot

Power Supplies

US AC Wall Adapter

Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Thermal Fuse
Input Voltage	108VAC min - 132VAC max
Input Frequency	47 - 63 Hz
Input Connector	North American wall plug, no ground
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11.5mm, Center Positive
Output Voltage	+12VDC, unregulated
Output Current	0 Amps min, 1.5 A max
Operating Temperature	32° F to 104° F / 0° C to 40° C
Storage Temperature	-13° F to 158° F / -25° C to 70° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

International AC Adapter

Operating Temperature	32°F to 104°F (-0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Input Power Switch	None
Power "ON" Indicator	None
Input Voltage	108VAC min - 264VAC max
Input Frequency	47 - 63 Hz
Input Connector	Customer supplied
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11mm, Center Positive
Output Voltage	+12VDC, regulated
Output Voltage Regulation	+/- 5%
Output Current	0 Amps min, 1.00 Amps max

Network Device Specifications

Summit Client in PCMCIA Adapter 2.4GHz

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 MX3X Environmental Specs
Storage Temperature	see MX3X Environmental Specs
Connectivity:	Novell, TCP/IP, Ethernet, ODI

PCMCIA 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 MX3X Environmental Specs
Storage Temperature	see MX3X Environmental Specs
Connectivity	Novell, TCP/IP, Ethernet, ODI
Antenna	Internal

PCMCIA Symbol Client 11Mb 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 MX3X Environmental Specs
Storage Temperature	see MX3X Environmental Specs
Connectivity:	TCP/IP, Ethernet, NDSI

Hat Encoding

The MX3X supports only 7-bit hat encoding which means only ^@ through ^_ (underscore) are supported.

Desired ASCII	Hex Value	Hat Encoded
NUL	**0X00**	**^@**
SOH	**0X01**	**^A**
STX	**0X02**	**^B**
ETX	**0X03**	**^C**
EOT	**0X04**	**^D**
ENQ	**0X05**	**^E**
ACK	**0X06**	**^F**
BEL	**0X07**	**^G**
BS	**0X08**	**^H**
HT	**0X09**	**^I**
LF	**0X0A**	**^J**
VT	**0X0B**	**^K**
FF	**0X0C**	**^L**
CR	**0X0D**	**^M**
SO	**0X0E**	**^N**
SI	**0X0F**	**^O**
DLE	**0X10**	**^P**
DC1 (XON)	**0X11**	**^Q**
DC2	**0X12**	**^R**
DC3 (XOFF)	**0X13**	**^S**
DC4	**0X14**	**^T**
NAK	**0X15**	**^U**
SYN	**0X16**	**^V**
ETB	**0X17**	**^W**
CAN	**0X18**	**^X**
EM	**0X19**	**^Y**
SUB	**0X1A**	**^Z**
ESC	**0X1B**	**^[**
FS	**0X1C**	**^**
GS	**0X1D**	**^]**
RS	**0X1E**	**^^**
US	**0X1F**	**^_ (Underscore)**
	0X7F	**^?**
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1
²	B2	~2
³	B3	~3

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~”
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~’
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z
Û	DB	~[
Ü	DC	~\\

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

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

Decimal - Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42[8]	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)

[8] 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 G, November 2006

Notices	Updated trademark statements.
Chapter 1 – Introduction	Updated “Overview” description. Added Wavelink Avalanche Enabler to “Features/Options of the MX3X Family”. Updated “Related Manuals” section. Updated RoHS Accessories.
Chapter 2 – Physical Description and Layout	Added contents of Chapter 3 “Power Supply” to Chapter 2.
Chapter 3 – Power Supply	Deleted. Contents added to Chapter 2.
Chapter 3 – System Configuration	Renumbered from Chapter 4. Updated “Wavelink Avalanche Enabler (Option)”. Added “Wavelink Avalanche Enabler Configuration”. Changed “radio” to “wireless” or “client” in context, if suitable. Updated default value for Display Backlight Idle Timer from 30 seconds to 3 seconds.
Chapter 4 – Scanner	New.
Chapter 5 – MX3-RFID	Deleted. Refer to the “MX3-RFID User’s Guide” and the “MX3-RFID Reference Guide”. Moved “Hat Encoding” and “Decimal-Hexadecimal Chart” sections to Appendix B “Technical Specifications”.
Chapter 5 – Wireless Network Configuration	Renumbered from Chapter 7 to Chapter 5. Added “Sign-on Screen for LEAP, PEAP/MS-CHAP, PEAP/GTC”. Added configuration instruction for PEAP/GTC on Summit devices. Updated parameters and options based on Summit version 1.2.10 differences.
Chapter 6 – AppLock	No change.
Appendix B – Technical Specifications	Added “Hat Encoding” and “Decimal-Hexadecimal Chart” from the deleted Chapter 3 “MX3-RFID” chapter. Added “ASCII Control Codes” chart.
Entire Manual	Removed MX3-RFID specific information and instruction. Placed in “MX3-RFID User’s Guide” and “MX3-RFID Reference Guide”; released for publication September 2006. Changed “radio” to “wireless” or “client” in context, if suitable. Changed Chapter cross-references to match Chapter number changes.

Revision F, August 2006

Notices	Added WEEE statement. Added trademarks for RAM mounting products and Summit radio.
Chapter 1 – Introduction	Added caution for battery well vent location “Battery Well Vent Aperture”. Added key sequence to use if the touchscreen is not accepting taps or needs recalibration to “Getting Started | Troubleshooting”. Expanded instruction when using audio cable and headsets. Added voice accessories to “Accessories”. Added ROHS marker to Accessories. Removed USB A and USB B cable photos. Changed MX3-RFID IP rating from “dust and water protection enclosure rating of IEC 60529 compliant to IP55” to “...IP65”. Added “Entering the Multi AppLock Activation Key”. MX3P: Added “Features/Options for the MX3X Family”. Added “RFID and MX3P Devices and the MX3 Cradles”. Replaced “RFID Device and LXE Cradles” and “The MX3-RFID Device and Cradles” with “The Passive Vehicle Cradle”.

	Added new section titled “Connect External Power Supply to the MX3P”. Added information and Accessories for the MX3P mobile device.
Chapter 2 – Physical Description and Layout	Added “RTS/CTS Handshaking and the Serial Port”.
Chapter 3 – Power Supply	Corrected the following statement: “The MX3X is designed to achieve 8+ hours of continuous operation.” The statement is now correct.
Chapter 4 – System Configuration	Added intro information for JAVA option, RFTerm option, AppLock option and Wavelink Avalanche option to “Installed Software”. Added Summit radio to “Start Menu Program Options”. Added note to “Bluetooth Manager” and “Scanner/Main”: “Bluetooth Manager, Bluetooth service or options are not available for all MX3X devices or in all MX3X software releases.” Revised “About” section to include pre-installed font information. Revised “Date/Time” section. Revised “Password” section. Revised “Scanner” sections for new features. Added new sections to Utilities: “Enabling GrabTime”, “Configuring CapsLock Behavior”, “Configuring IPv6”, “Configuring Touch Panel Behavior”. Revised “LAUNCH.EXE” section for Summit radio and new features. Expanded “Reflash the Mobile Device” section to include Reflash TAG file process.
Chapter 5 – MX3-RFID	Removed Scanner tab explanations. Referred reader to Chapter 4, section titled “Scanner” for explanation and instruction. Changed MX3-RFID IP rating from IP55 to IP65.
Chapter 6 – AppLock	Added Multi Application AppLock instruction.
Chapter 7 – Wireless Network Configuration	Added Summit Client Utility. Separated chapter into four sections: Summit, Cisco, Symbol, and Certificates.
Appendix B – Technical Specifications	Added “Revision History”. Removed USB A and USB B cable photos from “Cable Specifications”. Added Summit radio technical specifications. Changed MX3-RFID IP rating from “dust and water protection enclosure rating of IEC 60529 compliant to IP55” to “...IP65”.
Entire Manual	Clarified differences between MX3X, MX3P and MX3-RFID mobile devices, cradles, batteries and chargers. Noted the replacement of SE923 scanner with SE955 scanner (July 2006) where applicable. Updated Figures to display LXE 2005 logo. Changed part numbers for cradles from 2381A002DESKCRADLE to MX3RA002DESKCRADLE and 2381A003VMCRADLE to MX3RA003VMCRADLE where applicable.

Revision E, November 2005

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

Revision D, April 2005

Front Page	Updated LXE Logo for 2005. Added “Microsoft Windows CE .NET Equipped” on cover page to separate this device from similar MX3 mobile devices.
Chapter 4 – System Configuration	Deleted “LXE RFID Config” from Start Menu. Added “RFID Configuration Utility” to Control Panel section. Added Avalanche “persist” keys to “Utilities” section “LAUNCH.EXE”.

Chapter 5 – MX3-RFID	Updated RFID Configuration Utility: • Added Filter, Firmware, and Format tabs to RFID Configuration Utility Panel. • 96 bit Class 1 tag support added. • EPC Tag Data Formatting added. • Added robust Read support.

Revision C, December 2004

Entire Manual	Noted differences between MX3X standard and the MX3-RFID device.
Chapter 1 – Introduction	Consolidated ActiveSync information and instructions. Corrected part numbers for MX3-RFID accessories.
Chapter 4 – System Configuration	Updated LAUNCH persistent storage information. Added Administration to control panel.
Chapter 5 – MX3-RFID	Added chapter specifically for the MX3X with an RFID module.
Chapter 6 – AppLock	Added chapter specifically for AppLock on MX3X and MX3-RFID devices.

Revision B, August 2004

Chapter 1 – Introduction	Corrected Accessories section “Cables for Cradle and MX3X Serial Ports”.
Chapter 2 – Physical Description and Layout	Updated “USB Host/Client Port” section. Added cable part number to “Storage Cradles”. Updated “Storage Cradles” and “Tethered Scanners” sections.
Chapter 4 – System Configuration	Updated Scanner Key graphic to show Field Exit option to Programmable Scan Keys for 5250 devices only.
Appendix B – Technical Specifications	Added section titled “Cable Specifications”.

Revision A, First Release, June 2004

Index

2

2nd key function....58

A

About
software, hardware, version, network IP....82
Accessibility settings....84
Accessories
Electrostatic Discharge....8
Install....8
Activation Key....235
Activation Key, AppLock Multiple Applications....18
ActiveSync....34
Backup Data Files....34
Cold Boot and Loss of Host Re-connection....35
Configure....31
Connect....33, 34
Create Comm Option....93
Explore....33
IR port transmission....30
Prerequisites....34
Troubleshooting....36
Use this cable....54
ActiveSync Help....30
ActiveSync Options....36
ActiveSync Setup Wizard....30
ActiveSync version 3.7....30
ACU....192
Add new Symbol connection....214
Add prefix and suffix control....148
Adding Codes to the Match List for EAN128 Barcodes....167
Admin Hotkey
AppLock....232, 241
Administration
AppLock from Control Panel....84
Administrator
Summit client utility....173
Advanced
Add Prefix....158
Add Suffix....158
Code Enable....164
COM port settings tab....156, 157
Keys tab....156
Scanner Control Characters Tab....163
Strip Leading and Strip Trailing....158, 159
Strip Leading, Strip Trailing....160
Translate control codes....158, 163
Advanced tab
Barcode processing....154
Send Key Messages and Wedge....155
Wedge....155
Allow Connection....96
Alt key function....59
API calls....117
Appearance
Scheme....89
Application Panel....234
AppLock
EUIE....235
Hotkey for Administrator....232
AppLock....73
Setup....229
AppLock
End-user mode....232
AppLock
Passwords....233
AppLock Activation Key....18
AppLock registry settings....254
Approved stylus....62
At Power On....95
Audio Cable
Install....28
Audio Jack, connect....16
Audio Volume settings....22
Authenticate using the EAP-TLS protocol, Cisco208
Auto hide taskbar....80
Avalanche Enabler installation....118
Avalanche Enabler update....123

B

Background and Window colors....89
Backlight Timer....20
Backlight timers....89
Backup Battery
Maintenance....67
Replacement....67
Time Limit....66
Backup Data Files....34
Barcode
Enable or Disable....141
Symbology Settings....143
Barcode data

edit buttons....146
Barcode manipulation....136
Barcode match list....146
Barcode processing overview....136
Barcode Scanner
Integrated....53
Tethered....53
Barcode Tab....141
Barrel connector, MX3P power jack....13
Barrel connector, power jack....12
Battery
Backup....67
Charge New....8
Charge or Discharge buttons for backup battery maintenance....85
Charging....44
Handling Safely....66
Lithium-Ion (Li-Ion)....44
Nickel Cadmium (NiCad)....44
Battery Auto Turn Off....89
Battery Chargers....68
Battery Compartment....9
Battery Life
Approximate....66
Battery pack label location....69
Battery tab....98
Battery voltage and status display....85
Battery Well Vent Aperture....6
Battery, charge before using....9
Baud Rate....101, 135
Bluetooth....85

C

Cable ends, identified....281
Cable Pinouts and Diagrams....281
Cable Specifications....281
Calibration....107
Caps mode function....59
CapsLock
Configuring....116
Caution
Fused Circuit Connection....13
Certificates....86
Root CA....217
User....221
Certificates are date sensitive....169, 194, 217, 221
Chapter reference....7
Character Recognition
Touch screen....79
Charger, battery....68
Charging Battery
Time Required....44
Check battery status....9, 65
Checking for Cisco PEAP supplicant....195
Cisco
PEAP Supplicant....195
Cisco Client....192
Cisco client Setup....192
Cisco profile parameters....193
Cisco wireless configuration....196
Cisco WPA
System Requirements....194
CISCO.CAB....195
CISCOMSCHAP.CAB....195
CISCOPEAP.CAB....195
Cleaning....63
Clear Contents of Document Folder....80
Clear persistent memory....134
Code ID transmission setting....142
COLDBOOT.EXE....117
Color Codes....15
Color displays....44, 62
Color displays and backlight timers....20
Color screen
Backlight....89
COM port settings tab....105, 140
COM Port Switching....52
COM ports....51
COM Ports....101, 135
Command line utilities....117
Command Prompt....78
Commit button
Config....174
Global Settings....179
Communication connect option....77
Communications....77
compact flash memor....43
Components
Back....4
Endcap....5
Config buttons....174
Config parameters
Summit....175
Configuration
AppLock....234
Single User AppLock....241
Configuring IPv6 for Symbol....213
Connect
ActiveSync....77
Connect Using....96
Control characters....149, 163
Control Panel
Single User AppLock....241
Control Panel options....81
Controls, Physical....50
Copied on startup....75
Copyrights....110
Core Logic....44
CPU....43
Cradle
Manual....3
Cradle for MX3-RFID and MX3P....39

Cradles, function....37
Create a dialup, direct, or VPN connection....93
Creating Custom Keymaps....60
Critical Suspend....66
  what happens when....67
Critical Suspend mode....49
Critical Suspend state....67
Ctrl Char Mapping....141, 149
Ctrl key function....58
Cumulative mode timers....98
Current Time....87
Custom ID
  parameters....151
Custom identifiers....150
Custom Identifiers....141
Custom Key Mapping....260
  and programmable scan buttons....261
Custom Key Maps....60

D

Data Bits....101, 135
Data entry....26
Daylight Savings....87
DB9-DB9 Serial Cable
  Tech Specs....54
Decimal - Hexadecimal Equivalent
  0 - 159....288
  160 - 255....289
DEFAULT.KEY....261
Delay....92
Desktop....74
Desktop cradle....38
  Power connection....38
  RS-232 connection....38
  Status Indicator....37
Device Name and description....110
Device status
  power levels displayed....99
DHCP....93
Diags buttons....178
Diags tab
  Summit....178
Dialup properties for dial up access....88
Digital certificates
  Date and Time....86
Disable slot now....97
Display
  adjust contrast....20
  Features....62
  Pixels....62
Display and scanner aperture cleaning....63
Display Backlight Timer....62
Display Backlighting
  and the Touchscreen....62
Display brightness and contrast....20
Display Contrast....20
Display Specifications....280
Display Timer....62
Document Conventions....7
Dual Serial Port endcap....51

E

EAP-FAST Authentication, Summit....186
EAP-TLS Authentication Configuration, Cisco....208
Edit the button parameters....57
Electrostatic Discharge....45
Enable Code ID....142, 150
Enable Code ID drop-down box....141
Enable internal scanner sound....138
Enable or Disable specific symbology....141
Enabler
  Adapter options....130
  and Summit clients....131
  communication....121
  Configuration....121
  Connection....124
  Execution....125
  File Menu....122
  Global options....132
  Icon on taskbar....130
  Network adapter status, link speed....132
  Passwords....122
  Scan Configuration....128
  Server Contact....126
  Settings Menu....123
  Shortcuts....129
  Startup and shutdown options....127
  Window options....128
Enabler installation....118
Enabler Uninstall Process....118
End user switching
  Hotkey....239
  Touch....239
Endcap Combinations....52
Endcaps and COM Ports....51
Enter key function....58
Entering Data....26
Environmental Specifications....283
Error Messages
  AppLock....245
Examples
  Barcode processing....153
  Control Code replacement....152
  raw scanner data and resulting data....153
Expand Control Panel....80
External Auto Turn Off....89
External Power Supplies....12

F

Factory Default, reset registry to 134
Failure
  Battery Pack 67
Features.....2
Field Exit 156
Field Exit key function 57
FLASH.....43
FTP Server, start and stop.....77
Function
  2nd Key 58
  Alt Key.....59
  Caps Mode 59
  Ctrl Key.....58
  Enter Key 58
  Field Exit Key 57
  Scan Key 58
  Shft Key 59
  Spc Key.....59

G

Getting Started.....8
Global Delay.....235
Global Key.....235
Global parameters
  Summit.....179
GrabTime utility 115

H

Handling Batteries 66
Handstrap, installation 10
Hardware
  Configuration 43
Hardware Specifications.....279
Hat Encoding and RFID 286
Headset 64
Headset data entry.....29
Headset, Install and Adjust 28
Hexadecimal - Decimal Equivalent
  0x00 to 0x9F 288
  0xA0 to 0xFF 289
Hip-Flip, Assembly.....11
Host Connection prerequisites 23
Hot Swapping Main Battery 66
Hotkey
  AppLock 236
  Single User AppLock.....242
HyperTerminal.....36

I

Icons
  Explorer, Internet 74
  My Computer 74
  My Documents.....74
  Recycle Bin 74
Idle Time.....89
IEC IP66, MX3X 283
Inbox
  Outlook 78
InfraRed Port 64
Input Panel.....26, 90
Insert battery pack into charging pocket 68
Insert Main Battery 9
Installing Cisco client drivers 194
Internet Explorer
  AppLock 235
  Single User AppLock.....242
Internet Explorer
  Network card and ISP required 78
Internet Options
  CE 5.0 91
  CE NET 4.2.....90
IP Address
  DHCP.....93
  Static 93
IPv6 Broadcast Messages 213
IPv6 configuration 116
IR operating envelope.....64
IR Port.....64

J

JEM-CE 72

K

Keyboard
  Onscreen only 90
Keyboard 0409.....92
KEYCOMP.EXE 260
Keymaps 255
Keypad and entering data 26
Keypad Shortcuts.....17, 59
Keys tab 104

L

Language and fonts.....83
LAUNCH.EXE.....112
LEAP without WPA Authentication, Summit 185
LEDs
  2nd function.....61

ALT function 61
BATT B function 61
BATT M function 61
CAPS function 61
CHGR function 61
CTRL function 61
on keypads,location 61
SCNR function 61
SHFT function 61
STAT function 61
Levels, Logging
Single User AppLock 244
Li-Ion battery life 9
List configured ActiveSync connections 96
Lithium-Ion (Li-Ion) 65
Location, Components 4
Location, Ports 5
Logging
AppLock 238
Loss of Host Re-connection 35
Low Battery Warning 66
LXE Security Primer 169
LXE_MX3X 73
LXEAPI.LIB 117

M

MAC Address 83
Main 101
Main Battery
and Critical Suspend state 66
Hot Swapping 66
Main Battery Pack 66
Main Battery Power Failure 67
Main tab
Summit 172
Maintenance, required
Backup Battery 67
Manuals 40
Match list 146
rules 147
Match List rules 147
Media Player 78
Memory
allocate for programs or storage 109
Memory installed 109
Menu Options
Start 76
Microphone adjustment 28
mode
Block 161, 162
Key Message 161, 162
Mode Key Functions 59
Modes
AppLock 232
Modify the Registr 83
Multi AppLock 18
Multi AppLock Activation key 18
Multi-Application AppLock 230
MX3P
description 1
MX3P Power Jack, attach power supply 13
MX3-RFID
description 1
Manuals 3
MX3-RFID, MX3P and Cradles 29, 39
MX3X
Manuals 3
My Computer
Folders 75

N

NETWLAN1 Properties 215
Network Card
MAC Address 83
Network Specifications
Cisco 285
Summit 285
Symbol 285
New Battery 8
NiCad 65
NiCAD
50 mAh 44
Nickel-Cadmium (NiCad) 65
No Security
Summit 183

O

Off Mode 49
ON Mode characteristics 47
Operating Temperature 283
Optional Software
AppLock 73
JAVA 72
RFTerm 73
WaveLink Avalanche Enabler 73
Overview 1

P

Parity 101, 135
Passive Pen 62
Passive vehicle cradle 37
Password
Single User AppLock 243
Password 95
Passwords
AppLock 233

AppLock Save As 238
Passwords lost at cold boot 117
PC Card 45
Storage 25
PC card slots 24
PCMCIA 45
Slots 0, 1 and 2 97
PCMCIA Slots 45
PEAP GTC Authentication Configuration 202
PEAP MSCHAP Authentication, Summit 187
PEAP/MS-CHAP Authentication Configuration 199
PEAP-GTC 195
PEAP-MSCHAP for WPA 187
Pen Stylus 10, 17, 62
Pen Stylus and data entry 26
Persist RAM Base Files 108
Persistant Memory Drive
IPSM 43
Physical Specifications 279
Pin 9 Power 135
Popup blocker 91
Power Button 50
Power button, location 16
Power Jack, attach power supply 12
Power level used, devices 99
Power Modes diagram 46
Power Port 1 while asleep 103, 138, 155
Power Properties 98
Power slot during sleep 97
Power Supply 65
Battery Packs 44
Power Supply Specifications 283
Power Supply, Cigarette Lighter Adapter 70
Power Supply, International AC/DC 70
Power Supply, US AC/DC 70
Prefix and Suffix 159, 161
Pre-loaded Files 71
Preserved upon reboot 75
Privacy, Internet 91
Processing order 143
Programmable keys
Setup 104, 139, 156
Prompt
Command 78
Protective Film for Touchscreen 63
PrtScrn.exe 117

Q

Quick Start Instructions 8
QWERTY keypad 58

R

Rate 92
Recalibrate 19
Recalibration 107
Reflash
directions 134
keypress directions 133
with REFLASH.TAG 134
REFLASH.TAG 134
REGEDIT.EXE 115
REGLOAD.EXE 115
Remote desktop connection 79
Remove user installed programs 100
Repeat 92
Replacement 149
REPLLOG.EXE 36
Restart, reboot 16
Revision History
MX3X Reference Guide 291
Revision Level
Cisco 194
Summit 170
RFID Module 51
RFTerm 73
Root CA Certificates
Generating 217
Installing on mobile device 219
RS-232 Pinouts 53, 55
Rules
match list 147
Match list 147

S

Scan
Good and Bad Scan sounds 111
Scan buttons
and tethered scanners 29, 56
Scan Buttons 57
Scan buttons and tethered scanners 103, 139, 155
Scan buttons and the SCNR LED 57
Scan key function 58
Scan Keys
Left and Right 135
SCANBAD.WAV 111
ScanCodeLeft and ScanCodeRight 105, 139, 156
SCANGOOD.WAV 111
Scanner
Manual 3
Scanner configuration update and the Scan LED 101
Scanner Control Characters Tab 149
Scanner Control Menu 135
Scanner Keys tab 139
Scanner LED, functioning 27
Scanner, factory defaults 101
Scanning and data entry 27
Schemes tab 98, 99
Screwdriver

Phillips, for handstrap 10
SE923 scan engine 27
Security
Single User AppLock 242
Security options, supported 169
Security Panel
AppLock 236
Security Password
AppLock 237
Security, Internet 91
Send Key Messages and Wedge 103, 138
Serial Cable
for ActiveSync 54
Set the double-click sensitivity for stylus taps 93
Settings Menu 123
Adapters tab 130
Connection tab 124
Display tab 128
Execution tab 125
Scan Config tab 128
Server Contact tab 126
Shortcuts tab 129
Startup Shutdown tab 127
Status tab 132
Setup
AppLock 229
Shift key function 59
Show Clock 80
Shutdown time limits 66
Single Application AppLock 231
Soft Keyboard 90
Software and Files 71
Software Load 72
Software version 83
Sounds 111
Space key function 59
Speaker 64
SSID 175
Standard Range Scanner 51
Start Menu 76
Shutdown 74
Start Menu program options 76
Static IP Address 93
Status
Single User AppLock 244
Status Panel
AppLock 237
Stop Bits 101, 135
Stop the Enabler Service 119
Storage Manager
devices 106
Storage Temperature 283
Stored certificates 86
Storing PC Cards 25
Strip Code ID 150
Strip leading and trailing 145
Strip Leading and Trailing 135
Strip Leading, Strip Trailing 161
Stylus 17, 62
Stylus and data entry 26
Stylus Clip 10
Stylus properties 107
Stylus sensitivity 107
Suffix and Prefix 159, 161
Summit
Client configuration 170
EAP-FAST Authentication 186
LEAP without WPA Authentication 185
No Security 183
PEAP MSCHAP Authentication 187
WEP keys 184
WPA LEAP Authentication 189
WPA PSK Authentication 190
Summit client utility 170
Summit client utility (SCU)
Config tab 174
Diags tab 178
Global Settings tab 179
Status tab 177
Suspend button 74
Suspend Timer 21
Switching
COM ports 51
Symbol ID
and EV-15 Imager 142
Symbol profile parameters 213
Symbol Wireless Information 214
Symbology setting parameters 144
Symbology Settings 141
Synchronize desktop computer with the MX3X
ActiveSync 30
System
General 109
Memory 109
System Configuration 71
System Hardware Configuration 43
System Idle Timer 21
System Requirements, Cisco WPA 194

T

Taskbar 80
TCP/IPv6 information 213
Terminal Emulator, connect 23
Tethered Scanner and a Cradle 39
Tile 89
Time Zone 87
Timers
User, System, Suspend 21
Touch Screen 10, 17, 62
Touch Screen and data entry 26
Touch Screen and Keypad Shortcuts 17, 59
Touch screen calibration 19

TouchDisable....116
Touchscreen....62
Transcriber....79
Transflective Display....44
Translate All....149, 163
Translate control codes....149
Transmissive Display....44, 62
Troubleshooting
AppLock Password....233
Multi-Application AppLock....240
Troubleshooting
ActiveSync....36
Startup....8
Touchscreen....116
Unsuccessful scan....27

U

User Certificate on the MX3X....226
User Certificates
Generating....221
User Idle Timer....21
User-specific application version information....82
Utilities....112
Regedit....115

V

Vehicle 12VDC Power Cable....15
Vehicle 24/72VDC Power Supply....14
Vehicle cradle
RS-232 connection....38
Vehicle mount cradle
Components....38
Power connection....38
Video Subsystem
Display Characteristics....44
View
Display....62
Virtual Key, change....105, 156
Virtual Key, changing....139
Virtual Keyboard....90
VK_Code List....278
Volume
adjust audio volume....22
Volume and Sounds....111

W

Wake the device from Suspend....74
Wake up action for display backlight....47, 48
WARMBOOT.EXE....115
Warning
Low Battery beeps....66
Wavelink Avalanche Enabler....73
Wavelink Avalanche Enabler installation....118
WAVPLAY.EXE....115
Wedge....103, 138
Wedge, Barcode....135
WEP Keys
Cisco....193
Summit....184
Windows CE on-line Help....115
Windows CE. NET on-line Help....71, 74
Windows Explorer....79
Windows version....109
Wireless Network Configuration....169
Wireless Network Connection screen....197
Wireless Security
Summit Client....182
Wiring Color Codes....15
WPA LEAP
Cisco....205
WPA LEAP Authentication, Summit....189
WPA PSK Authentication, Summit....190
WPA PSK Configuration, Cisco....212

Z

Zero Config Utility, Microsoft....196