

MX8

Hand-Held Computer

Microsoft® Windows® Mobile 6.1 Operating System

Reference Guide

Disclaimer

Honeywell International Inc. ("HII") reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

© 2009-2012 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

RFTerm is a trademark or registered trademark of EMS Technologies, Inc. in the United States and/or other countries.

Microsoft® Windows, ActiveSync®, MSN, Outlook®, Windows Mobile®, the Windows logo, and Windows Media are registered trademarks or trademarks of Microsoft Corporation.

Marvell® is a registered trademark of Marvell Technology Group Ltd., or its subsidiaries in the United States and other countries.

Summit Data Communications, the Laird Technologies Logo, the Summit logo, and "Connected. No Matter What" are trademarks of Laird Technologies, Inc.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Hand Held is a trademark of Hand Held Products, Inc., a subsidiary of Honeywell International.

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

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

Acrobat® Reader © 2012 with express permission from Adobe Systems Incorporated.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, please refer to www.honeywellaidc.com/patents.

Limited Warranty

Refer to www.honeywellaidc.com/warranty_information for your product's warranty information.

Table of Contents

Chapter 1: Introduction	1-1
Components	1-2
Front	1-2
Back	1-3
Keypads	1-4
32 Key Triple-Tap Keypad	1-4
32 Key Alpha-Mode Keypad	1-5
Scanner / Imager Aperture	1-6
Handle	1-6
Handstrap	1-6
I/O Port and Cables	1-7
Startup Help	1-8
Device Unlocked / Device Locked	1-8
Reboot Sequences	1-9
Suspend / Resume	1-9
Cold Boot / Restart	1-9
Clean Boot / Reset	1-9
Chapter 2: Hardware	2-1
System Hardware	2-1
802.11 b/g and a/b/g Wireless Client	2-1
Central Processing Unit	2-1
System Memory	2-1
Internal Mini SD Memory Card	2-1
Video Subsystem	2-2
Power Supply	2-2
COM Port	2-3
RS232 Serial Port	2-3
USB Client Port	2-3
Audio Headset Connection	2-3
Audio Support	2-3
Scanner / Imager Port	2-4
Bluetooth EZPair	2-4
Keypads	2-5
Using the Triple-Tap Keypad	2-5
Using the Alpha-Mode Keypad	2-6
Standard Keys	2-7
Function Keys	2-8

Sticky Keys.....	2-8
Mode Key Functions.....	2-9
Power Key.....	2-9
Power States.....	2-9
Display.....	2-10
Display Backlight Timer.....	2-10
LED Indicators.....	2-11
System Status LED.....	2-11
Scan Status LED.....	2-11
Alpha Mode LED.....	2-12
Chapter 3: Power	3-1
Power Modes.....	3-1
On Mode.....	3-1
Suspend Mode.....	3-1
Off Mode.....	3-1
Batteries.....	3-2
Checking Battery Status.....	3-2
Main Battery Pack.....	3-2
Battery Hotswapping.....	3-2
Low Battery Warning.....	3-3
Backup Battery.....	3-3
Handling Batteries Safely.....	3-3
Chapter 4: Software	4-1
Operating System.....	4-1
Windows Mobile 6.1.....	4-1
Software Development.....	4-1
Clearing Registry Settings.....	4-1
Installed Software.....	4-2
Software Load.....	4-2
Software Backup.....	4-2
Version Control.....	4-3
Boot Loader.....	4-3
Startup Folders and Launch Sequences.....	4-3
Today Screen.....	4-4
Start Menu.....	4-5
Configurable Today Screen Listing.....	4-5
Date.....	4-5
Device Unlocked / Device Locked.....	4-5
Notification Bar.....	4-6

Status Icons.....	4-7
Soft Keys.....	4-7
Start and Program Menus.....	4-8
Installed Programs.....	4-9
Internet Explorer.....	4-9
Office Mobile Applications.....	4-10
ActiveSync.....	4-10
AppLock (Option).....	4-10
Summit.....	4-10
SCU (Summit Client Utility).....	4-10
Certs.....	4-10
Windows Media Player.....	4-10
Bluetooth (Option).....	4-11
RFTerm (Option).....	4-11
Status Popup.....	4-12
HSM Connect.....	4-12
GrabTime.....	4-12
Synchronize with a local time server.....	4-13
Enhanced Launch.....	4-13
RegLoad.....	4-13
RegEdit.....	4-13
Remote Desktop.....	4-14
Set Remote Desktop Mobile Options.....	4-14
Connect to a Remote Server.....	4-15
Installing Applications.....	4-16
Preparation.....	4-16
Package File Installation.....	4-16
Installing Applications Help.....	4-19
Settings.....	4-21
Personal Panels.....	4-23
Buttons.....	4-23
Program Buttons.....	4-23
Up/Down Control.....	4-24
Input.....	4-25
Input Method.....	4-25
Word Completion.....	4-26
Options.....	4-27
Lock.....	4-28
Password.....	4-28
Hint.....	4-29

Menus.....	4-30
Owner Information.....	4-31
Sounds & Notifications.....	4-33
Sounds.....	4-33
Notifications.....	4-34
Today.....	4-35
System Panels.....	4-36
About.....	4-36
Version.....	4-36
Device ID.....	4-37
Copyrights.....	4-38
About MX8WM.....	4-39
Software.....	4-39
Hardware.....	4-40
Versions.....	4-40
Network IP.....	4-41
Administration - for AppLock.....	4-42
Introduction.....	4-42
Setup a New Device.....	4-43
Administration Mode.....	4-44
End User Mode.....	4-45
Passwords.....	4-46
AppLock Password Help.....	4-46
End-User Switching Technique.....	4-47
Using a Stylus Tap.....	4-47
Using the Switch Key Sequence.....	4-47
Hotkey (Activation hotkey).....	4-47
End User Internet Explorer (EUIE).....	4-48
Application Configuration.....	4-48
Application Panel.....	4-49
Launch Button.....	4-51
Auto At Boot.....	4-52
Auto Re-Launch.....	4-53
Manual (Launch).....	4-54
Match.....	4-54
Allow Close.....	4-54
Security Panel.....	4-55
Setting an Activation Hotkey.....	4-55
Setting a Password in the Security Panel.....	4-56
Options Panel.....	4-57

Status Panel.....	4-58
View.....	4-58
Log.....	4-59
Save As.....	4-59
AppLock Help.....	4-59
AppLock Error Messages.....	4-60
Backlight.....	4-67
Battery Power.....	4-67
External Power.....	4-68
Brightness.....	4-69
Bluetooth.....	4-70
Initial Configuration.....	4-72
Subsequent Use.....	4-72
Discover.....	4-73
Stop Button.....	4-73
Bluetooth Devices.....	4-74
Clear Button.....	4-74
Bluetooth Device Menu.....	4-75
Bluetooth Properties.....	4-76
Settings.....	4-77
Turn On Bluetooth.....	4-77
Options.....	4-77
Reconnect.....	4-79
Options.....	4-79
About.....	4-81
Easy Pairing and Auto-Reconnect.....	4-82
Bluetooth Bar Code Reader Setup.....	4-83
MX8 with Label.....	4-84
MX8 without Label.....	4-84
Bluetooth Reader Beep and LED Indications.....	4-85
Bluetooth Printer Setup.....	4-85
Certificates.....	4-86
Personal.....	4-86
Intermediate.....	4-87
Root.....	4-88
Clock & Alarms.....	4-89
Time.....	4-89
Alarms.....	4-90
More.....	4-91
Customer Feedback.....	4-92

Encryption.....	4-93
Error Reporting.....	4-94
External GPS.....	4-95
Access.....	4-96
License Manager.....	4-97
Managed Programs.....	4-98
Memory.....	4-99
Main.....	4-99
Storage Card.....	4-100
MX8WM Options.....	4-101
Communication.....	4-101
Misc.....	4-102
Status Popup.....	4-103
Power.....	4-104
Battery.....	4-104
Advanced.....	4-105
Regional Settings.....	4-106
Remove Programs.....	4-108
Screen.....	4-109
Alignment.....	4-109
Clear Type.....	4-110
Text Size.....	4-111
Task Manager.....	4-112
Windows Update.....	4-113
Connections Panel.....	4-114
Beam.....	4-114
Connections.....	4-115
Domain Enroll.....	4-116
Wi-Fi (Network Adapters).....	4-117
Wi-Fi (Network Access).....	4-119
Wireless.....	4-119
Network Adapters.....	4-120
Wireless Manager.....	4-121
Wi-Fi.....	4-121
Bluetooth.....	4-122
ActiveSync.....	4-123
Introduction.....	4-123
Initial Install.....	4-124
Install ActiveSync on Desktop/Laptop.....	4-124
Serial Connection.....	4-124

USB Connection.....	4-124
Connect – Initial Install Process.....	4-125
Synchronize Files.....	4-125
MX8 and PC Partnership.....	4-125
Serial Port Transfer.....	4-125
USB Transfer.....	4-125
Explore.....	4-125
Disconnect.....	4-126
Cold Boot and Loss of Host Re-connection.....	4-126
ActiveSync Help.....	4-127
Configuring with HSM Connect.....	4-128
Install HSM Connect.....	4-128
Using HSM Connect.....	4-130
Chapter 5: Data Collection.....	5-1
Data Processing Overview.....	5-3
Main Tab.....	5-4
Continuous Scan Mode.....	5-5
COM1 Tab.....	5-6
Notification Tab.....	5-7
Vibration.....	5-8
Data Options Tab.....	5-9
Enable Code ID.....	5-10
Options.....	5-10
Buttons.....	5-11
Symbology Settings.....	5-12
Clear Button.....	5-12
Advanced Button.....	5-13
Processing Order.....	5-14
Enable, Min, Max.....	5-14
Strip Leading/Trailing Control.....	5-16
Barcode Data Match List.....	5-17
Barcode Data Match Edit Buttons.....	5-18
Match List Rules.....	5-18
Add Prefix/Suffix Control.....	5-19
Symbologies.....	5-20
AIM Symbologies.....	5-21
HHP Symbologies.....	5-22
Advanced (Hand Held Products Only).....	5-23
OCR Symbology.....	5-31

OCR Template Examples.....	5-32
OCR Checksum Calculation.....	5-32
HHP Properties.....	5-33
Ctrl Char Mapping.....	5-35
Translate All.....	5-35
Custom Identifiers.....	5-37
Control Code Replacement Examples.....	5-39
Bar Code Processing Examples.....	5-39
Length Based Bar Code Stripping.....	5-41
Processing Tab.....	5-43
About Tab.....	5-44
Hat Encoding.....	5-45
Chapter 6: Launch Utility.....	6-1
Introduction.....	6-1
Registry Based Launch Items.....	6-1
Launch Startup options.....	6-3
Example.....	6-3
Script Based Launch Items.....	6-4
Enhanced Launch Utility Use.....	6-4
File Names.....	6-5
Command line structure.....	6-5
Comments.....	6-5
Commands Supported by Launch.....	6-6
Launch Error Messages.....	6-19
Example Script File.....	6-21
Chapter 7: Wireless Network Configuration.....	7-1
Introduction.....	7-1
Important Notes.....	7-1
Summit Client Utility.....	7-2
Help.....	7-2
Summit Tray Icon.....	7-3
Using Windows Mobile Wireless Manager.....	7-4
Create a New Network Connection.....	7-4
Edit a Network Connection.....	7-6
Switch Control to SCU.....	7-6
Main Tab.....	7-7
Auto Profile.....	7-8
Admin Login.....	7-9
Profile Tab.....	7-10

Buttons.....	7-11
Profile Parameters.....	7-12
Status Tab.....	7-14
Diags Tab.....	7-15
Global Tab.....	7-16
Custom Parameter Option.....	7-17
Global Parameters.....	7-18
Sign-On vs. Stored Credentials.....	7-22
How to: Use Stored Credentials.....	7-22
How to: Use Sign On Screen.....	7-23
Windows Certificate Store vs. Certs Path.....	7-25
User Certificates.....	7-25
Root CA Certificates.....	7-25
Configuring the Profile.....	7-27
No Security.....	7-28
WEP.....	7-29
LEAP.....	7-31
PEAP/MSCHAP.....	7-33
PEAP/GTC.....	7-36
WPA/LEAP.....	7-39
EAP-FAST.....	7-41
EAP-TLS.....	7-43
WPA PSK.....	7-46
Certificates.....	7-48
Generating a Root CA Certificate.....	7-49
Installing a Root CA Certificate.....	7-53
Generating a User Certificate.....	7-54
Exporting a User Certificate.....	7-57
Installing a User Certificate.....	7-59
Chapter 8: Keymaps.....	8-1
32 key Numeric-Alpha Keymap.....	8-1
32 key Alpha-Mode Keymap.....	8-7
Chapter 9: Technical Specifications.....	9-1
Dimensions and Weight.....	9-2
Environmental Specifications.....	9-2
Network Card Specifications.....	9-3
Summit 802.11 b/g.....	9-3
Summit 802.11 a/b/g.....	9-3
Bluetooth.....	9-3

Pinout I/O Port	9-4
AC Wall Adapter.....	9-5
Chapter 10: Technical Assistance	10-1

Chapter 1: Introduction

The MX8 is a rugged, portable, hand-held Microsoft® Windows® Mobile® 6.1 equipped computer capable of wireless data communications. The MX8 can transmit information using an 802.11 network card and it can store information for later transmission through an RS232 or USB port.

The MX8 is vertically oriented and features backlighting for the display. The touch-screen display supports graphic features and Windows icons that the Windows Mobile operating system supports. The keypad is available in a 32-key numeric-alpha triple-tap version and a 32-key Alpha mode version.

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

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

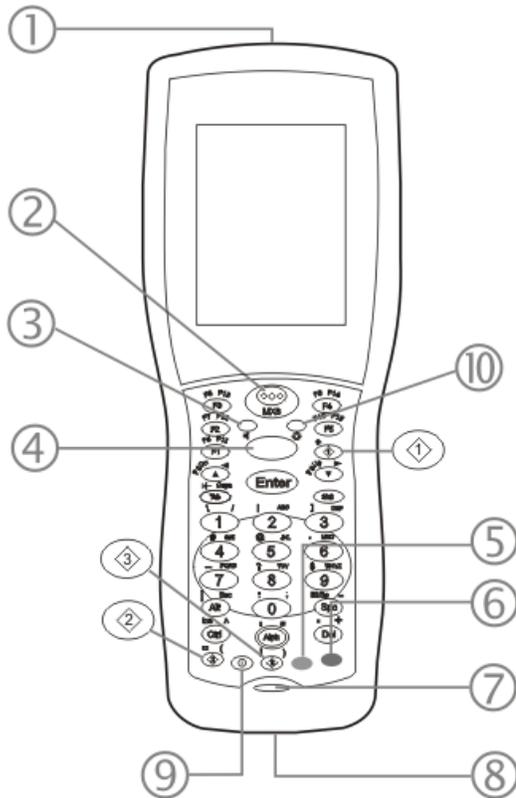
The MX8 is powered by a 3000 mAh Lithium-Ion main battery pack and an internal Ni-MH backup battery.

- If the MX8 has AppLock installed, please refer to [AppLock](#) for setup and processing information.
- Wireless configuration and security parameters are described in detail in [Wireless Network Configuration](#).
- Review the [Unlock](#) process before locking the MX8.

Note: Contact [Technical Assistance](#) for upgrade availability if your application or control panels are not the same as the application or control panels presented in this guide.

Components

Front

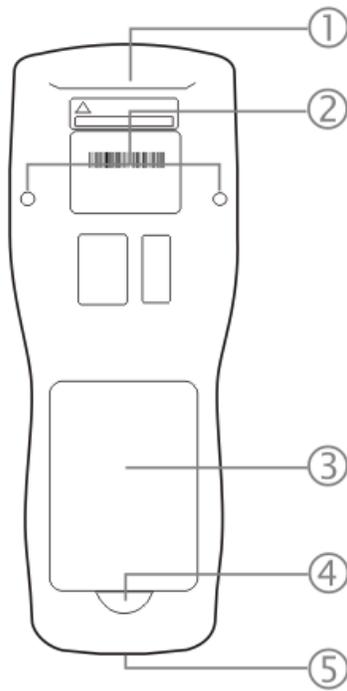


1. Scanner/Imager Aperture
2. Speaker
3. System Status LED
4. Scan Button
5. Orange Key (Sticky Key)
6. Blue Key (Sticky Key)
7. Scan Status LED
8. Cable Port
9. On / Off Button
10. Alpha Lock LED

Diamond Keys



Back

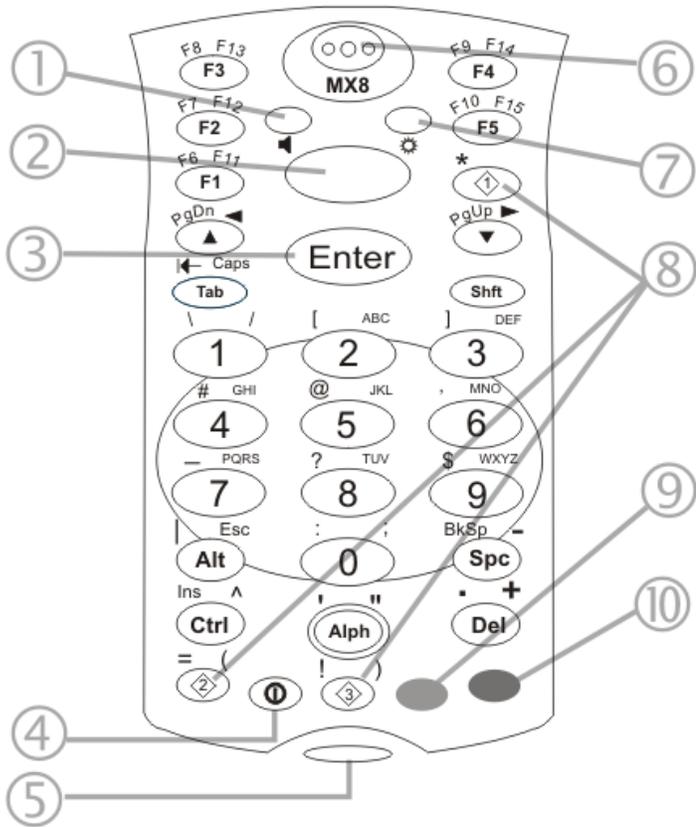


1. Scanner/Imager Aperture
2. Trigger Handle Attach Points
and
Handstrap Retainer Bracket Attach Points
3. Main Battery
4. Battery Fastener
5. Cable Port

Note: The touch screen stylus can be tethered to the [handstrap](#) or the [trigger handle](#).

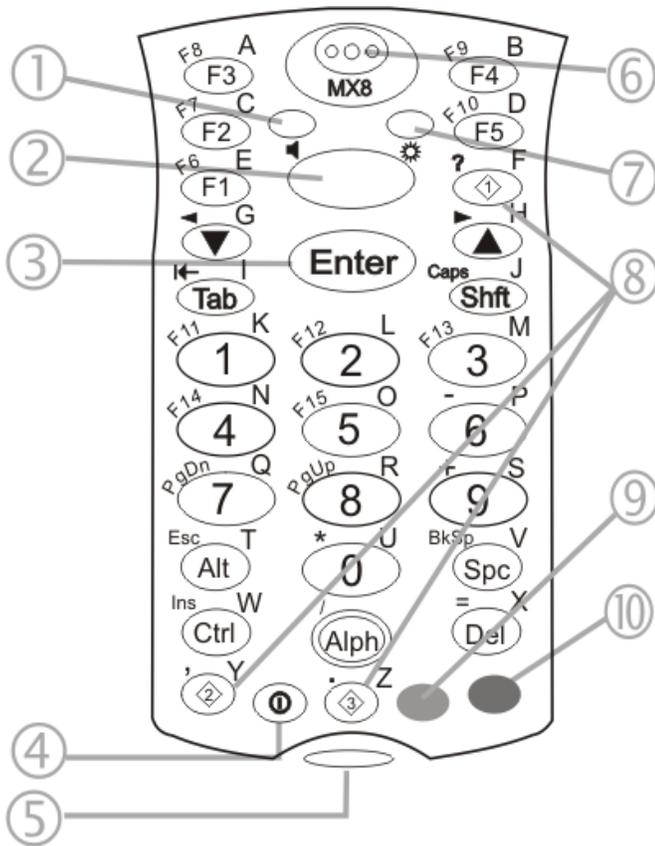
Keypads

32 Key Triple-Tap Keypad



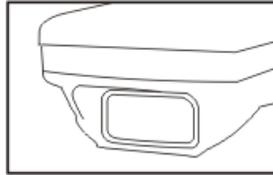
1. System Status LED
2. Scan Button
3. Enter Button
4. On / Off Button
5. Scan Status LED
6. Speaker
7. Alpha Status LED
8. Diamond Keys
9. Orange Key (Sticky)
10. Blue Key (Sticky)

32 Key Alpha-Mode Keypad



1. System Status LED
2. Scan button
3. Enter Button
4. On / Off Button
5. Scan Status LED
6. Speaker
7. Alpha Status LED
8. Diamond Keys
9. Orange Key (Sticky)
10. Blue Key (Sticky)

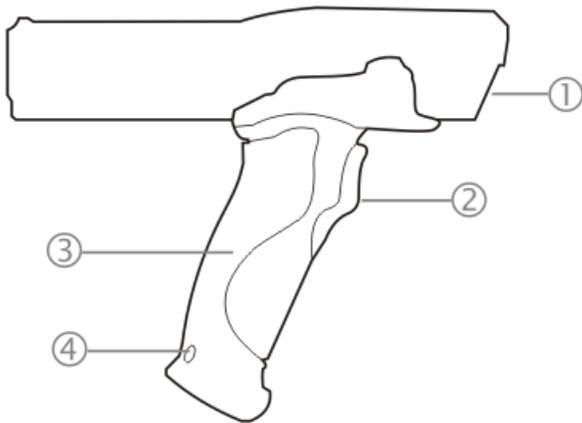
Scanner / Imager Aperture



Caution: Never stare directly into the beam aperture.

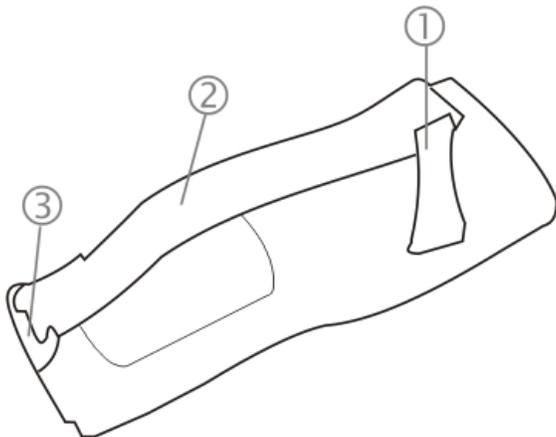
If [Continuous Scan Mode](#) has been enabled (default is disabled), the laser is always on and decoding. Caution: Laser beam is emitted continuously. Do not stare into the laser beam.

Handle



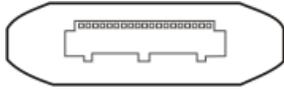
1. Imager / Scanner Aperture
2. Trigger
3. Handle
4. Tether Attach Point

Handstrap

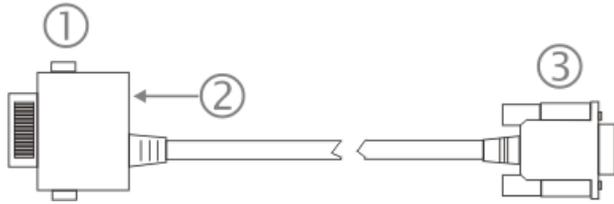


1. Handstrap Retainer Bracket
2. Handstrap
3. Handstrap Clip

I/O Port and Cables

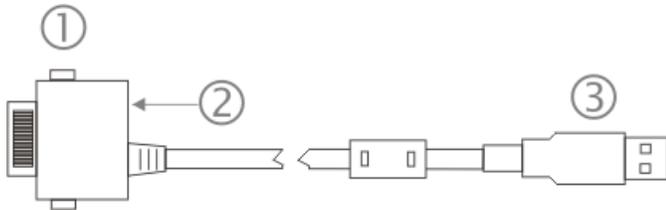


Input/Output Port



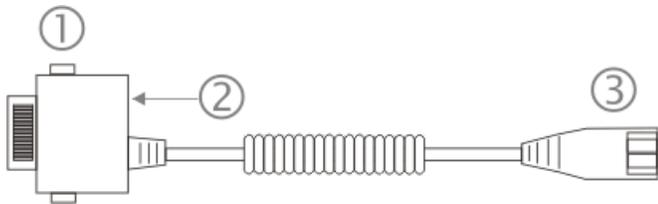
Cable: Multipurpose RS232 and Power
MX8055CABLE

1. To MX8 I/O port
2. Attach A/C Adapter barrel connector
3. To RS232 device



Cable: Multipurpose USB and Power
MX8051CABLE

1. To MX8 I/O port
2. Attach A/C Adapter barrel connector
3. To USB device



Adapter/Cable : Audio
MX8060CABLE

1. To MX8 I/O port
2. Attach A/C Adapter barrel connector
3. To audio device



AC/DC Adapter for MX8 and MX8 Desktop Cradles
MX8301PWRSPLY (US)
MX8302PWRSPLY (WW)

1. To power port
2. To adapter
3. To wall plug

Startup Help

Can't change the date/time or adjust the volume.	AppLock is installed and may be running in User Mode on the MX8. AppLock user mode restricts access to the control panels.
Touch screen is not accepting stylus taps or needs recalibration.	See Also: "Screen" when the touch screen needs recalibration, or if the touch screen is not accepting stylus taps, hold down the Blue key, the Scan key and the Power key until the screen blanks. Release the keys and the MX8 will coldboot.
MX8 seems to lockup as soon as it is rebooted.	There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, and Bluetooth relationships establish or re-establish. When an application begins, the MX8 is ready for use.
New MX8 main batteries don't last more than a few hours.	New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the MX8 is always 'on' even when in the Suspend state and draws battery power at all times.

Note: Base Laser Scanner, 955E does not support aim mode. Any attempt to adjust the aiming beam using 955 programming bar codes will fail. The Base Laser scanner does not decode Codablock, Code93i or Telepen symbologies.

Device Unlocked / Device Locked

The MX8 can be locked manually by tapping *Device unlocked* on the Today screen. By default, this option is included on the Today screen. Care should be taken to not accidentally tap this area of the Today screen.

Lock option can be removed from the Today screen by selecting [Start > Settings > Personal > Today > Items](#) tab.

The MX8 can also be configured to Lock automatically after a defined period of inactivity. This setting is accessed by [Start > Settings > Personal > Lock > Password](#) tab. By default, this option is Disabled.

When the MX8 is locked, the Today screen displays Device locked.

Click **Unlock** at the lower part of the screen:

- If there is no password or PIN set, click Unlock on the next screen to unlock the MX8. The MX8 is returned to normal operation.
- If there is a password or PIN set, enter the password or PIN and click Unlock. If several unsuccessful attempts are made, the MX8 may be configured to display a password hint.

The password and hint are configured by selecting [Start > Settings > Personal > Lock > Password](#) and Hint tabs.

Reboot Sequences

When the Windows Mobile Today panel is displayed or an application begins, the power up sequence is complete. If you have previously saved your settings, they will be restored on reboot. Application panel changes are saved when ok is tapped on an application properties panel.

During the processes that follow there may be small delays while the wireless client connects to the network and Bluetooth relationships establish or re-establish.

Suspend / Resume

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

or

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

Cold Boot / Restart

Temporary data not saved is lost. All programs are re-launched, programs installed from CAB files are reinstalled. Previously saved user settings are restored. Restart may also be called cold boot. Hold down the Blue key, the Scan key and the Power key until the screen blanks. Release the keys and the MX8 cold boots.

Be sure to press the Scan key not the Enter key. Pressing the Enter key begins a suspend/resume function instead of a cold boot function.

Clean Boot / Reset

Important – Because of the extreme nature of resetting the MX8 to factory default settings, this process should only be used as an emergency procedure and Suspend/Resume or cold boot should be used whenever necessary. When re-imaging, the Mini-SD Flash card must be formatted as FAT16 and be less than 1GB.

To reset **all** MX8 configuration to factory defaults:

1. Hold down the Blue + Scan + Power keys at the same time. After the keypress, the display turns solid white. Be sure to press the Scan key, not the Enter key.
2. Release the keys and immediately press and hold the Enter + Scan keys. After the keypress, the display turns dark. (If these keys are not pressed immediately the MX8 performs a Cold Boot. Wait until the MX8 boots and try again.)
3. Release the Reset keys. A “returning to factory defaults” message is displayed at the bottom of the display. If the message does not appear, please try again.

When all programs have finished loading, the Windows Mobile 6.1 Welcome screen is displayed. If prompted, tap the touch screen to set up your Windows Mobile-based device.



Chapter 2: Hardware

System Hardware

802.11 b/g and a/b/g Wireless Client

The MX8 has an 802.11 network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Adjusting power management on the network card is set to static dynamic control. WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is a 520MHz Marvell Xscale PXA-27X CPU. The operating system is Microsoft® Windows® Mobile® 6.1. The OS image is stored on an internal flash memory card and is loaded into DRAM for execution.

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

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

System Memory

The CPU configuration supports 128MB Strata Flash, 128MB SDRAM. The system optimizes for the amount of SDRAM available.

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

Internal Mini SD Memory Card

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

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

Video Subsystem

The touch screen is a 2.8" (7.1 cm) diagonal viewing area, ¼ VGA 320 by 240 pixel TFT Transmissive Active Color LCD. Backlighting is available. The turn-off timing is configured through the [Start > Settings > System > Backlight](#) icon. The display controller supports Microsoft CE 5.0 graphics modes.

A touch screen allows mouse functions (tapping on the display or signature capture) using a stylus. The touch screen has an actuation force with finger less than 100 grams. The color display has an LED backlight and is optimized for indoor use.

The display appears black when the MX8 is in Suspend Mode.

Power Supply

The MX8 uses two batteries for operation.

- **Main Battery** A replaceable 3000 mAh Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while in the MX8 when the device is connected to the optional external MX8 AC/DC power source. The main battery pack can be removed from the **MX8** and inserted in the MX8 Multi-Charger which simultaneously charges up to four battery packs in five hours. The MX8 status indicator is illuminated when the backup battery is being charged by the main battery pack. A new main battery pack can be fully charged in 5 hours when it is in an MX8 connected to AC power and 5 hours when it is in the MX8 multicharger.
- **Backup Battery** An internal 160mAh Nickel Metal Hydride (Ni-MH) battery. The backup battery is recharged directly by the MX8 main battery pack. Recharging maintains the backup battery near full charge at all times. When the backup battery is fully drained, it may take up to 5 hours to recharge. The capability to discharge the backup battery is provided to allow the user to condition the battery in order to recover full battery capacity. The backup battery must be replaced by qualified service personnel. The battery has a minimum 2 year service life.

Note: An uninterrupted external power source (wall AC adapters) transfers power to the MX8's internal charging circuitry which, in turn, recharges the main battery and backup battery. Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.

COM Port

The MX8 has one 20-pin multifunction I/O port that can be configured by the user. Tethered scanners connected to the MX8 I/O port are not supported on the MX8.

Note: The MX8 AC Power Adapters (MX8301PWRSPPLY and MX8302PWRSPPLY) are only intended for use with the MX8 multi-purpose cables and the MX8 Desktop Cradle.

RS232 Serial Port

Configured as COM1. Bi-directional full duplex and supports data rates up to 115 Kb/s. The port does not have RI or CD signals nor does it support 5V switchable power on pin 9 for tethered scanners. The serial port driver supports full duplex communications over the serial port. It supports data exchange using ActiveSync, but does not automatically start ActiveSync when connected. The “[Cable, Multipurpose RS232 and Power](#)” accessory can be used with the RS232 serial port. External AC power is available when the multipurpose RS232/Power cable is connected.

USB Client Port

The MX8 has one USB Client port for ActiveSync applications. An accessory USB cable, “[Cable, Multipurpose USB and Power](#)” is available to connect the MX8 to a USB Type A plug on a PC for ActiveSync functions. External AC power is available when the multipurpose USB Client/Power cable is connected.

Audio Headset Connection

An audio headset interface is available using the “[Adapter, Audio](#)” accessory with the I/O port. The connection cable connects the MX8 to a Voxware quick disconnect 4-pin interface. This cable adapts to specific styles of headsets for voice input, stereo or mono output. The MX8 with a Summit Client supports mono only. A 3-wire connector with (at a minimum) connections for ground, microphone, and 1 speaker. Connecting the headset to the MX8 COM port turns off audio output to the MX8 speaker on the front of the mobile device. All sounds previously directed to the speaker are redirected to the headphone, including beeps. Bias voltage for an electric condenser microphone is available. External AC power is not available for this option. Power is drawn from the main battery pack.

Audio Support

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

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

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

Volume Control Volume control is managed by a Settings panel, an API and the Orange-Scan up/ down arrow key key sequence.

Voice All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the “[Adapter, Audio](#)” accessory cable and the MX8 I/O connector at the base of the device.

Scanner / Imager Port

The MX8 has one integrated bar code scanner/imager port. Only one scan engine is installed at a time. Scan engines are not “hot swappable”. The MX8 may have one of the following scan engines:

- Intermec EV-15 linear imager
- Short Range Laser Scanner, SE955I
- Base Laser Scanner, SE955E
- Hand Held Products 2D Area Imager, 5300
- Honeywell Laser Scanner, N43XX

Note: Base Laser Scanner, 955E does not support aim mode. Any attempt to adjust the aiming beam using 955 programming bar codes will fail. The Base Laser scanner does not decode Codablock, Code93i or Telepen symbologies.

The integrated scan engine activates when the Scan button on the front of the MX8 is pressed or when the trigger on an installed trigger handle is pressed. A system panel ([Start > Settings > System > Data Collection](#)) is available to set scanner/imager options.

Functionality of the integrated scan engine driver is based on the decoder driver version installed in the MX8. Functions may include audible tones on good scan (at the maximum db supported by the speaker), failed scan, LED indication of a scan in progress, among other functions. If enabled, a vibration device provides a tactile response on a good scan event.

Note: If the SPN number on the label on the back of your MX8 ends in Rev B, your device has an integrated N43XX scan engine. For example, SPN: MX8X9X9X9X9X9XX Rev B.

Bluetooth EZPair

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

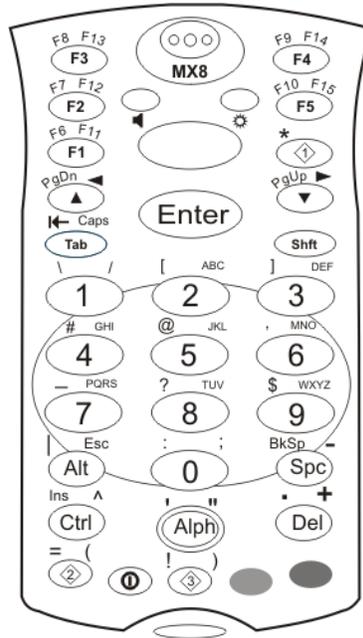
The user will not be able to select PIN authentication or encryption on connections from the MX8. However, the MX8 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX8 displays a prompt for the PIN or passcode. Maximum encryption is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

The Bluetooth client can simultaneously connect to one Bluetooth scanner and one Bluetooth printer. Up to four Bluetooth devices can be paired and managed using a system panel ([Start > Settings > System > Bluetooth](#)).

- The MX8 does not have a Bluetooth managed LED.
- The LED on the mobile Bluetooth scanner illuminates during a scanning operation; the Scan LED on the MX8 does not illuminate.
- Bar code data captured by the Bluetooth scanner is manipulated by the settings in the MX8 Data Collection panel.
- Multiple beeps may be heard during a bar code scan using the mobile Bluetooth scanner; beeps from the Bluetooth scanner as the bar code data is accepted/rejected, and other beeps from the MX8 during final bar code data manipulation.

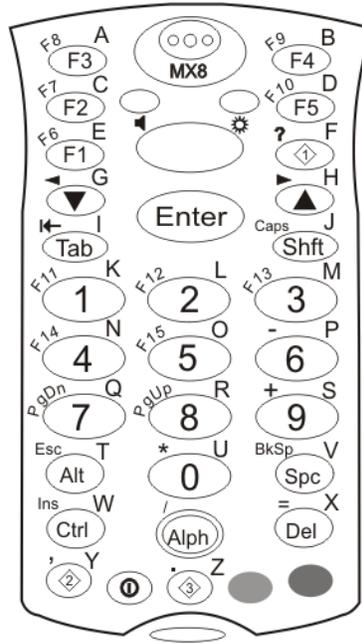
Keypads

Using the Triple-Tap Keypad



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

Using the Alpha-Mode Keypad



- When using a sequence of keys that require a lowercase alpha key, first press the Alpha key. Use the Shft sticky key for upper case alphabetic characters.
- Pressing the Alpha key forces “Alpha” mode for the numeric keys.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alpha key to toggle between Alpha and Numeric mode.
- When using a sequence of keys that do not include the Alpha key but does include a sticky key, press the sticky key first then the rest of the key sequence.
- Since letters are mapped to Alt, Ctl, Shft, these modifiers must be pressed before the Alpha key is pressed. For example, for Alt T, press Alt, then Alpha, then Alt again.
- A modifier key pressed after itself toggles that modifier key off.
- Pressing Alpha locks the keypad into Alpha mode. Pressing Alpha a second time toggles alpha mode off.

Standard Keys

Scan

The integrated scanner scans only when the Scan button is pressed (or when the scan trigger is pressed on the optional trigger handle).

Enter

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

Diamond

The Diamond keys can be programmed using the Buttons feature (Start > Settings > Personal > Buttons) to perform certain functions or launch a program.

F1 - F5

The function keys provide an F1 – F5 key press or can be programmed using the Buttons feature (Start > Settings > Personal > Buttons) to perform certain functions or launch a program.

Numeric

The number keys are used to add numbers to data entry fields.

Alpha

The alpha keys are used to add letters and characters to data entry fields.

Space

The Spc key adds a space to the line of data on the display. This function is similar to a regular keyboard's Spacebar. Note that the Spc key only stays active for one keystroke.

Function Keys

Sticky Keys

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

Sticky Key	Function
Ctl / Ctrl (Control key)	A Control sticky key press stays active until the Control key is pressed again. The Control key enables the control functions of the keypad. This function is similar to a regular keyboard's Control key. Each time you need to use a Control function, you need to press the Ctl / Ctrl key before pressing the desired key.
Alt (Alternate key)	An Alt sticky key press stays active until the Alt key is pressed again. The Alt key enables the alternate functions of the keypad. This function is similar to a regular keyboard's Alt key. Each time you need to use an alternate function, you need to press the Alt key before pressing the desired key.
Shft (Shift key)	<p>A Shift key press ends a sticky key function. The Shft key enables the shifted functions of the keypad. This function is similar to a regular keyboard's Shift key. Note that the Shift key only stays active for one keystroke. Each time you need to use a Shifted function, you need to press the Shft key before pressing the desired key.</p> <p>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.</p>
Orange and Blue Keys	<p>The Orange and Blue keys are sticky keys that, when tapped, activate the second functions of the keypad. Printed above many keys are small characters, in either orange (on the left side of the key) or blue (on the right side of the key), that represent the second function of that key. Using the sticky key activates the second key function. Note that the blue and orange sticky keys only stay active for one keystroke. Each time you need to activate a second function you must press the Orange or Blue key. To cancel a sticky key function before pressing another key, press the same sticky key again.</p>
	<p>Orange Key Tap the Orange key to enter "orange" mode. Tap it again to cancel "orange" mode. If you were in "blue" mode before you pressed the Orange key, blue mode is cancelled and you enter Orange mode.</p>
	<p>Blue Key Tap the Blue key to enter "blue" mode. Tap it again to cancel "blue" mode. If you were in "orange" mode before you pressed the Blue key, orange mode is cancelled and you enter Blue mode.</p>

Mode Key Functions

CapsLock Mode

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

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

To enter a string of letters in a text field, tap the Alph key to toggle it On. It remains active until it is tapped again and toggled off.

To enter a string of numbers in a text field, make sure the Alph key is toggled off.

Power Key

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

Power States

On	Normal operating state when a user is interacting with the device. Devices in use are in the Full On state. Devices not in use go the Sleep or Off state to save battery power.
Resuming	Initial state after the device wakes up from suspend. If the device does not transition to another state, the device returns to Suspend. Devices are the same as the On state.
System Idle	After a period of inactivity, the screen/backlight is off. Other devices may be turned off as well, though most devices are the same as Screen Off state. The MX8 transitions directly to the System Idle state where both the display and backlight are Off, there is no separate User Idle state where only the backlight is Off.
Unattended	State in which a program runs without the user's interaction, such as an automatic synchronization. Upon exit the application, the device goes directly to the Suspend state without waiting on the timer to expire.
Suspended	Sleep state. No threads are running. The CPU is idle. The system can wake up only by means of a hardware interrupt. All devices go into Sleep state, or if Sleep is not defined, Off state.

Display

The touch screen display is an active color LCD unit capable of supporting VGA graphics modes. Display size is 240 x 320 pixels in portrait orientation. The covering is designed to resist stains. The touch screen allows signature capture and touch input. A pen stylus is included. The touch screen responds to an actuation force (touch) of 4 oz. of pressure (or greater). The color display is optimized for indoor lighting. The display appears black when the device is in Suspend Mode or when both batteries have expired and the unit is Off.

Display Backlight Timer

[Start > Settings > System > Backlight](#)

When the Backlight timer expires the display backlight is turned off. The default value for the battery power timer is 3 seconds. The default value for the external power timer is “never” and the checkbox is blank.

The backlight timer dims the backlight on the touch screen at the end of the specified time.

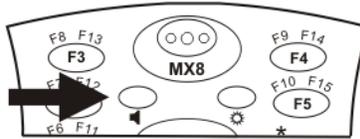
When the display wakes up, the Backlight timer begins the countdown again.

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

LED Indicators

The MX8 does not have a **Bluetooth managed LED**. Any Bluetooth activity indicators are located in the Desktop taskbar.

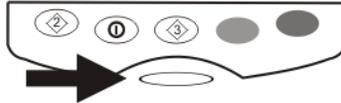
System Status LED



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

LED	Color - Activity	Indicates ...
System Status	Red - Blinking	Power fail. Replace the main battery with a fully charged main battery. Or Connect the MX8 to external AC power then replace the main battery with a fully charged main battery.
	Red - Steady	Main Battery Low. If the main battery is not replaced with a fully charged battery before the main battery fails, the MX8 is turned Off.
	Green - Blinking	Display Off. No user intervention required.
	No Color	Status is good. No user intervention required.

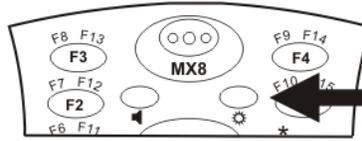
Scan Status LED



The Scan Status LED is located below the keypad.

LED	Color - Activity	Indicates ...
Scan Status	Green - Steady	Good scan.
	Red - Steady	Scan in progress.
	No color	Scanner / Imager ready for use.
	Amber - Steady	Decoder engine storing changed parameters.

Alpha Mode LED



The Alpha Mode LED is located next to the F5 key on the 32-key keypad (Numeric-Alpha keypad).

LED	Color - Activity	Indicates ...
Alpha Mode (Alph LED)	Green - Steady	MX8 is in Alpha character input mode.
	No color	MX8 is in Numeric key input mode.

Chapter 3: Power

Power Modes

On Mode

The Display

When the display is On:

- the keyboard, touch screen and all peripherals function normally
- the display backlight is on until the Backlight timer expires, then it dims

The MX8

After a new MX8 has been received, a charged main battery inserted, and the Power key tapped, the MX8 is always On until both batteries are drained completely of power.

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

Suspend Mode

The Suspend mode is entered when the unit is inactive for a predetermined period of time or the user taps the Power key. MX8 Suspend timers are set using Start > Settings > Systems > Power > Advanced tab.

A Power key tap wakes the unit and resets the display backlight timers. Primary Wake up events can be configured by a Power Management API call, e.g., any key press, a trigger press, a touch screen tap, AC adapter insert, USB cable insert, or Serial cable CTS will also wake the unit and reset the display backlight timers. When the unit wakes up, the Display Backlight and the Power Off timers begin the countdown again.

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

Off Mode

The unit is in Off Mode when the main battery and the backup battery are depleted. Insert a fully charged main battery and press the Power key to turn the MX8 On.

Batteries

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

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

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

Checking Battery Status

Tap the Start > Settings > System > Power > Battery tab. Battery level, power status and charge remaining is displayed.

Main Battery Pack

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

When the main battery pack is properly installed in the unit it provides up to eight hours of operation depending upon use and accessories installed. The battery pack is resistant to impact damage and falls of up to four feet to a concrete surface. Under normal conditions it should last approximately eight hours before requiring a recharge. The more you use the scanner or the wireless transmitter, the shorter the time required between battery recharges.

Battery Hotswapping

Important: When the backup battery power is Low (Start > Settings > System > Power > Battery tab) connect the AC adapter to the MX8 before replacing the main battery pack.

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

Note: Battery low warnings may be turned off using [MX8WM Options > Misc tab](#).

Replace the main battery by first placing the MX8 in Suspend Mode then removing the discharged main battery and installing a charged main battery within a five minute time limit (or before the backup battery depletes). When the main battery is removed the MX8 enters Critical Suspend state, the MX8 remains in Suspend mode, the display is turned off and the backup battery continues to power the unit for at least five minutes.

Though data is retained, the MX8 cannot be used until a charged main battery pack is installed. After installing the new battery, press the Power key. Full operational recovery from Suspend can take several seconds while the client is reestablishing a network link. If the backup battery depletes before a fully charged main battery can be inserted, the MX8 will turn Off. Full operational recovery from Off can take several seconds while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the MX8 startup completes, and Bluetooth relationships establish or re-establish.

Low Battery Warning

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

Note: Once you receive the main battery Low Battery warning, you have approximately 5 minutes to perform an orderly shutdown and replace the main battery pack before the device powers off. The Low Battery warning will transition the MX8 to Suspend before the MX8 powers off.

Backup Battery

The MX8 has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 160 mAh Nickel Metal Hydride (Ni-MH) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times is drawn from the MX8 main battery. It takes several hours of operation before a depleted backup battery is capable of supporting the operation of the MX8. The duration of backup battery life is dependent upon operation of the MX8, its features and any operating applications. The backup battery has a minimum service life of two years. The backup battery is replaced by Honeywell.

Handling Batteries Safely

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

Caution

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

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



Chapter 4: Software

Operating System

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

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

Windows Mobile 6.1

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

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

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

Based on your installed software version and hardware options, your setup may not be exactly the same as those that are described in this guide. Contact [Technical Assistance](#) for information on the latest upgrades for your MX8.

Software Development

The *CE API Programming Guide* documents Honeywell-specific API calls for the MX8. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on the Technical Assistance Portal. Contact [Technical Assistance](#) for more information.

Clearing Registry Settings

Use the [Clean Boot](#) process to return the registry to factory default values.

Installed Software

Note: Some standard Windows options require an external modem connection.

When you order an MX8 you receive the software files required by the separate programs needed for operation and wireless client communication. The files are pre-loaded and stored in folders in the mobile device.

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

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

Software Load

The software loaded on the MX8 computer consists of Windows Mobile 6.1 Operating System, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer for Windows Mobile browser and MX8-specific utilities. The software supported by the MX8 is summarized below:

Operating System

Full Operating System License: Includes all operating system components, including Windows Mobile 6.1 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.

Network and Device Drivers

Bluetooth (Option)

AppLock (Option)

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

API Routines

Software Backup

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

Version Control

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

The MX8 has a unique 128-bit ID code as required by the Windows Mobile 6.1 specification. This ID number is generated by the boot loader. This ID code is available in the About MX8WM settings panel, and by a Win32 standard API.

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

Boot Loader

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

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

The MX8 starts the OS every time during cold boot.

Startup Folders and Launch Sequences

The MX8 operating system uses two startup folders:

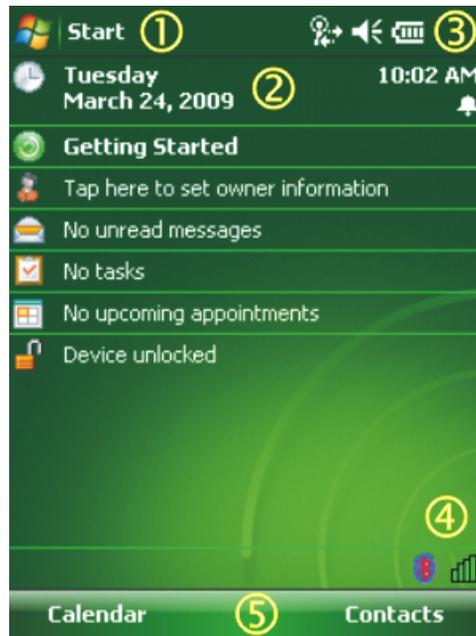
- User applications placed in the Windows\Startup folder automatically run during a cold boot. They are deleted upon a clean boot.
- User applications placed in the System\Startup folder automatically run during a cold boot.

Today Screen

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

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

The main screen for the MX8 is known as the Today screen. The Today screen shows various options and status icons. The Today screen appearance is configurable by selecting Start > Settings > Personal > Today. Both the appearance of the Today screen and the items displayed may be configured.



1. Start menu
2. Configurable Today screen listing
3. Notification Bar
4. Status icons
5. Soft Keys

Start Menu

The Start menu consists of applications and folders.

- Selecting an application from the menu starts that application.
- Selecting a folder opens a window displaying the contents of the folder.
- Selecting Settings displays the Settings panels by category.
- Selecting Help displays contact sensitive help. The contents displayed in the help window vary depending on the screen displayed before Help was accessed.

Programs not appearing on the Start menu can be accessed by using the File Explorer.

Configurable Today Screen Listing

The items displayed in the Today screen listing can be configured from Start > Settings > Personal > Today > Items.

For more information, please see [Today](#) settings later in this section.

Date

When the Date is enabled to display on the Today screen, the date is displayed on the left side of the screen and the time is displayed on the right side. If there are any alarms set, a bell icon is displayed under the current time.

For more information, please see the [Clock & Alarm](#) settings section.

Device Unlocked / Device Locked

When the MX8 is unlocked, clicking on **Device unlocked** locks the MX8.

When the MX8 is locked, clicking on **Unlock** at the bottom of the screen unlocks the MX8. Depending on the settings, a password may be required. The MX8 can also be configured to lock after a period of inactivity. For more information, please see the [Lock](#) settings.

Notification Bar

The Notification Bar is displayed at the top of the Today screen. The notification bar remains visible even when other screens are selected, though the icons displayed may vary.

When the Notification bar is displayed on other screens there may be an X (close the current screen/program) or an ok (accept the current input and close the screen).

Category	Icon	Meaning
Network		The Windows Mobile Wireless Manager is managing the wireless connection and the MX8 is connected to a wireless network.
		The Summit Client Utility is managing the wireless connection -or- The Windows Mobile Wireless Manager is managing the wireless connection and the MX8 is not connected to a wireless network.
		The Windows Mobile Wireless Manager is managing the wireless connection and has detected one or more wireless networks in range.
		The Windows Mobile Wireless Manager is managing the wireless connection and has not detected a wireless network in range.
Volume		The speaker is on.
		The speaker is off.
		Vibrate is on.
Power		The MX8 is connected to external power.
		The MX8 is operating on battery power. The strength of the battery is indicated by the number of bars displayed: 0 (low battery) to 4 (fully charged battery).

Status Icons

Additional icons may be displayed at the lower edge of the Today screen.

Note: Summit signal strength icons are displayed only when the Summit Client Utility is controlling the radio.

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

More information on Bluetooth can be found in the [Bluetooth settings](#) section.

More information on wireless connections can be found in Wireless Network Configuration.

Soft Keys

Soft Keys are displayed at the bottom of the Today screen. The keys displayed may vary by the active screen/application.

The soft keys generally provide menus for the selected application. By default, the left Soft Key can also be accessed by pressing F3 and the right Soft Key can be accessed by pressing F4. The assignments for the Soft Keys can be edited by selecting Start > Settings > Personal > Buttons.

Start and Program Menus

Start > Programs or Start

The following options represent the factory default program installation. Your system may be different based on the software and hardware options purchased. The location of the program may be in either the Start menu or the Start > Programs menu depending on the configuration in Settings > Personal > Menus.

ActiveSync	Basic ActiveSync configuration, including synchronization with an Exchange server.	
Calculator	Calculator	
Calendar	Calendar/date book application. Can be synchronized with PC Outlook calendar using ActiveSync.	
Contacts	Address book application. Can be synchronized with PC Outlook address book using ActiveSync.	
File Explorer	Displays a structured picture of files on the system.	
Games	Access installed games.	
Getting Started	This application provides several wizards to walk a user through device configuration.	
Help	Access Windows Mobile help system.	
Internet Explorer	Access web pages on the Internet.	
Messaging	Email application. Can be synchronized with PC Outlook email using ActiveSync or to synchronize with an Exchange server.	
Notes	Notebook application. Can be synchronized with PC Outlook notes using ActiveSync.	
Office Mobile		
	Excel Mobile	Microsoft Excel for Windows Mobile
	OneNote Mobile	Microsoft OneNote for Windows Mobile
	PowerPoint Mobile	Microsoft PowerPoint for Windows Mobile
	Word Mobile	Microsoft Word for Windows Mobile
Pictures & Video	Picture/video viewer application. Can be synchronized with PC documents folder using ActiveSync.	
RegEdit	Edit the system registry info.	
Remote Desktop (Auto)	A shortcut to Remote Desktop Mobile with Connect activated.	
Remote Desktop Mobile	Display remote desktop. Setup for computer, user name, password and domain required. Use Options to setup connected options for the remote desktop.	
Search	Search function searches all storage units in the device. It can be filtered to look for running tasks.	
Summit		
	scu	Wireless client management program.
Task Manager	View and cancel running tasks.	
Tasks	Task list application. Can be synchronized with PC Outlook task list using ActiveSync.	

Windows Live	Interfaces with Microsoft Windows Live online service.
Windows Media	Audio visual management program.

Installed Programs

Additional information on some installed programs is listed below.

Internet Explorer

Start > Internet Explorer

This browser is IEMobile 8.12. Configuration options for Internet Explorer are accessed by clicking Menu > Tools > Options from an Internet Explorer window.

Configuration of Internet Explorer for the MX8 is similar to configuration of Internet Explorer for a desktop PC. For more information on general configuration options, please see the Windows Mobile help system on the MX8 or other commercially available Internet Explorer configuration resources.

If an Internet Explorer web page is larger than the MX8 screen can display at one time, scroll bars are provided for horizontal and vertical scrolling. The scroll bars can be enabled or disabled using the [MX8WM Options](#) settings.

Internet Explorer for Windows Mobile includes an option to display web sites as a Mobile Device or a Desktop computer. The option can be accessed by selecting Menu > Tools > Options > Other.

For information on the version of Internet Explorer loaded on the MX8, click the Favorites soft key and select About Internet Explorer.

Office Mobile Applications

Start > Office Mobile

Office 2003 and Office 2007 formats are supported, though these are subset applications so not all objects may appear as expected.

ActiveSync handles all file format conversions for these files transferred between the MX8 and the host PC.

ActiveSync

Start > Programs > ActiveSync

ActiveSync can be setup to synchronize with an Exchange server. Contact your system administrator for configuration information.

AppLock (Option)

Start > Settings > System > Administration

The AppLock program is accessed by the user or the AppLock Administrator at bootup or upon completion of a suspend/resume. Set parameters using the Administration option in the Settings Panel.

Summit

SCU (Summit Client Utility)

Start > Programs > Summit

Summit automatically installs and runs after every cold boot. See Wireless Network Configuration for Summit Client Utility setup information and instruction.

Certs

Start > Programs > Summit > Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication. See Wireless Network Configuration for directions for acquiring CA and user certificate files.

Windows Media Player

Start > Programs > Media Player

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

Codecs are included for WMA, WMV, MP3 and WAV files.

Bluetooth (Option)

Start > Settings > System > Bluetooth

Only installed on a Bluetooth equipped MX8. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX8. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly Name for each MX8. Bluetooth can be accessed by tapping [Start > Settings > System > Bluetooth](#), or by tapping the Bluetooth icon on the Today screen.

RFTerm (Option)

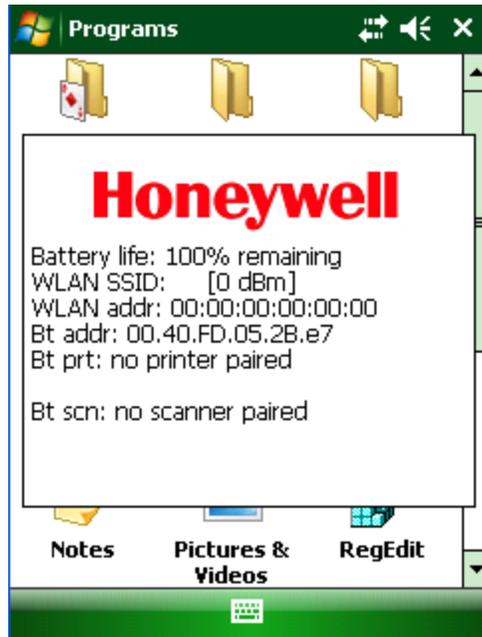
Start > Programs > RFTerm

The application can be accessed by tapping Start > Programs > RFTerm. Refer to the *RFTerm Reference Guide* for complete information and instruction. WAV files added by the user should be stored in System\LXE\RFTerm\Sounds.

Status Popup

Start > Settings > System > MX8 WM Options

The Status Popup provides real time information on several status icons when a specified keypress occurs.



To use the Status Popup, first map a key to the status window. Use the Buttons panel (Start > Settings > Personal > Buttons) to assign a key to Admin Statpop (for the Admin Popup) and StatPopup (for the User Popup). Use a Diamond key for the popup. If a Function key is used, that Function key is not available to other applications such as RFTerm.

Use the MX8 Options panel ([Start > Settings > System > MX8WM Options](#)) to configure other parameters including:

- Dismiss Status Popup on 5 second timeout
- Information to include in Admin or User Status Popup.

The Status Popup can be dismissed by the expiration of the timeout (if enabled), tapping the status window or pressing the key assigned to the popup.

For more information, please refer to the [Buttons](#) and [MX8WM Options](#) settings.

HSM Connect

HSM Connect allows a user with an [ActiveSync](#) connection between a PC and the MX8 to display the MX8's display on the host PC. Any keystrokes on the host PC are passed to the MX8 as if they were keystrokes on the MX8 keypad.

HSM Connect for the MX8 is available on the *Getting Started Disc*.

GrabTime

GrabTime is a utility to synchronize the MX8 with a world-wide time server. GrabTime can be started as a service by setting it in the Launch option (see the following section for details on Launch).

Synchronize with a local time server

- Use ActiveSync to copy GrabTime.ini from the Windows folder on the MX8 to the host PC.
- Edit GrabTime.ini (on the host PC) to add the local time server's domain name to the beginning of the list of servers. You can then optionally delete the remainder of the list.
- Copy the modified GrabTime.ini to the Windows folder on the MX8.

Enhanced Launch

Launch is a utility that runs automatically at startup. A partial list of Enhanced Launch functions includes:

- Launch a .CAB file
- Run an .EXE or .BAT file
- Process a .REG file
- Manipulate files and directories
- Modify registry keys
- Perform conditional operations

Note: The Enhanced Launch utility does not interact with or affect the AppLock Launch command.

For a complete list of Launch functions including commands and command structure, please see [Launch Utility](#).

RegLoad

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.

RegEdit

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

The Registry Editor allows viewing, searching for items and changing settings in the registry (Launch.REG). The registry contains information about how the mobile device runs. Use caution when inspecting and editing the Registry as making incorrect changes can damage the mobile device operating system.

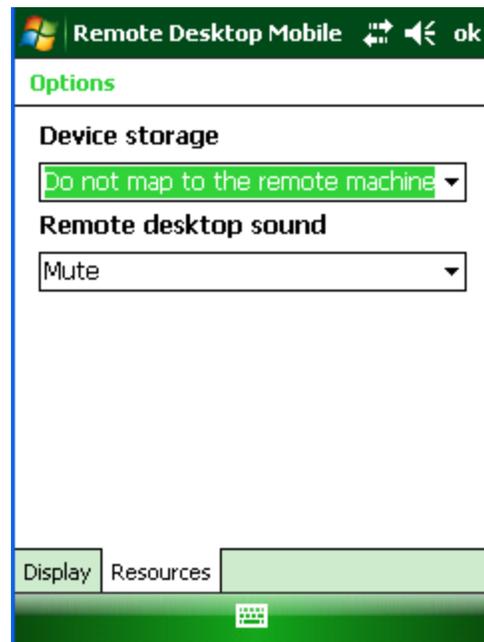
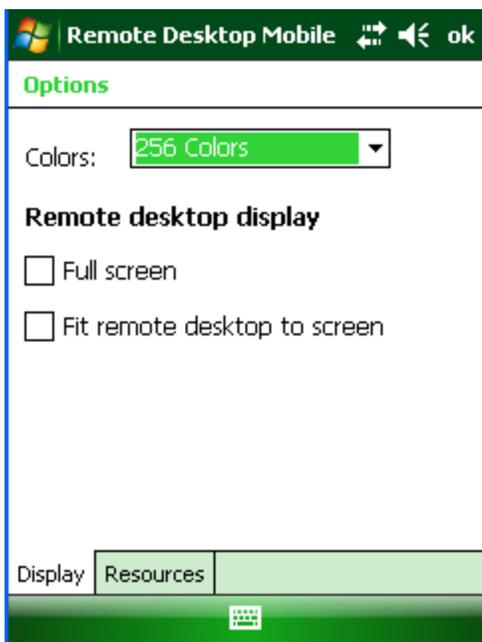
Remote Desktop

Start > Remote Desktop Mobile

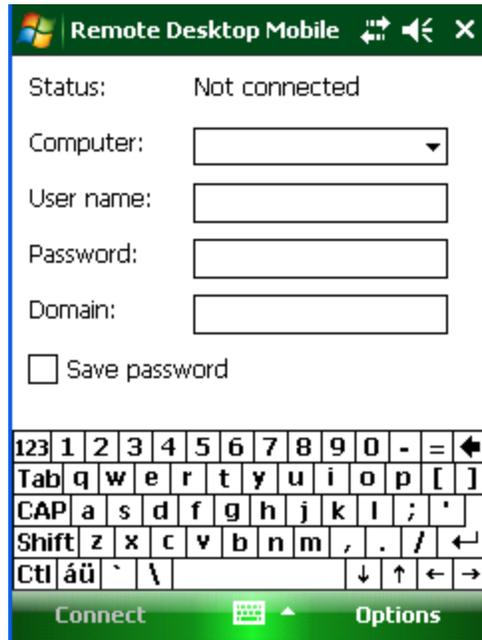
Using Remote Desktop Mobile, you can log on to a remote computer running Terminal Services or Remote Desktop and use all the programs available on that computer from your mobile device. For example, instead of running Word Mobile on the MX8, you can run the desktop computer version of Word and access all of the .doc files on that computer from your device.

Set Remote Desktop Mobile Options

Before connecting to a remote computer, set Remote Desktop Mobile options to improve display and resource when connected, if desired. Tap **Options** in the taskbar. Tap **OK** when finished.



Connect to a Remote Server



1. Configure the radio.
2. Enter the name of the computer to which you want to connect. If needed, enter the port number at the end of the computer name (*remotecomputername:portnumber*).
3. Enter the user name, password and domain.
4. Tap the Save password checkbox if it is blank.
5. Tap Connect to complete the connection and save the password.
6. Select Disconnect from Remote Desktop connection.
7. Create a folder titled Startup under the System folder.
8. Copy Remote.exe from the Windows folder to the \System\Startup folder just created.
9. Select Start > Settings > System > MX8WM Options and check Remote Desktop Autologon.
10. Select OK and 'yes' to reboot.
11. Result: The unit will boot into the Remote Desktop Connection.

Installing Applications

Applications can be installed on the MX8 from CAB files or package files.

Package files have some unique characteristics:

- Package files patch the operating system so they become non-volatile. Even a Clean Boot does not remove the programs.
- CAB files are (re)installed after a cold boot, but not after a suspend/resume since the OS was not reset during a suspend/resume and the CAB files are still in use.
- Packages can contain registry settings which are installed at setup, similar to a CAB file.
- Package files cannot be uninstalled, reinstalled or reverted to an earlier version.
- Packages can be digitally signed.
- A super package file can be created containing multiple package files. Because the MX8 must reboot after every package installation, a super package may make the installation faster.
- Package files have a .PKG extension, super package files have a .PKS extension.
- The MX8 must be connected to AC power to install a package or super package file.

An unsigned executable (CAB or package file) prompts the user when executed:

The program is from an unknown publisher. Running it can possibly harm your device. Do you want to continue?

If you trust the program, tap Yes. Otherwise tap No.

Preparation

Package files can be copied to the MX8 using ActiveSync or they can be installed from the Mini SD card.

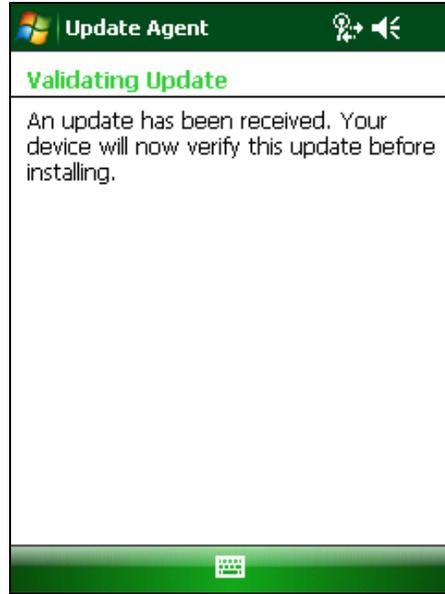
Package File Installation

The MX8 must be connected to external AC power. **IMPORTANT** – Because the package file installation actually rewrites portions of the operating system, it is important that the AC power is not interrupted during package file installation. If power is interrupted, the operating system may be damaged, requiring the MX8 to be returned to Honeywell for repair.

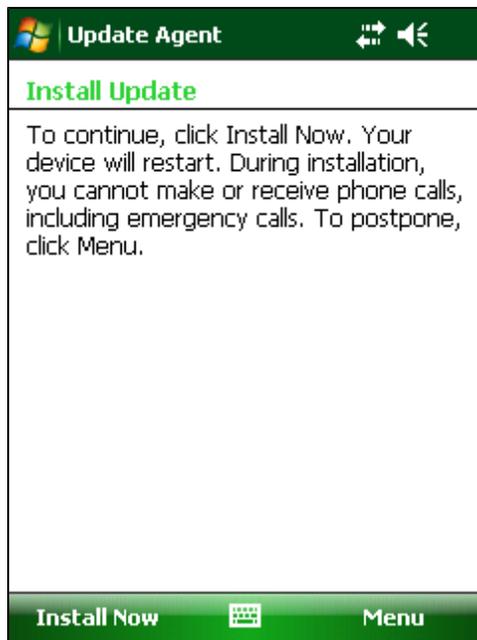
Use File Explorer to browse to the location of the package file.

Tap the package file. Note that by default the file extension is hidden. The package file can be either a single package file or a super package file.

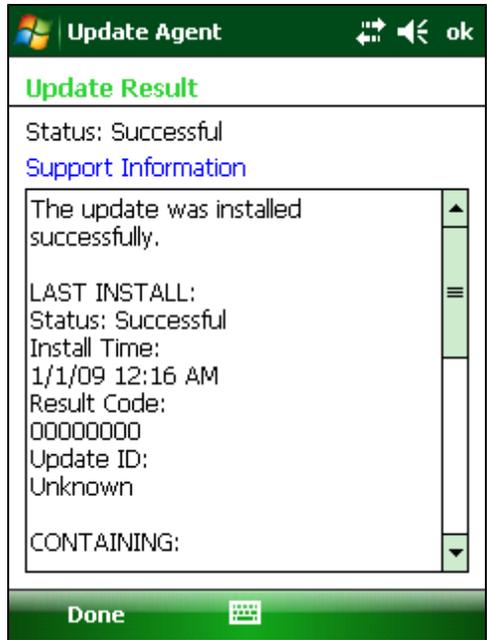
The installation process begins.



Click Install Now to begin the installation.



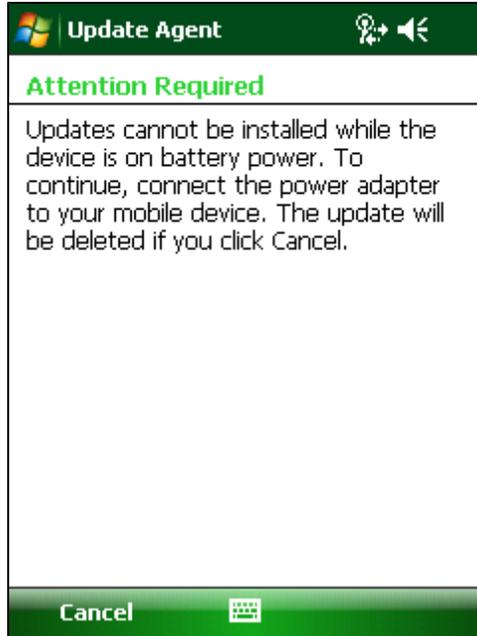
MX8 reboots and displays an Update message while the package is being installed. When the installation is completed, the MX8 reboots again and displays the summary screen.



Refer to *Installing Applications Help* if there is a problem with the package installation.

Installing Applications Help

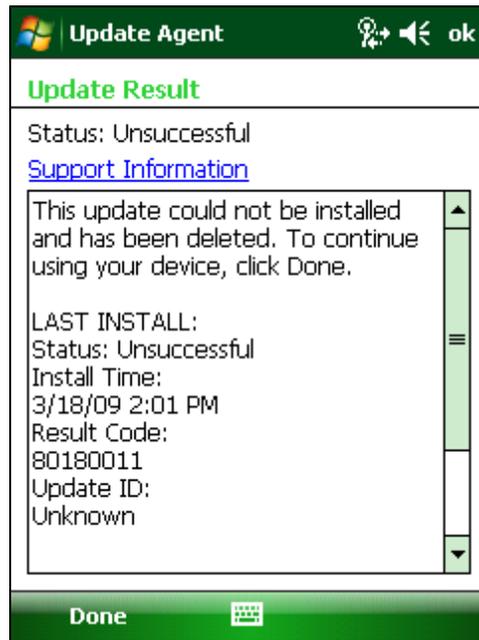
Message: The MX8 isn't connected to AC power.



Tap Cancel. Connect the MX8 to AC power and try the update again.

Note: The message that the update will be deleted only means that the scheduled update was deleted. The package file IS NOT deleted and remains on the storage card.

Message: **The package is already installed or is an older version than installed.**



The update could not be installed because the update has already been installed or the package file is an earlier version than is already installed on the MX8.

Tap Done to exit the update process.

Note: The message that the update could not be installed and is deleted only means that the scheduled update was deleted. The package file IS NOT deleted and remains on the storage card.

Contact [Technical Assistance](#) or your system administrator for more information on package versions.

Settings

Start > Settings

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

The settings in Windows Mobile are divided into three tabs: [Personal](#), [System](#) and [Connections](#).

Personal	Function
Buttons	Set functions of programmable buttons.
Input	Set input options for keypad, touch screen and voice.
Lock	Set password protection.
Menus	Select Start menu items.
Owner Information	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters.
Sounds & Notifications	Enable / disable sounds and vibrations. Set volume parameters and assign sound (wav) files to OS events.
Today	Configure the Today screen.

System	Function
About	Display OS version information. Set device name.
About MX8WMM	Display hardware, software and version information.
Administration	Use this option to set parameters for the MX8 when it is to be used as a dedicated, single or multiple application device. Only the applications or features specified in the AppLock configuration by the AppLock Administrator are available to the MX8 user.
Backlight	Set the display backlight brightness and display/keypad backlight timeout. Each item may be configured for battery and external power.
Bluetooth	Discover and manage Bluetooth devices.
Certificates	Manage digital certificates used for secure communication.
Clock & Alarms	Set Date, Time, Time Zone, and alarms.
Customer Feedback	Enable feedback to Microsoft.
Data Collection	Set scanner key wedge, internal scanner port, enable/disable internal scanner sounds, enable/disable illumination LEDs, and set vibration options. Assign baud rate, parity, stop bits and data bits for COM1 port.
Encryption	Enable file encryption on removable storage cards.
Error Reporting	Enable sending error reports to Microsoft.
External GPS	Configure serial GPS access.
License Manager	Displays license information for installed licensed applications.
Managed Programs	Display install history for .NET programs.

System	Function
Memory	Display current state of virtual memory.
MX8WM Options	Set the MX8 specific configuration options.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Remove user installed programs.
Screen	Calibrate touch screen, adjust text options.
Task Manager	Display running tasks and cancel running tasks.
Wi-Fi	Configure Wi-Fi access using the Summit Client Utility.
Windows Update	Configure and run Windows Update.

Connections	Function
Beam	Enable receiving IR and Bluetooth beams.
Connections	Configure connections to a host PC, network, etc.
Domain Enroll	Enroll in Active Directory domain.
Network Cards	Set the parameters for a wireless network using the utility included in Windows Mobile. See Wireless Network Configuration for details on using this utility. The label for this option may be either "Network Card" or "Wi-Fi" depending on radio configuration.
Wi-Fi	
Wireless Manager	Display the status of currently connected wireless networks.

Personal Panels

Buttons

Start > Settings > Personal > Buttons

Program Buttons

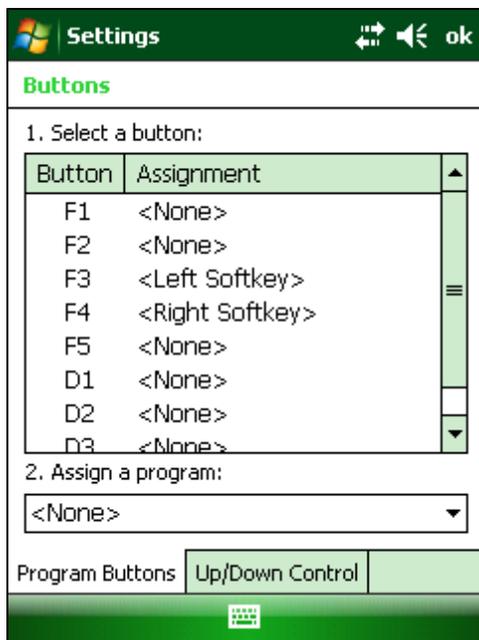
Program buttons can be used to assign functions to certain keys such as F1-F5 and the three diamond keys. Buttons can only be assigned to programs that have an icon in the Start menu or the Programs folder (including sub-folders). A program that is not in the above mentioned locations does not show up in the list here.

Note: The button links to the shortcut to the program, not the executable file.

Note: The System Administrator uses the Buttons setting panels to assign a Status User key and a Status Admin key on the [Status Popup panel](#).

Factory Default Settings

F1, F2, F5, D1, D2, D3	<None>
F3	Left Softkey
F4	Right Softkey

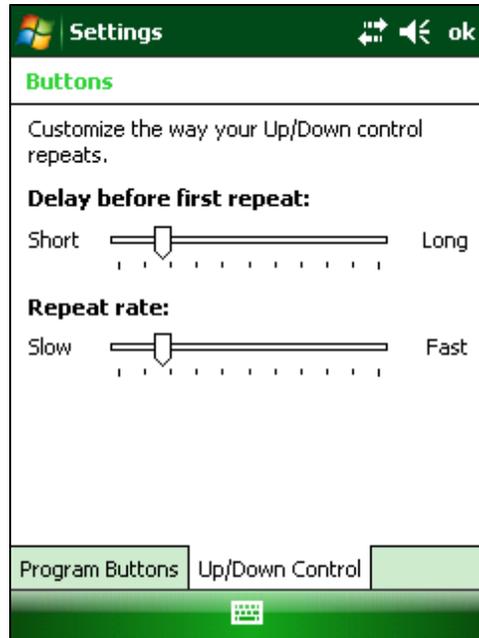


To assign a button:

1. Tap the desired button.
2. Select the program or shortcut from the *Assign a program* pulldown box.
3. Tap ok.

Up/Down Control

Customize the delay before repeating and the repeat rate for the up/down controls.



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Input

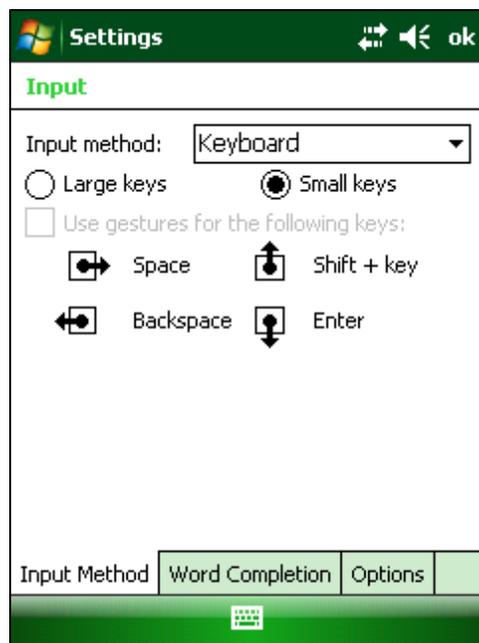
Start > Settings > Personal > Input

Input Method

Select the preferred method of input.

Factory Default Settings

Input Method	Keyboard
Small keys	Enabled



The default method of input is the keyboard or input panel. When the cursor is located in a field allowing text input, the input panel may automatically be displayed. If not automatically displayed, the input panel can be accessed by clicking on the keyboard icon at the bottom center of the screen.

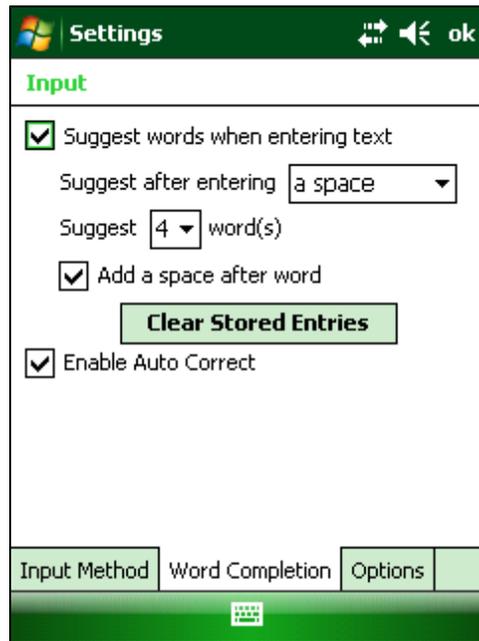
If a different input method is active, the icon for that input method is displayed instead of the keyboard icon.

Tap ok to save any changes.

Word Completion

Factory Default Settings

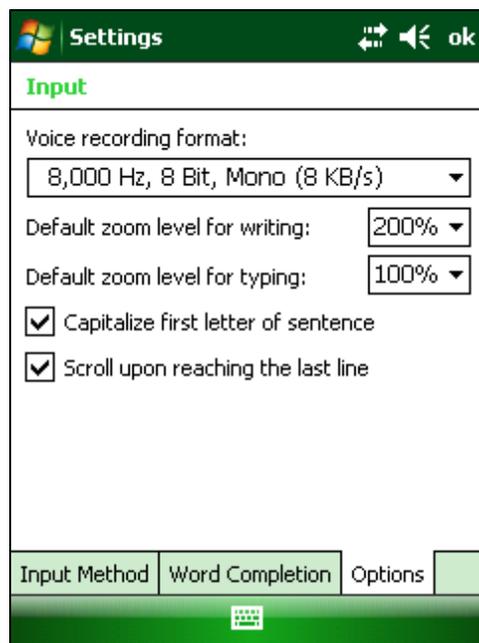
Suggest words when entering text	Enabled
Suggest after entering	A space
Suggest _ word(s)	4
Add a space after word	Enabled
Enable auto correct	Enabled



Options

Factory Default Settings

Voice recording format	8000 Hz, 8 Bit, Mono
Default zoom level for writing	200%
Default zoom level for typing	100%
Capitalize first letter of sentence	Enabled
Scroll upon reaching the last line	Enabled



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Lock

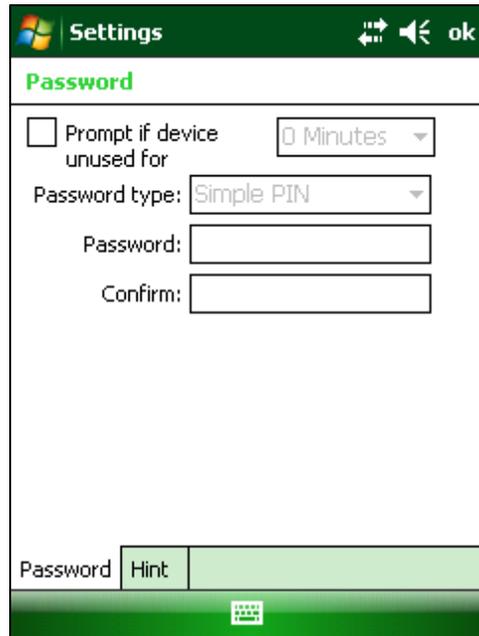
Start > Settings > Personal > Lock

Password

Set the lock / unlock behavior of the MX8.

Factory Default Settings

Prompt if device unused for	Unchecked
Timer	0 minutes
Password type	Simple PIN
Password	blank
Confirm	blank



Prompt if device is unused for – Check/enable the checkbox and set the inactivity timeout before the MX8 locks. Then the screen displays a numeric keypad or the input panel depending on the type of password selected.

Note: Once a password has been entered, the password must be used to access the Lock panels again.

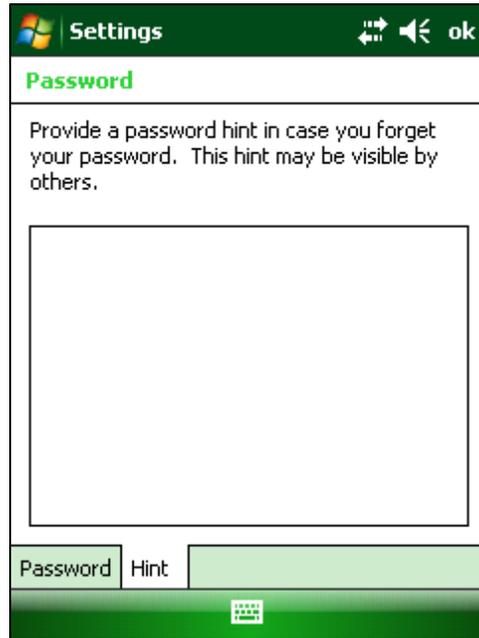
Select the Password type, Simple PIN (numeric) or strong alphanumeric. Enter the desired password and confirm. Note that Windows Mobile places restrictions on what it considers a valid password. If the chosen password is not strong enough, a warning is displayed and a new password should be entered and confirmed.

Hint

If the password entry isn't successful after a predefined number of attempts, the password hint is displayed.

Factory Default Settings

Password hint	<blank>
---------------	---------

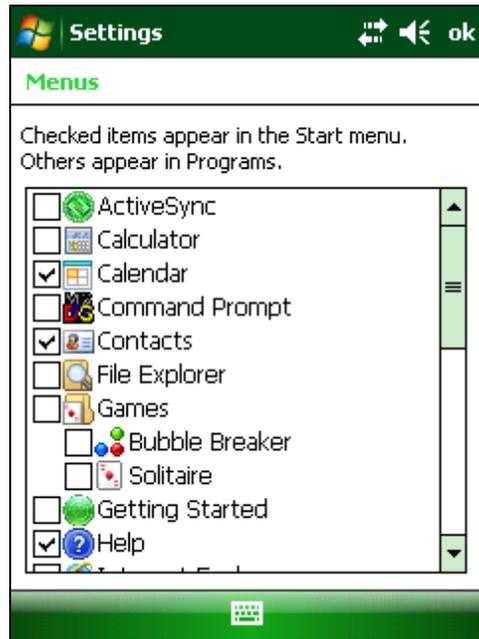


Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Menus

Start > Settings > Personal > Menus

Use this panel to select the programs to appear in the Start menu.



See Also: ["Start and Program Menus"](#)

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Owner Information

Start > Settings > Personal > Owner Information

Set the MX8 owner details.

Factory Default Settings

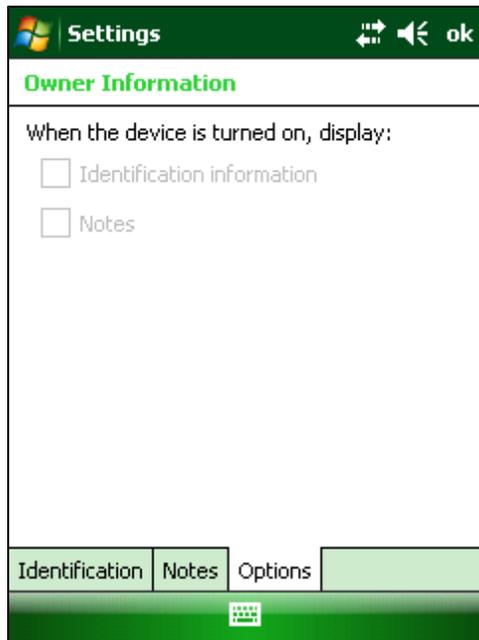
Identification	
Name, Company, Address, Telephone, E-mail	Blank
Notes	
Notes	Blank
Options	
When the device is turned on, display:	
Identification information	Disabled
Notes	Disabled

The screenshot shows the 'Owner Information' settings screen. At the top, there is a green header with the Windows logo, the word 'Settings', and navigation icons (back, forward, and 'ok'). Below the header, the title 'Owner Information' is displayed in green. The main content area contains five input fields, each with a label to its left: 'Name:', 'Company:', 'Address:', 'Telephone:', and 'E-mail:'. At the bottom of the screen, there is a green bar with four tabs: 'Identification', 'Notes', 'Options', and a fourth unlabeled tab. A keyboard icon is visible at the very bottom.

The screenshot shows the 'Owner Information' settings screen, specifically the 'Notes' section. The top header and title are identical to the previous screenshot. The main content area features a large, empty rectangular text input field. At the bottom, the same green bar with 'Identification', 'Notes', 'Options', and an unlabeled tab is present, along with a keyboard icon at the very bottom.

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

Note: Owner Identification name listed in Start > Settings > Personal > Owner > Information is not used during Bluetooth operation.



If owner information and notes are entered, use the options on this screen to enable the owner information or notes to be displayed at startup.

Note: Tap *Start > Help* for context sensitive *Windows Help* when changing or viewing options. Tap the *X* icon in the top right corner to close *Windows Help*.

Sounds & Notifications

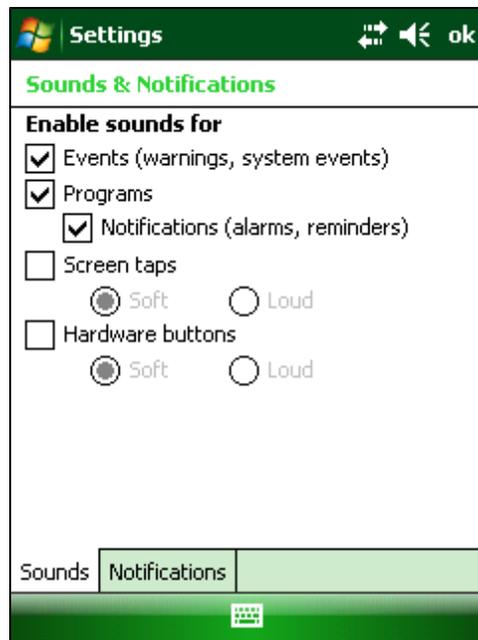
Start > Settings > Personal > Sounds & Notifications

Set volume parameters and assign sound wav files to Windows Mobile events.

Sounds

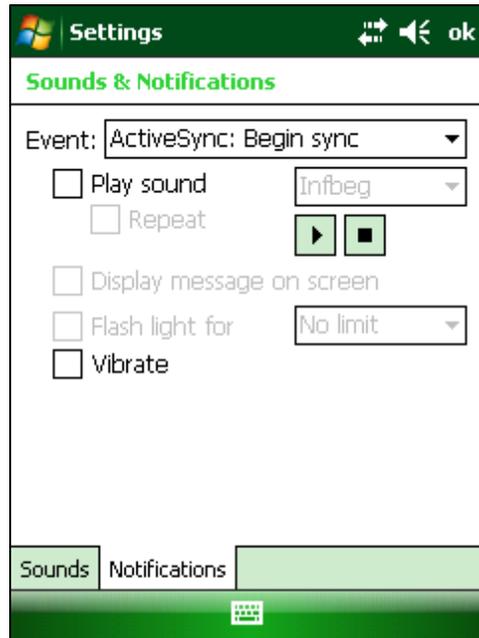
Factory Default Settings

Volume	
Events	Enabled
Programs	Enabled
Notifications	Enabled
Screen taps	Disabled
Hardware buttons	Disabled



Follow the instructions on the screen and tap ok to save the changes. Changes take effect immediately.

Notifications



The Event box lists several events that can have an associated notification. The notification, depending on the even selected, may consist of playing a sound, displaying a screen message, flashing a light or triggering the vibration motor.

When the flash light option is selected, the MX8 flashes the Alpha LED.

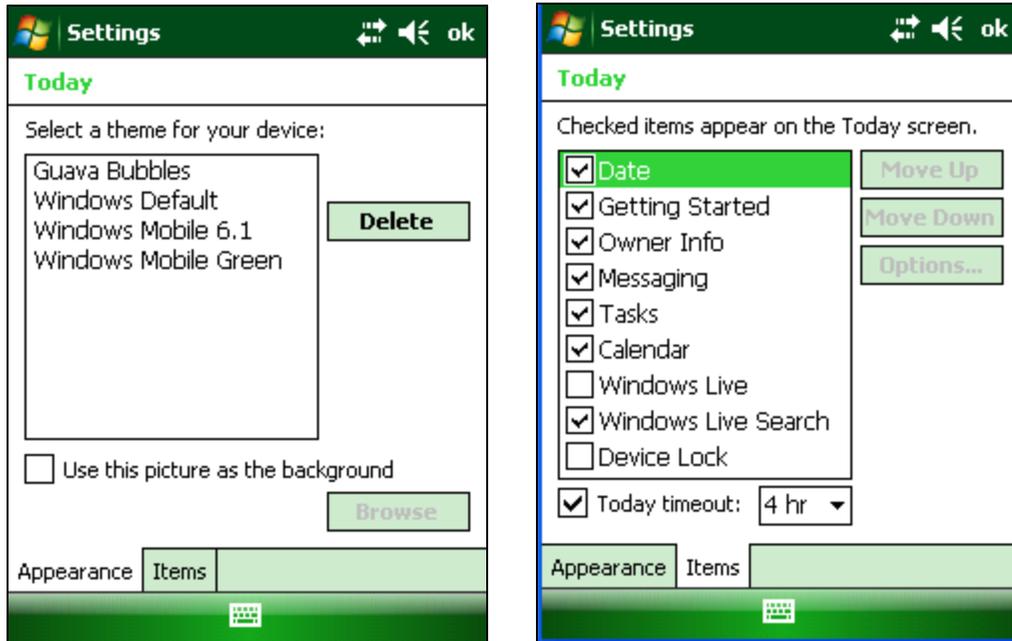
When you have finished changing the settings, tap ok to save the changes.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Today

Start > Settings > Personal > Today

Select a theme and the items to display on the Today screen.



Use the Appearance panel to assign a theme for the device. The default theme is Windows Mobile 6.1. Any user installed themes are included in the list.

Use the Items panel to select the items to be displayed on the Today screen.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

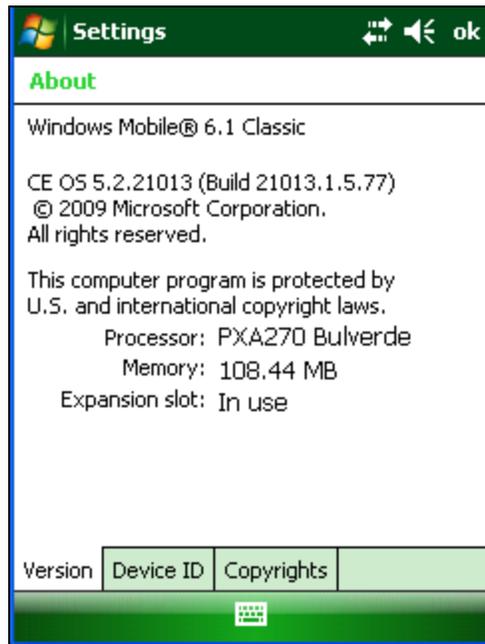
System Panels

About

Start > Settings > System > About

The About panels show OS versions, allow device name and description input and display copyright information.

Version



This screen displays information on the installed operating system and the hardware.

Note that Windows Mobile is based on a Windows CE engine. The underlying version of Windows CE is displayed on this panel.

Device ID

Factory Default Settings

Device Name	MX8001
Device Description	HSM_MX8WM



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.

Note: The Device Name listed in Start > Settings > System > About > Device ID is not used during Bluetooth operation.

Copyrights



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

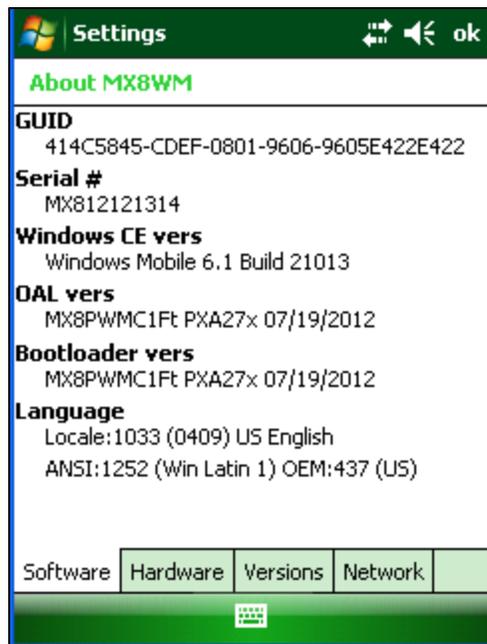
About MX8WM

Start > Settings > Personal > About MX8WM

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Language. Note:“Windows CE Version” refers to the version of Windows CE on which Windows Mobile was built. Windows Mobile 6.1 is built on Windows CE 5.2.
Hardware	CPU Type, Codec Type, Display, Flash memory, and DRAM memory
Versions	Utilities such as the Data Collection (DC) Wedge, EZPair, Summit radio driver, etc.
Network IP	Lists the adapters with MAC, IP and Gateway addresses for each as appropriate.

Software



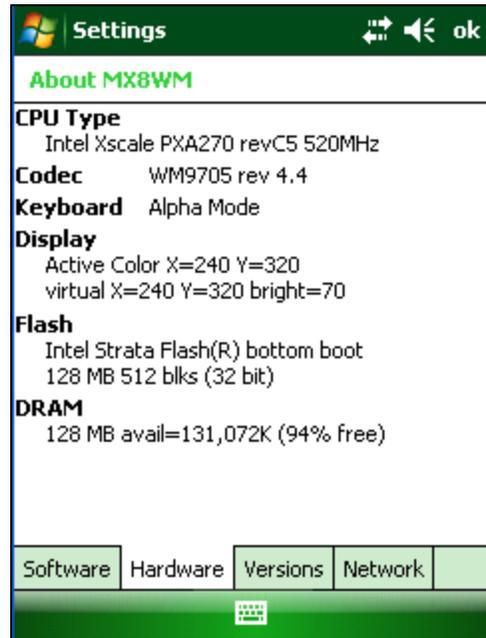
User application version information can be shown in the Version window. Version window information is retrieved from the registry.

Modify the Registry using the Registry Editor (see section titled “Utilities”). Use caution when editing the Registry and make a backup copy of the registry before any changes are made.

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

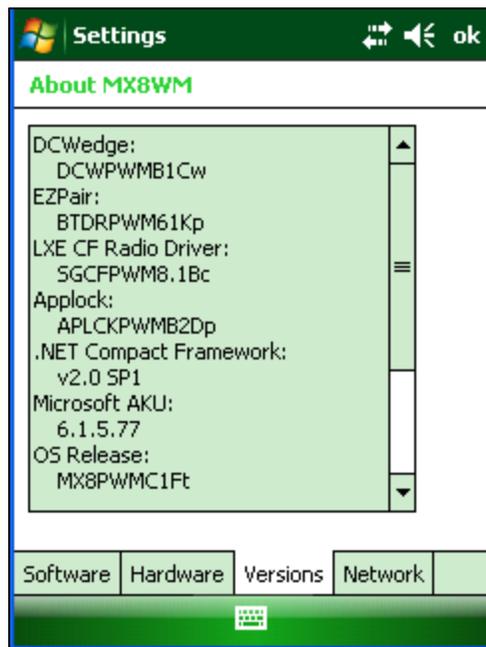
Create a new string value under this key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Hardware

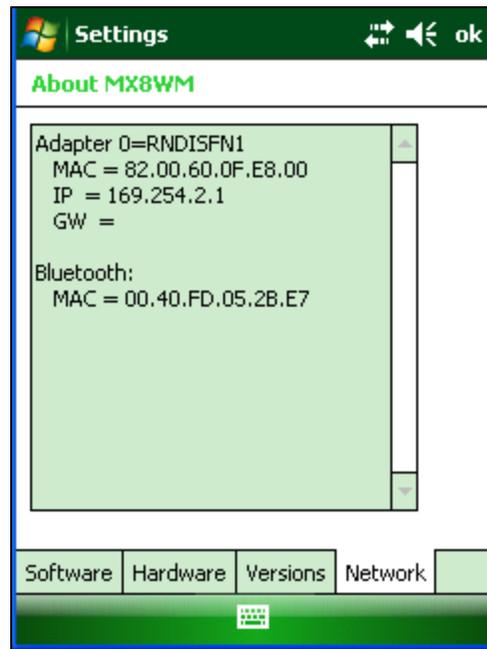


Note: The integrated bar code reader is identified by selecting Start > Settings > System > Data Collection > About tab.

Versions



Network IP



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Administration - for AppLock

Introduction

AppLock is designed to be run on Honeywell certified Windows based devices only. The AppLock program is pre-loaded. MX8 AppLock is setup by the Administrator by tapping Start > Settings > System > 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. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this section, is that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator panel file Launch option does not inter-relate with similarly-named options contained in other MX8 System Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact [Technical Assistance](#) for assistance, downloads and update availability.

Setup a New Device

Before you begin setting up a new device assign a default input method (Input Panel, Transcriber, or custom input method). Devices ordered with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

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 > System > Administration icon.
5. Assign a Switch Key (hotkey) sequence for AppLock. See Security Panel.
6. Assign an application on the Application tab screen. More than one application can be assigned.
7. Assign a password on the Security tab screen.
8. Select a view level on the Status tab screen, if desired.
9. Tap OK.
10. Press the Switch Key sequence to launch AppLock and lock the configured application(s).

The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application 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 clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the Administrator hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds (and within three attempts) to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt – this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e., an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g., missing DLLs).
- Corrupted registry settings.

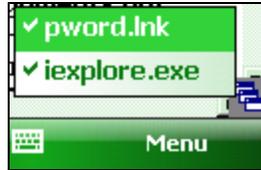
To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

AppLock Password Help

Contact [Technical Assistance](#) for help with AppLock passwords.

End-User Switching Technique

Note: The touch screen must be enabled.



A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX8 default input method (Input Panel, Transcriber, or custom input method) is activated.

The check to the left of the application name indicates that the application is active.

If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by clicking on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

See Also: Application Panel > Launch > Manual (Launch) and Allow Close

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter.

When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: Application Panel > Global Key

Hotkey (Activation hotkey)

The default Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. 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.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Application Configuration

Settings > System > Administration icon

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

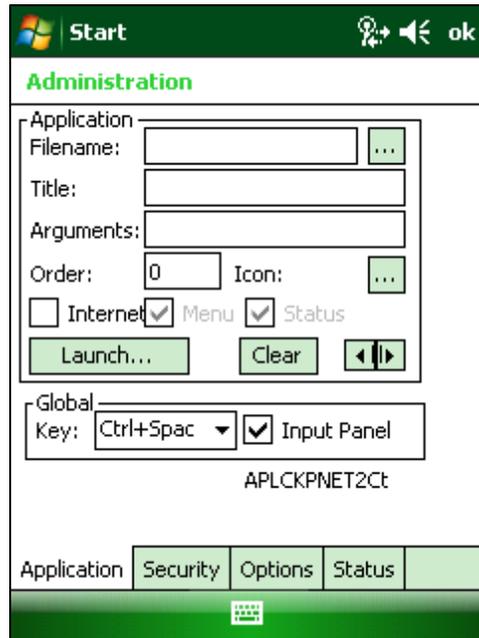
Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Panel.

If a password has not been configured, the Administrator panel is displayed.

Important: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application Panel



Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

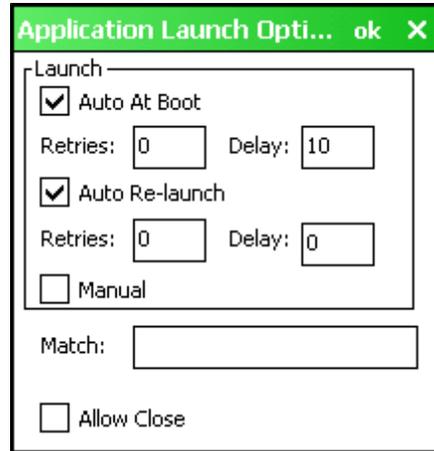
If no application is specified when the Administrator Panel is closed, the MX8 reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad .
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button .
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global

Option	Explanation
	Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



The image shows a dialog box titled "Application Launch Opti..." with "ok" and "X" buttons. The dialog contains a "Launch" section with the following options:

- Auto At Boot
 - Retries: Delay:
- Auto Re-launch
 - Retries: Delay:
- Manual

Below the "Launch" section, there is a "Match:" label followed by an empty text input field. At the bottom of the dialog, there is an Allow Close option.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot

Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch

Default is Enabled.

When enabled for a specific application, automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)

Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Match

Default is blank (Match is not used).

AppLock works by associating display windows with the launched process ID. If an application uses different process IDs for windows it creates, the Match field must be used.

Use the Match field to specify up to 32 characters of the class name for the application.

- DOS applications using a standard DOS display box should specify **condev_appcls** in the Match textbox.
- Remote Desktop (remote.exe) should specify TSSHHELLWND in the Match textbox.

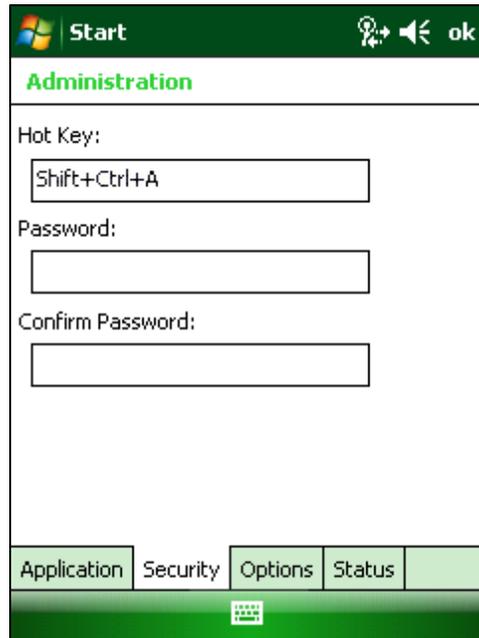
Note: An update may be required to support locking remote.exe. Contact [Technical Assistance](#) for details.

Allow Close

Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Security Panel



Setting an Activation Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is Shift+Ctrl+A.

A 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 using the keypad. Some hotkeys cannot be entered using the Input Panel. Also, hotkeys entered using the Input Panel are not guaranteed to work properly when switching operational modes.

For example, if the Ctrl key is pressed followed by A, Ctrl+A is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch user modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

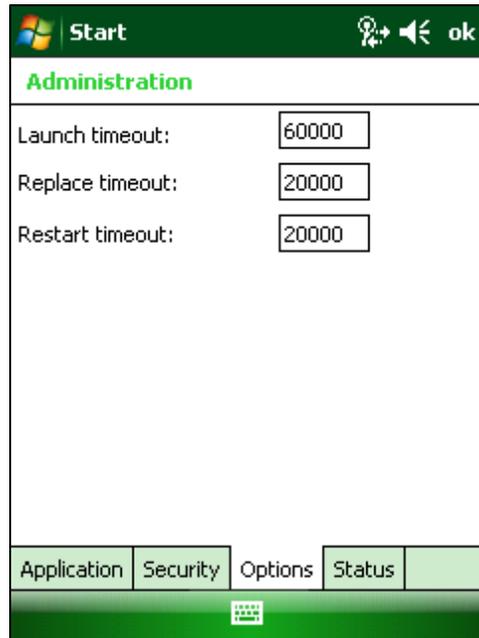
Setting a Password in the Security Panel

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator 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"](#)

Options Panel



AppLock uses 3 timeout values when locking applications:

Launch timeout -- the time to wait for an application to initially launch before timing out. Default value is 60000 milliseconds (60 seconds).

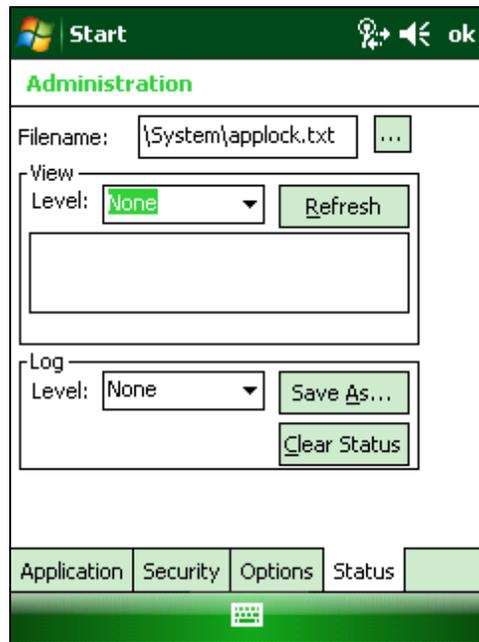
Replace timeout -- the time to wait for an application to replace the current window with another one before timing out. Default value is 20000 milliseconds (20 seconds).

Restart timeout -- the time to wait for an application to restart itself before timing out. Default value is 20000 milliseconds (20 seconds).

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.



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 which does not have as many options.

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 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.

AppLock Help

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word and RFTerm, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. Honeywell 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.

Can't locate the password that has been set by the administrator?

Contact [Technical Assistance](#) for assistance.

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter..." is logged at the beginning of the function specified in the message and "Exit..." is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
*****	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR

Message	Explanation and/or corrective action	Level
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 panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
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

Message	Explanation and/or corrective action	Level
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
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

Message	Explanation and/or corrective action	Level
Exit EncryptPwd	Exiting password encryption processing.	LOG_ PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_ PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_ PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_ PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_ PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_ PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_ PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_ PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_ PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_ PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_ PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_ PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_ PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_ PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_ PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_ PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
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

Message	Explanation and/or corrective action	Level
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. If the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the "Registry read failure" above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
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

Backlight

Start > Settings > System > Backlight

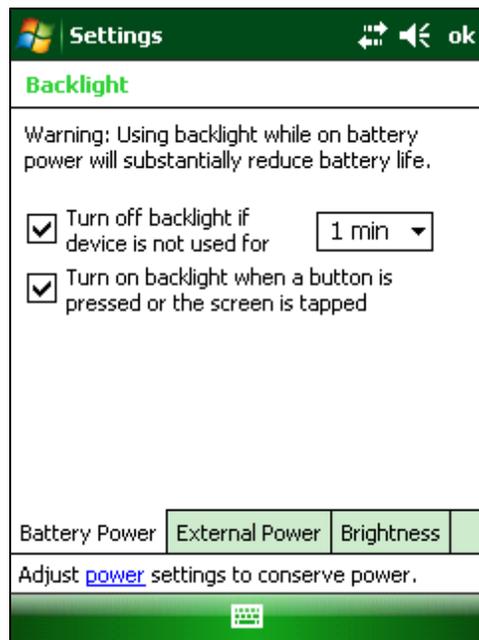
Set the power management timers for the display and keyboard backlights. Set the display brightness for battery and external power.

IMPORTANT – When the backlight timer expires, the display backlight and the display are OFF, as is the keypad backlight. This is the System Idle state, there is no separate User Idle state.

Battery Power

Factory Default Settings

Turn of backlight is device not used for	Enabled
Timer	1 min
Turn on backlight when a button is pressed or the screen is tapped	Enabled Note: This option is always Enabled, unchecking this option has no effect.

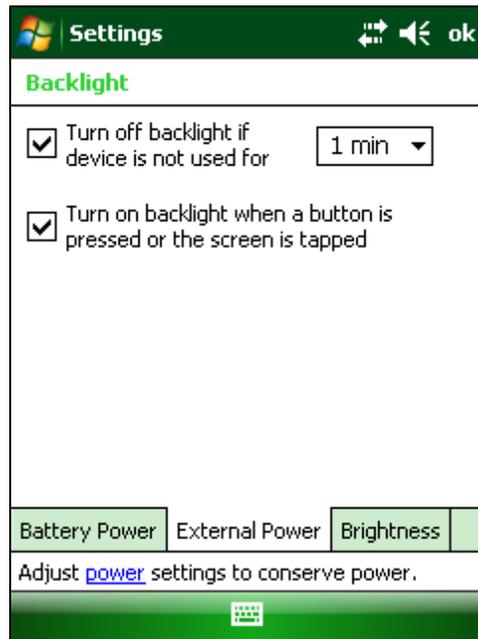


When the MX8 is on battery power and the backlight timer expires, the display and the backlights for the display and keypad are turned off. Default value is 1 minute and both the check boxes are enabled. Adjust the settings and tap ok to save the changes. The changes take effect immediately.

External Power

Factory Default Settings

Turn off backlight if device not used for	Enabled
Timer	1 min
Turn on backlight when a button is pressed or the screen is tapped	Enabled Note: This option is always Enabled, unchecking this option has no effect.

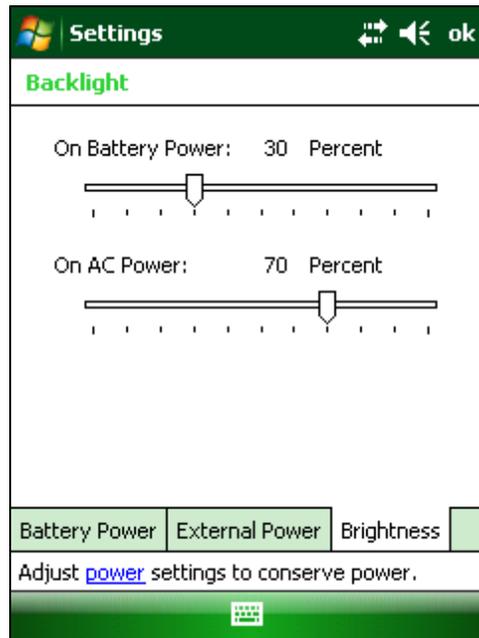


When the MX8 is on external power and the backlight timer expires, the display and the backlights for the display and keypad are turned off. Default value is 1 minute and both the check boxes are enabled. Adjust the settings and tap ok to save the changes. The changes take effect immediately.

Brightness

Factory Default Settings

On Battery Power	30 Percent
On AC Power	70 Percent



Adjust the brightness of the display when the MX8 is on battery and AC power. Use the slider bars to adjust the brightness level and tap ok to save.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Bluetooth

Start > Settings > System > Bluetooth

Note: Contact [Technical Assistance](#) for upgrade availability if your EZPair panels are not the same as the panels presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings

Discovered Devices	None
Settings	
Turn On Bluetooth	Default value is Off (at initial startup)
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled (checked)
Printer Port on COM9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	[System Name]
Reconnect	
Report when connection lost	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled

Bluetooth icon state and Bluetooth device icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the mobile device.

- The default Bluetooth setting is Off. If the Discover button is not active, check the Bluetooth button status on the Settings tab.
- The MX8 cannot be discovered by other Bluetooth devices when the *Computer is discoverable* option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be *Non-Discoverable or Invisible*.
- When **Filtered Mode is enabled**, the MX8 can pair with one Bluetooth scanner and one Bluetooth printer.
- When **Filtered Mode is disabled**, the MX8 can pair with up to four Bluetooth devices, with a limit of one scanner, one printer, two **HID**¹ (one Mouse, one Keyboard), one **PAN**² device and one **DUN**³ device connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the MX8.
- The target Bluetooth managed device should be as close as possible (line of sight - no more than 32.8 feet or 10 meters) to the MX8 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the MX8. The MX8 operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

¹Human Interface Device profiles used by Bluetooth keyboards, mice, pointing devices and remote monitoring devices.

²Personal Area Networking profile. Un-modified Ethernet payloads (using BNEP) can exchange packets between Bluetooth devices. PANU is a PAN User service that uses either the NAP or the GN service.

³Dial-Up Networking provides access to the Internet and other dial-up services using Bluetooth technology.

Initial Configuration

1. Select **Start > Settings > System > Bluetooth** or tap the Bluetooth icon on the Start screen. The EZPair application opens.
2. Tap the **Settings** Tab.
3. Tap the **Turn On Bluetooth** button. The button name changes to Turn Off Bluetooth.
4. Change the Computer Friendly Name at the bottom of the Settings display. The Bluetooth MX8 default name is determined by the factory installed software version. Best practice is to assign every MX8 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
5. Check or uncheck the MX8 Bluetooth options on the Settings tab.
6. Tap the OK button to save your changes.

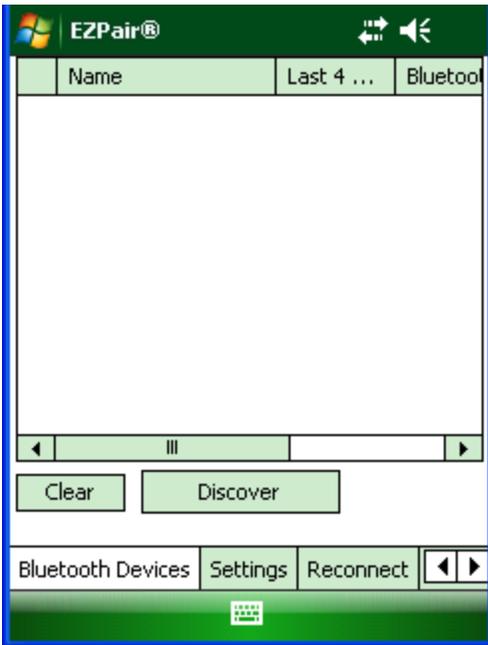
Subsequent Use

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

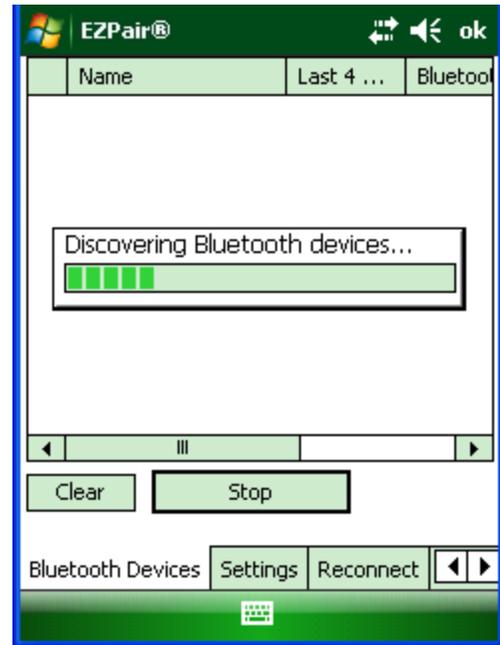
1. Tap the Bluetooth icon on the Start screen to open the EZPair application.
2. Tap the Bluetooth Devices tab.
3. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Tap to highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap Pair as Scanner to set up the MX8 to receive scanner data.
7. Tap Serial Device to set up the MX8 to communicate with a Bluetooth serial device.
8. Tap Pair as Printer to set up the MX8 to send data to the printer.
9. Tap Disconnect to stop pairing with the device. Once disconnected, tap Delete to remove the device name and data from the MX8 Bluetooth Devices list, if desired. The device is deleted from the list after the OK button is clicked.
10. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX8 display.
11. Whenever the MX8 is turned On, all previously paired, active, Bluetooth devices in the vicinity are paired, one at a time, with the MX8. If the devices cannot connect to the MX8 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if [Report Failure to Reconnect](#) is disabled.

Discover

Note: Change the Computer Friendly Name at the bottom of the [Settings](#) display. The Bluetooth MX8 default name is determined by the factory installed software version. Best practice indicates assigning every MX8 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.



Before Discovering



During Discover

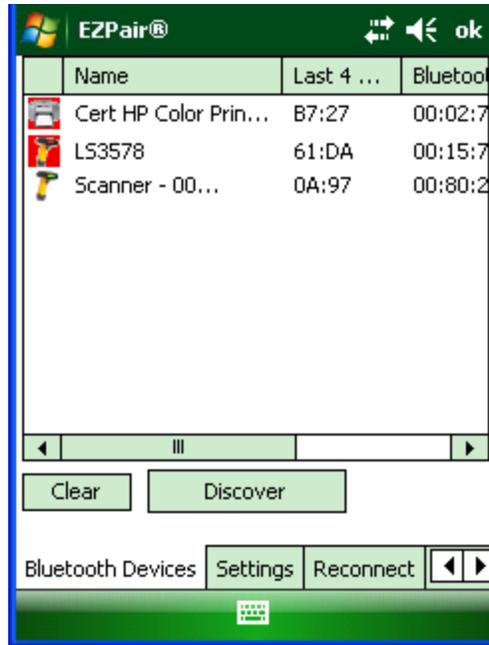
Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier for each device discovered. It may be necessary to tap the **Turn on Bluetooth** button on the Settings tab before beginning discovery as Bluetooth is Off by default.

Stop Button

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

Bluetooth Devices

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



Note: When an active paired device, not the MX8, enters Suspend Mode, is turned Off or leaves the MX8 Bluetooth scanning range (approximately 32 feet or 10 meters), the Bluetooth connection between the paired device and the MX8 is lost. There may be audible or visual signals as paired devices disconnect from the MX8.

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired; the Bluetooth panel assigns an icon to the device name.

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

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

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

Clear Button

Deletes all devices from the Device table that are not currently paired. A dialog box is presented, "*Delete all disconnected devices? Yes/No*". Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence and when EZPair is re-launched without a reboot sequence. Tap the No button to make no changes.

[See Clearing Pairing Table on Boot.](#)

Bluetooth Device Menu

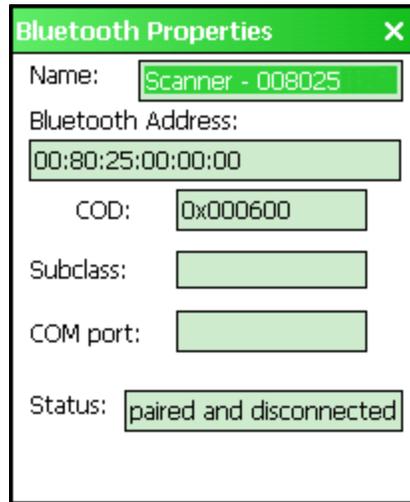
Click on a device in the Discover list to highlight it. Doubletap the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.



Right Click Menu Options

Pair as Scanner	Receive data from the highlighted Bluetooth scanner or Bluetooth imager.
Pair as Printer	Send data to the highlighted Bluetooth printer.
Pair as Serial Device	Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled/unchecked.
Pair as HID Device	Communicate with the highlighted HID (Human Interface Device). This option is available when Filtered Mode is disabled/unchecked.
Pair as PAN Device	Communicate with the highlighted PAN (Personal Area Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Pair as DUN Device	Communicate with the highlighted DUN (Dial-Up Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Disconnect	Stop the connection between the MX8 and the highlighted paired Bluetooth device.
Delete	Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the MX8 Bluetooth Devices panel after the user taps OK.
Properties	More information on the highlighted Bluetooth device.

Bluetooth Properties



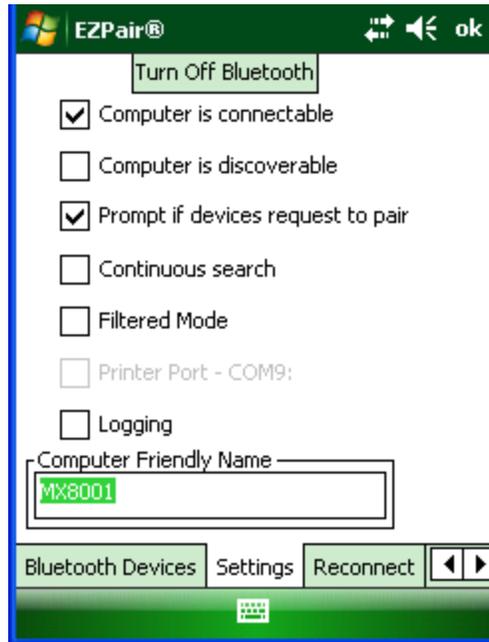
The image shows a screenshot of a 'Bluetooth Properties' dialog box. The title bar is green with a white 'X' icon. The dialog contains several fields with light green backgrounds and black text:

- Name: Scanner - 008025
- Bluetooth Address: 00:80:25:00:00:00
- COD: 0x000600
- Subclass: (empty field)
- COM port: (empty field)
- Status: paired and disconnected

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

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

Settings



Turn On Bluetooth

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*. The default value is Bluetooth is Off.

Options

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

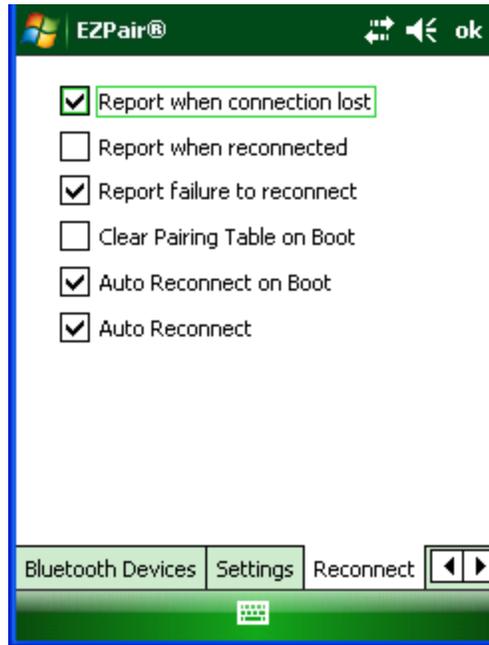
Option	Information
Computer is connectable	This option is Enabled by default. Disable this option to inhibit MX8 connection with all Bluetooth devices.
Computer is discoverable	This option is Disabled by default. Enable this option to ensure other devices can discover the MX8. When this option is enabled the Windows Mobile Wireless Manager displays Bluetooth status as "Visible".
Prompt if devices request to pair	This option is Enabled by default. A dialog box appears on the MX8 screen notifying the user a Bluetooth device requests to pair with the MX8. The requesting Bluetooth device does not need to have been Discovered by the MX8 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.

Option	Information
Continuous Search	<p>This option is Disabled by default.</p> <p>When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the MX8 stops searching after 30 minutes. This option draws power from the MX8 Main Battery.</p>
Filtered Mode	<p>This option is Disabled by default.</p> <p>Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked).</p> <p>When Filtered Mode is disabled, the MX8 can pair with up to four Bluetooth devices, with a limit of one Bluetooth scanner, one Bluetooth printer, one PAN, and one DUN. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard.</p> <p>A Restart is required every time Filtered Mode is toggled on and off.</p>
Printer Port - COM9	<p>This option is Disabled by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled.</p>
Logging	<p>This option is Disabled by default.</p> <p>When logging is enabled, the MX8 creates bt_log.txt and stores it in the \System folder. Bluetooth activity logging is added to the text file as activity progresses. A bt_log_bak.txt file contains the data stored by bt_log.txt prior to reboot.</p> <p>During a reboot process, the MX8 renames bt_log.txt to bt_log_bak.txt. If a file already exists with that name, the existing file is deleted, the new bt_log_bak.txt file is added and a new bt_log.txt is created.</p>
Computer Friendly Name	<p>Default: Computer System Name (System Panel > Device Name tab).</p> <p>The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.</p>

Note: The Device Name listed in [Start > Settings > System > About > Device ID](#) is not used during Bluetooth operation.

Note: Owner Identification name listed in [Start > Settings > Personal > Owner > Information](#) is not used during Bluetooth operation.

Reconnect



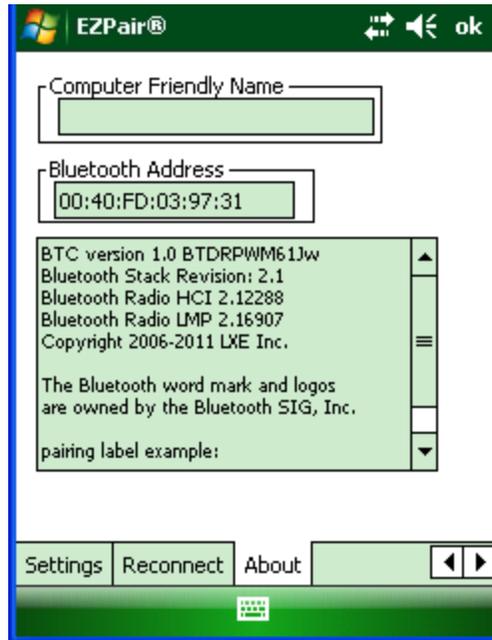
Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Options

Option	Information
Report when connection lost	<p>This option is Enabled (checked) by default.</p> <p>There may be an audio or visual signal when a connection between a paired, active device is lost.</p> <p>A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.</p>
Report when reconnected	<p>This option is Disabled (unchecked) by default.</p> <p>There may be an audio or visual signal when a connection between a paired, active device is made.</p> <p>A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the ok button to remove the dialog box from the screen.</p>

Option	Information
Report failure to reconnect	<p>This option is Enabled (checked) by default.</p> <p>The default time delay is 30 minutes. This value cannot be changed by the user.</p> <p>There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed.</p> <p>Tap the X button or ok button to close the dialog box.</p> <p>Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.</p>
Clear Pairing Table on Boot	<p>This option is Disabled (unchecked) by default.</p> <p>When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected.</p> <p>When enabled (checked) <i>Auto Reconnect on Boot</i> is automatically disabled (dimmed).</p>
Auto Reconnect on Boot	<p>This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence.</p> <p>When disabled (unchecked), no devices are reconnected upon any reboot sequence.</p>
Auto Reconnect	<p>This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior.</p> <p>When Auto Reconnect is disabled (unchecked), <i>Auto Reconnect on Boot</i> is automatically disabled and dimmed.</p> <p>When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of <i>Auto Reconnect on Boot</i> is ignored and no devices are reconnected on boot. The status of <i>Clear Pairing Table on Boot</i> controls whether the pairing table is populated on boot.</p> <p>When Auto Reconnect is enabled (checked) and <i>Auto Reconnect on Boot</i> is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range).</p> <p>When Auto Reconnect is enabled (checked) and <i>Clear Pairing Table on Boot</i> is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of <i>Auto Reconnect on Boot</i> is ignored and the option is automatically disabled (unchecked) and dimmed.</p>

About



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

Easy Pairing and Auto-Reconnect

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

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

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

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

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the MX8 while AppLock is in control.

The [Windows Mobile Wireless Manager](#) also indicates the status of the Bluetooth radio:

- On – The Bluetooth radio is on.
- Off – The Bluetooth radio is off
- Visible – “Computer is discoverable” is checked on the Settings tab.

Bluetooth Bar Code Reader Setup

Please refer to the mobile Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the MX8 using Bluetooth functions.

- The MX8 must have the Bluetooth hardware and software installed. An MX8 operating system upgrade may be required.
- If the MX8 has a Bluetooth address identifier bar code label affixed, then Bluetooth hardware and software are installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The MX8 batteries are fully charged. Alternatively, the MX8 may be cabled to AC/DC power.
- **Important:** The bar code numbering examples in this segment are not real and should not be created or scanned with a Bluetooth scanner.
- To open the EZPair program, tap Start > Settings > System > Bluetooth or tap the Bluetooth icon at the bottom of the Today screen.



Locate the bar code label, similar to the one shown above, attached to the MX8. The label is the Bluetooth address identifier for the MX8.

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

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

MX8 with Label

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

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

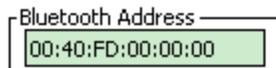
The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes. Refer to the following section titled “[Bluetooth Beep and LED Indications](#)”.

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

MX8 without Label

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

First, locate the MX8 Bluetooth address by tapping Start > Settings > System > Bluetooth > About tab.



Next, create a Bluetooth address bar code label for the MX8. Free bar code creation software is available for download on the world wide web. Search using the keywords “bar code create”.

The format for the bar code label is as follows:

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

Create and print the label.

Scan the MX8 Bluetooth address bar code label with the Bluetooth bar code reader.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes. Refer to the following section titled “[Bluetooth Beep and LED Indications](#)”.

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

Bluetooth Reader Beep and LED Indications

Beep Type from Mobile Bluetooth Device	Beep Pattern
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

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

Upon startup, if the mobile Bluetooth device sounds a long tone, this means the device has not passed its automatic Selftest and has entered isolation mode. If the device is reset, the sequence is repeated. Contact [Technical Assistance](#) for help with a mobile Bluetooth device.

Bluetooth Printer Setup

The Bluetooth managed printer should be as close as possible, in direct line of sight, with the MX8 during the pairing process.

1. Open the EZPair Panel (Start > Settings > System > Bluetooth).
2. Tap Discover. Locate the Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or doubletap) on the Bluetooth printer until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the MX8 with the Bluetooth managed printer.

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

Please refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact [Technical Assistance](#) for Bluetooth product assistance.

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the MX8 and the printer are currently paired.

Certificates

Start > Settings > System > Certificates

Manage digital certificates used for secure communication.

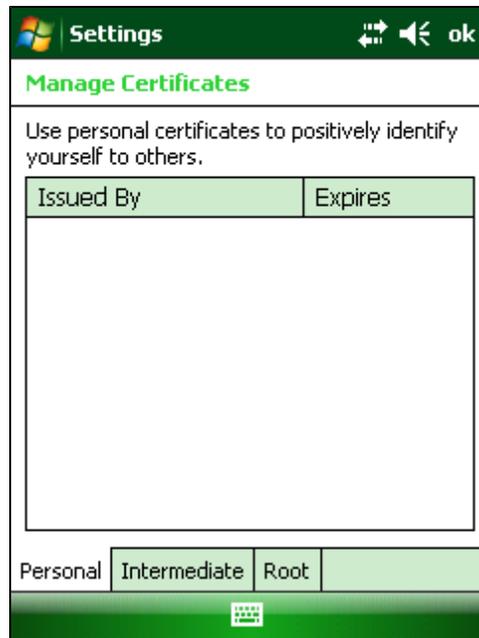
View – displays details of the certificate. Personal certificates may be extended from the view screen.

Delete – removes the certificate from the device. Delete is not available if the certificate was installed by a device administrator.

Certificates are divided into three types: Personal, Intermediate and Root.

See "[Certificates](#)" in the Wireless Network Configuration section for detailed instruction on generating certificates.

Personal



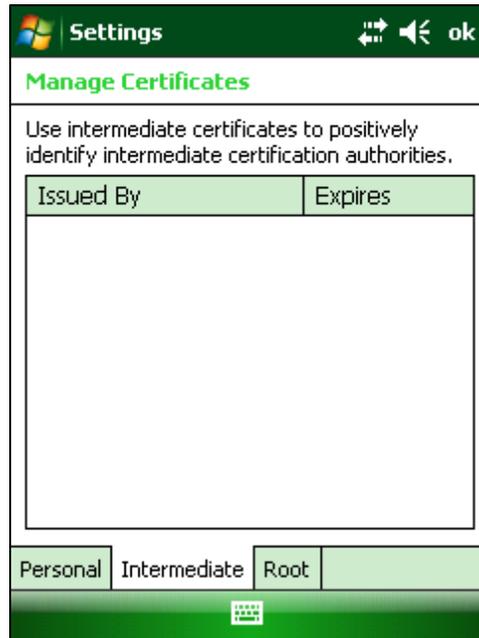
This panel lists any installed Personal certificates. Personal certificates are used to identify the user of the device.

To install a User certificate:

1. Copy the .pfx or .p12 file to a folder on the MX8.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.
3. Type in the password to unlock the certificate and tap Done.

The new certificate is copied to the Personal certificate store on the MX8.

Intermediate



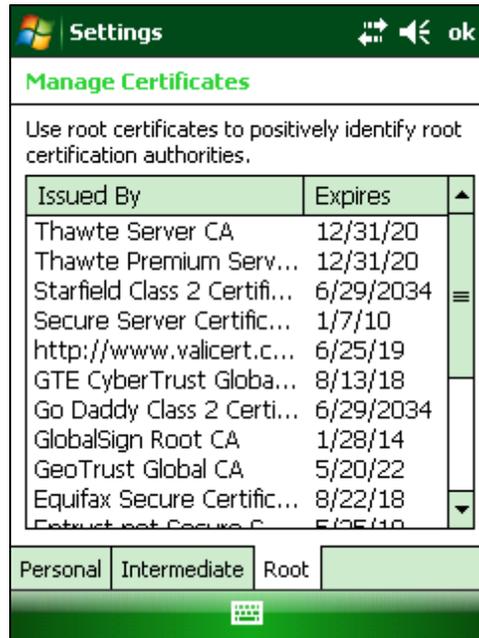
This panel lists any installed Intermediate certificates. Intermediate certificates are used to help authenticate certificates received from other hosts.

To install an Intermediate certificate:

1. Copy a DER-encoded .cer file, a base64-encoded .cer file or a .pfx file to a folder on the MX8.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.

The new certificate is copied to the Intermediate certificate store on the MX8.

Root



This panel lists any installed Root certificates. Root certificates are used to authenticate certificates received from other hosts.

To install a Root certificate:

1. Copy a DER-encoded .cer file, a base64-encoded .cer file or a .pfx file to a folder on the MX8.
2. Use File Explorer to browse to the location of the file and open the file by tapping the file name.

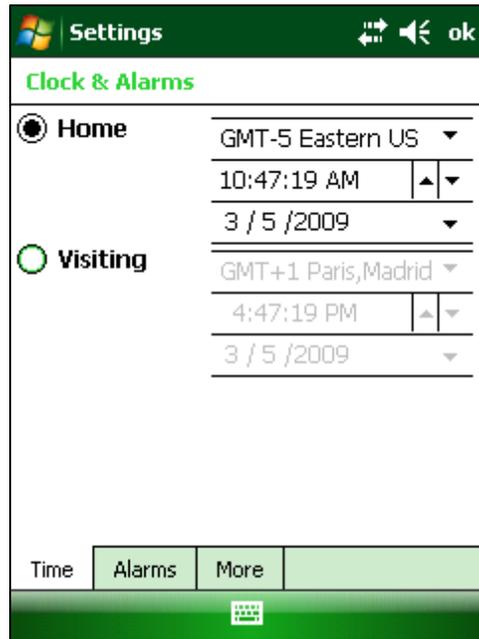
The new certificate is copied to the Root certificate store on the MX8.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Clock & Alarms

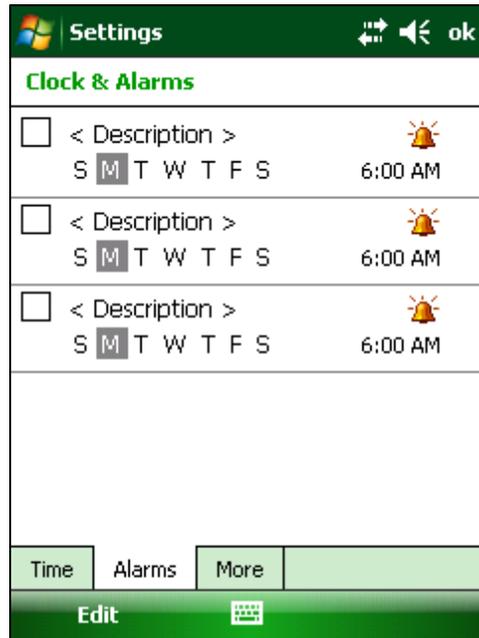
Start > Settings > System > Clock & Alarms

Time



Adjust the settings and tap ok to save the changes. The changes take effect immediately. The Time can be set for both a Home and Visiting location.

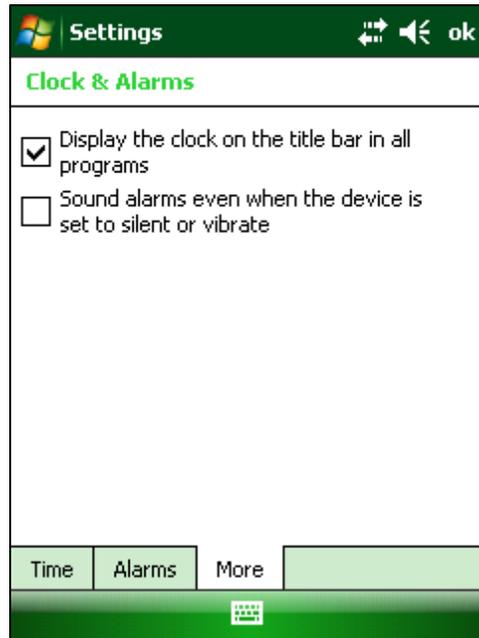
Alarms



To set an alarm:

1. Tap the checkbox to enable the alarm.
2. Tap <Description> and enter a description. The description is limited to 63 characters.
3. Tap the day (or days) to play the alarm.
4. Tap the time to set the time to play the alarm. Set the time and tap ok to return to the Alarms panel.
5. Tap the Bell icon to set the notification. Notifications may include sound, light flash (the Alpha LED flashes) and vibration. Set the desired options and tap ok to return to the Alarms panel.
6. Tap ok when finished to dismiss the Alarms panel.

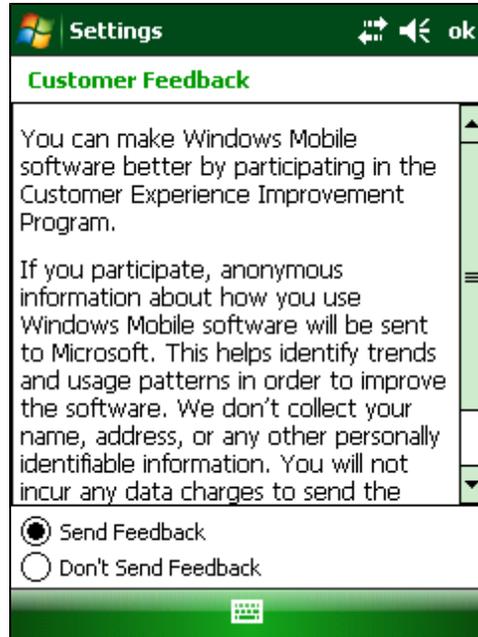
More



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Customer Feedback

Start > Settings > System > Customer Feedback



Elect to send or not send feedback as part of Microsoft's Customer Experience Improvement Program. The default is Send Feedback.

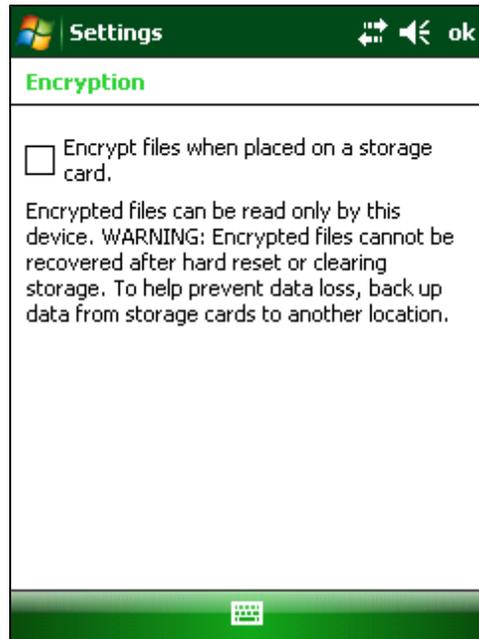
In order to send feedback, the MX8 must have Internet access.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Encryption

Start > Settings > System > Encryption

This panel enables or disables encryption of data files on removable storage cards. The default is Disabled.



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Error Reporting

Start > Settings > System > Error Reporting

This panel enables or disables error reporting to Microsoft.



An Internet connection is required for error reporting.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

External GPS

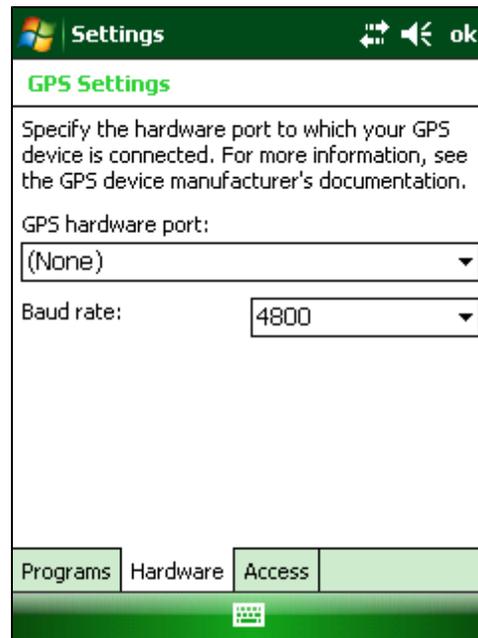
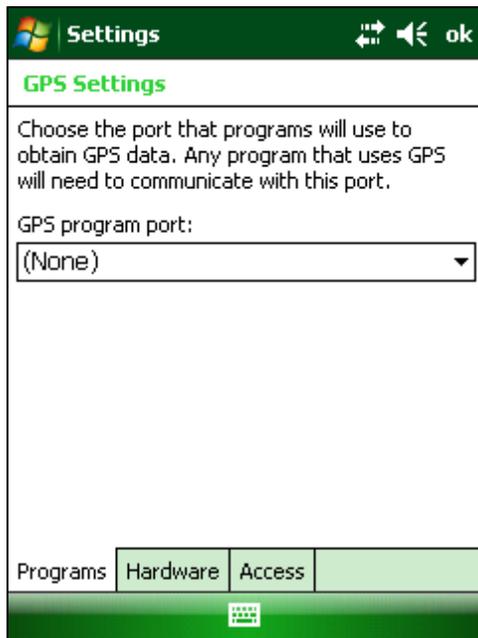
Start > Settings > System > External GPS

Factory Default Settings

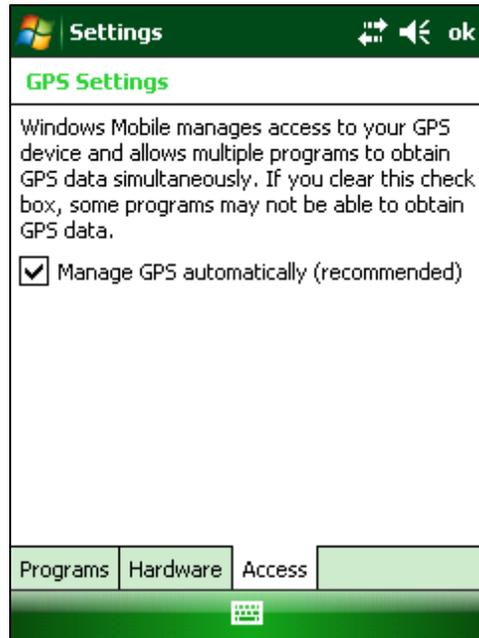
GPS Program Port	None
GPS Hardware Port	None
Baud Rate	4800
Access	Automatic

This panel configures for serial GPS access over hardware serial ports using the Microsoft GPS manager. The port used, baud rate and sharing of the port must be specified.

In order to use the configuration items on these panels, applications must use the Microsoft GPS API interface rather than reading the serial port directly. If the application reads the serial port directly, these settings are not necessary.



Access



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

License Manager

Start > Settings > System > License Manager

Use this option to view software license registration details, and service contract length for a MX8. Information on the License Viewer tabs is unique for each MX8.

Note: Following image is a sample screen.

Your License Manager control panel may show more tabs, e.g., RFTerm, depending on the number of software applications running on the MX8 that require a license. Contact [Technical Assistance](#) for software updates and releases as they become available.



Software and driver version information is located in the **Personal > About MX8WM** control panel. Copyright information is located in the **System > About** control panel.

Managed Programs

Start > Settings > System > Managed Programs

This panel displays the install history for .NET managed programs. The list is read only.



See Also: ["Remove Programs"](#)

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

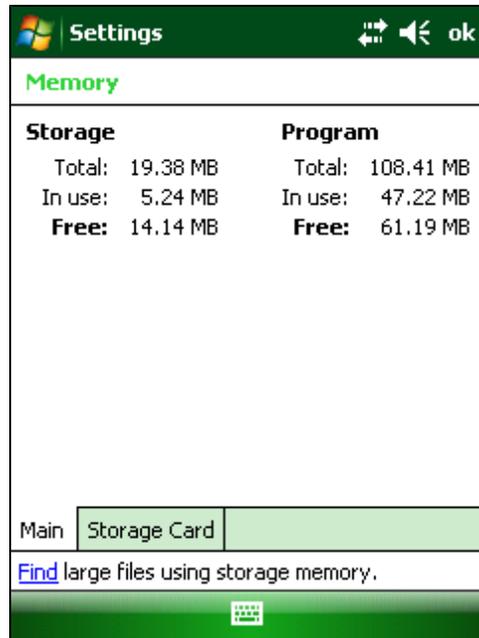
Memory

Start > Settings > System > Memory

These panels report the current state of virtual memory.

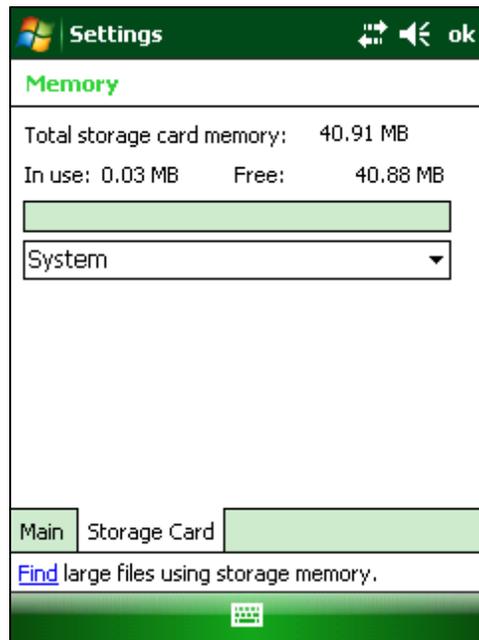
The Find prompt at the bottom of the screen launches the Search utility.

Main



The split between Storage memory and Program memory is not adjustable.

Storage Card



The pop-up list shows all mounted storage, both fixed and removable.

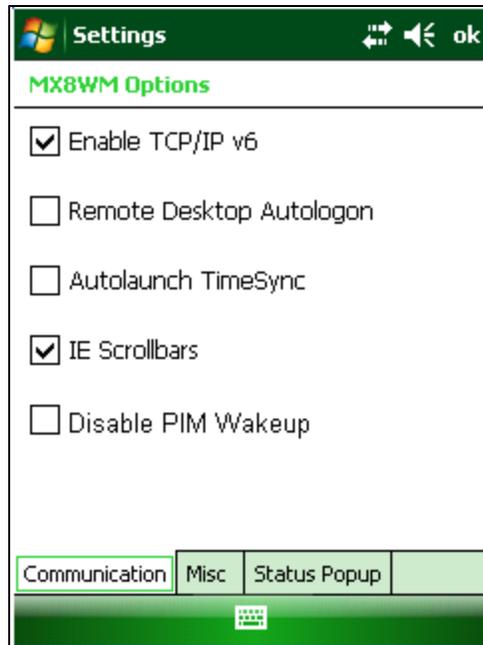
Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

MX8WM Options

Start > Settings > System > MX8WM Options

Set MX8 specific device options.

Communication



By default, **TCP/IP version 6** is enabled. Check this checkbox to disable (unchecked) TCP/IP version 6.

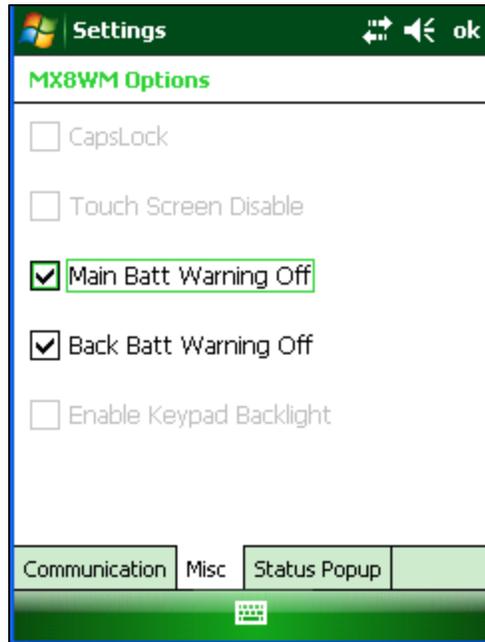
By default, **Remote Desktop Autologin** is disabled. Check this checkbox to enable Remote Desktop Autologin.

Autolaunch TimeSync enables time synchronization when the MX8 boots.

IE Scrollbars allows the scrollbars in Internet Explorer to be turned off when the check box is unchecked.

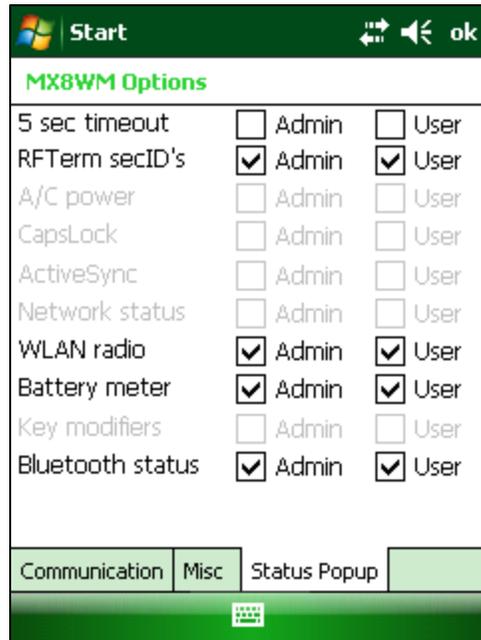
Check the checkbox to enable **Disable PIM Wakeup**. When Disable PIM Wakeup is enabled, the next time the MX8 is in Suspend mode, the MX8 does not wake up to synchronize Outlook.

Misc.



Low battery warnings for the **Main Battery** and the **Backup Battery** are not presented to the user until their check boxes are unchecked. The default setting is both warnings are turned off. CapsLock, Touch Screen Disable and Enable Keypad Backlight are dimmed and cannot be edited by the user.

Status Popup



When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it.

The Status Popup window is closed by pressing the assigned Status User or Status Admin key sequence.

Note: Select a Diamond key for the assigned key sequence to use when opening and closing the popup. If a Function key is used, that Function key is not available to applications that generally use Function keys such as RFTerm.

Using the Buttons settings panel ([Start > Settings > Personal > Buttons > Program Buttons](#)), the System Administrator must first assign a Status User key for the end-user when they want to toggle the Status Popup Window on or off. Select the desired key (F1-F5, D1-D3) and assign that key to StatPopup.

Similarly the System Administrator must also assign a Status Admin key to perform the same function for the Admin popup. Select the desired key (F1-F5, D1-D3) and assign that key to Admin StatPop.

Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g., Network status, WLAN status, Bluetooth status, RFTerm secID's (Secondary ID), etc.

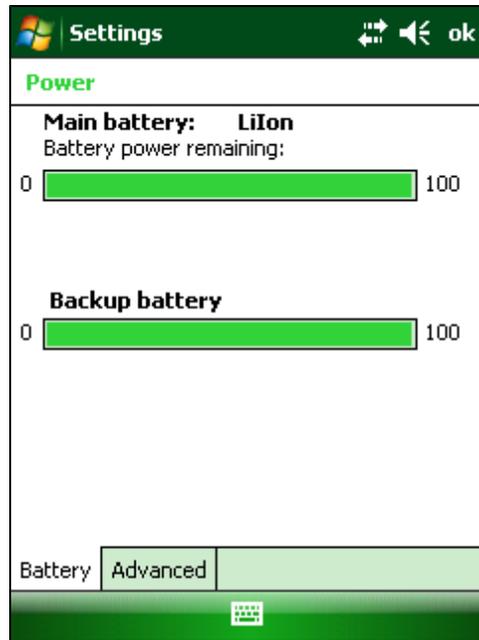
The default setting for the User and Admin status popup windows is to show all status information. The 5-second timeout to remove the status popup from the display is disabled (unchecked) by default for the User and Admin status popup windows.

Power

Start > Settings > System > Power

Reports the current battery state and allows the user to set suspend timeouts.

Battery

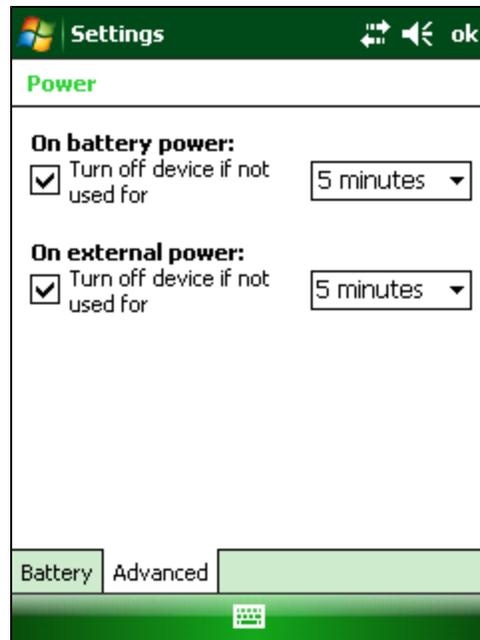


Battery power is displayed for both the main and backup batteries.

Advanced

Factory Default Settings

On battery power:	
Turn off device if not used for	Enabled
Timer setting	5 minutes
On external power:	
Turn off device if not used for	Enabled
Timer setting	5 minutes

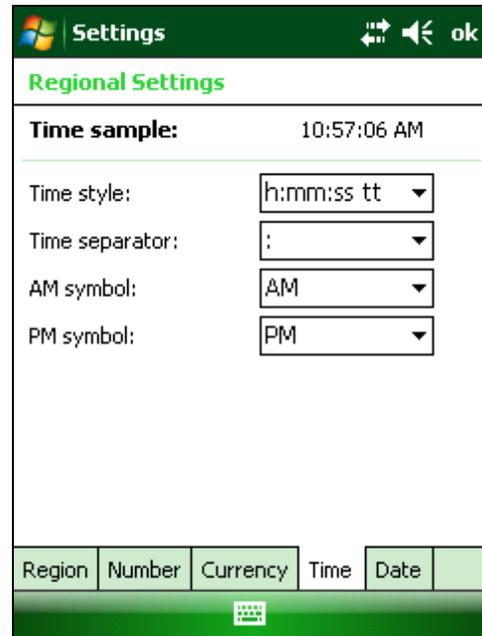
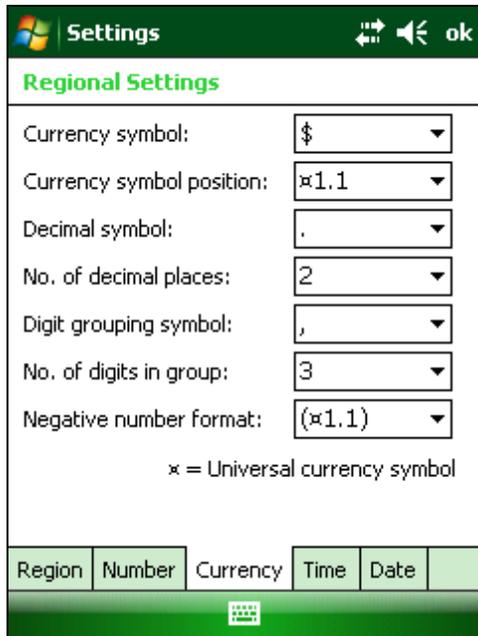
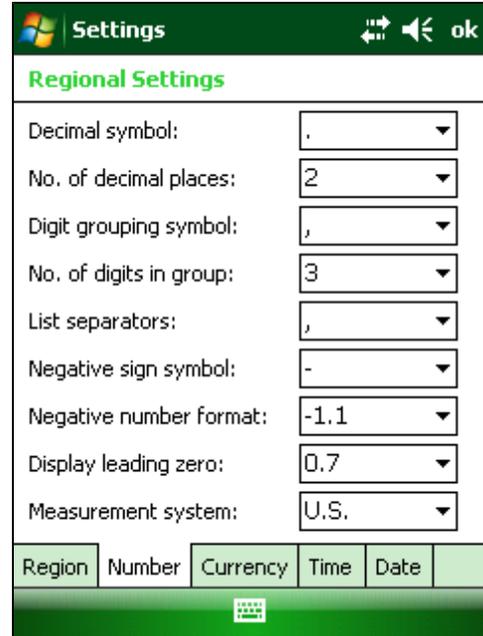
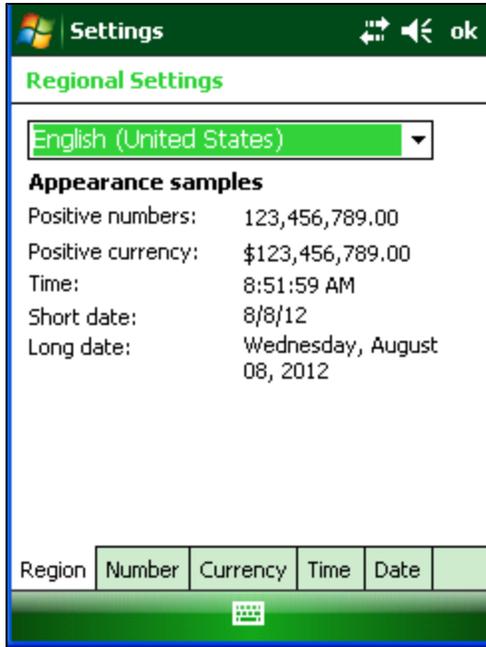


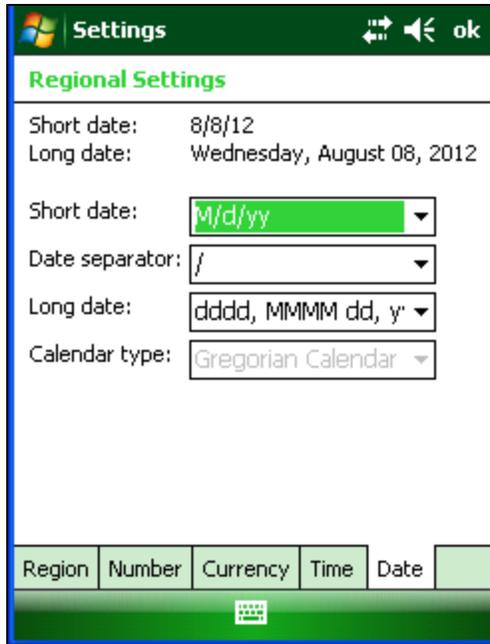
Select the inactivity timeout period before the MX8 goes into suspend. The settings on this panel are for the suspend timers only. Backlight timers are set using the [Backlight](#) settings panel.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Regional Settings

Start > Settings > System > Regional Settings





Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Remove Programs

Start > Settings > System > Remove Programs

This panel is used to uninstall programs. The Remove Program listing is for all programs installed by ActiveSync or a CAB file. Programs installed by a package file are not included in this list.

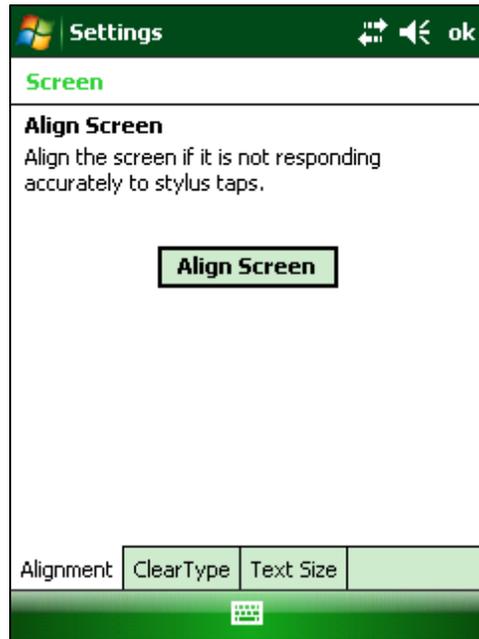


Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Screen

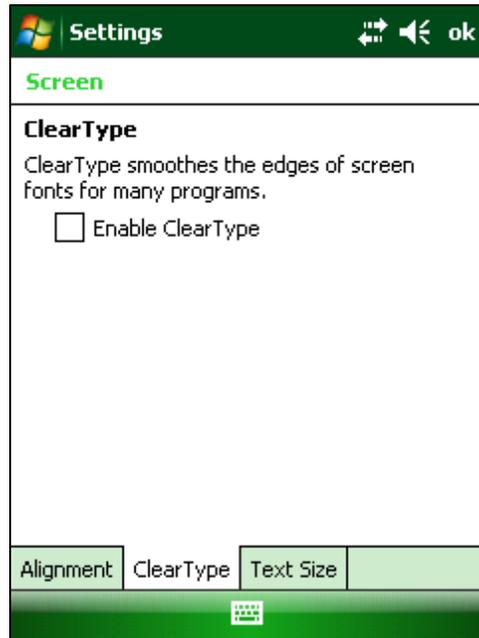
Start > Settings > System > Screen

Alignment



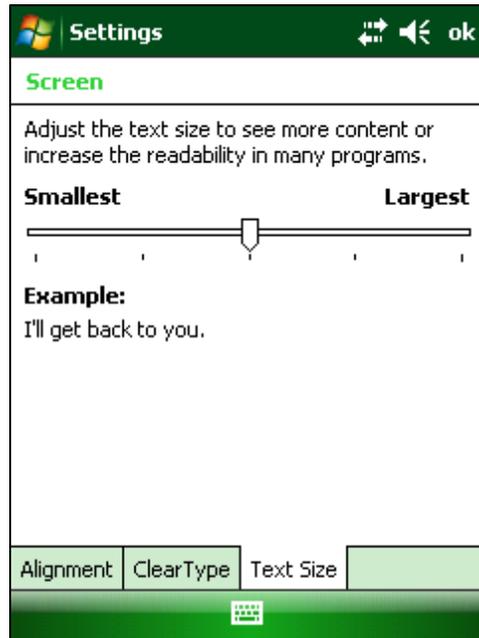
Tap the Align Screen button. The align screen opens and displays a large cross-hair in the middle of the screen. Tap the middle of the cross-hair as it moves around the screen. When the process is complete, the Align Screen is displayed. Tap ok and the changes are saved. The new alignment is in effect immediately.

Clear Type



Tap the Enable ClearType checkbox to enable this option. The default setting is Disabled (unchecked).

Text Size



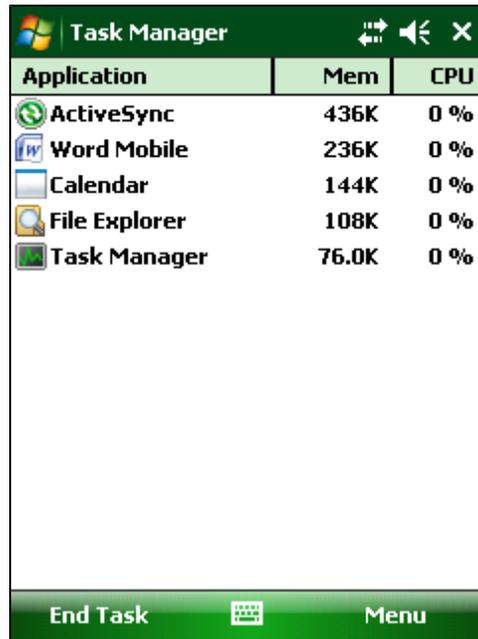
Tap the marker and slide it across the bar. As the marker moves, the example text increases or decreases. Tap ok and the change is saved. The new text size is in effect immediately.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Task Manager

Start > Settings > System > Task Manager

This panel displays all running tasks as well as the CPU bandwidth being used by each task.



Application	Mem	CPU
ActiveSync	436K	0 %
Word Mobile	236K	0 %
Calendar	144K	0 %
File Explorer	108K	0 %
Task Manager	76.0K	0 %

Clicking on the column headings at the top of the screen sorts the tasks by the contents of that column. Clicking the same heading a second time reverses the sort order of that column.

Right-clicking on an application name displays a popup menu with the following choices:

- Switch To – Switch to the highlighted task. Double-clicking on the task name also performs this function.
- End Task – End the selected task only.
- End All Tasks – End all tasks.

The list is reset by cold boot.

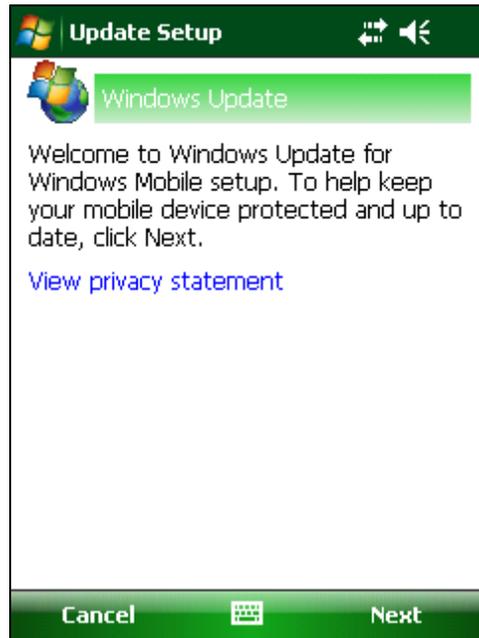
IMPORTANT – Any Windows Mobile program that has been run, even if the program has been exited, remains in memory ready to run again. If memory runs out, the programs are released from memory. However, to avoid out of memory operational problems, it is best to manually terminate unwanted tasks using this option.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Windows Update

Start > Settings > System > Windows Update

Configure Windows Update to check for updates to the Windows Mobile operating system. Requires an active Internet connection.



Click **Next** to configure Windows Update.

The default setting is "Manual", manually download and install important updates.

Automatic checking for updates is available.

Click **Finish** to end the Windows Update setup wizard. Click **ok** to close Windows Update.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

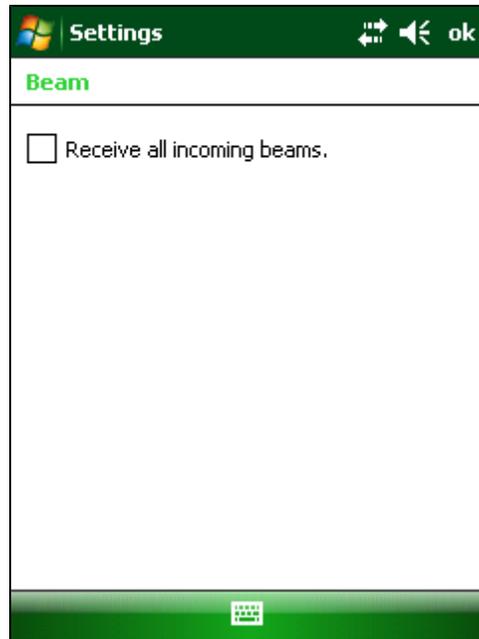
Connections Panel

Beam

Start > Settings > Connections > Beam

Enable or disable receiving OBEX (oBject EXchange) data beams, either by IrDA (Infrared Data Association) or Bluetooth.

Note: The MX8 does not support beaming.

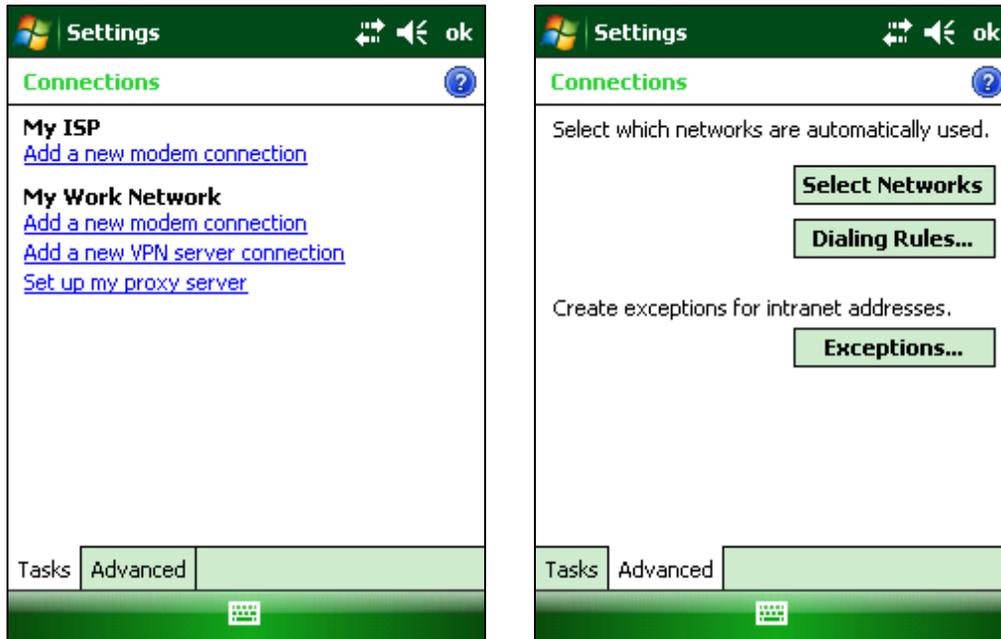


The default setting for Beam Settings is Disabled as the MX8 does not support beaming.

Connections

Start > Settings > Connections > Connections

Configure connections to a host PC.

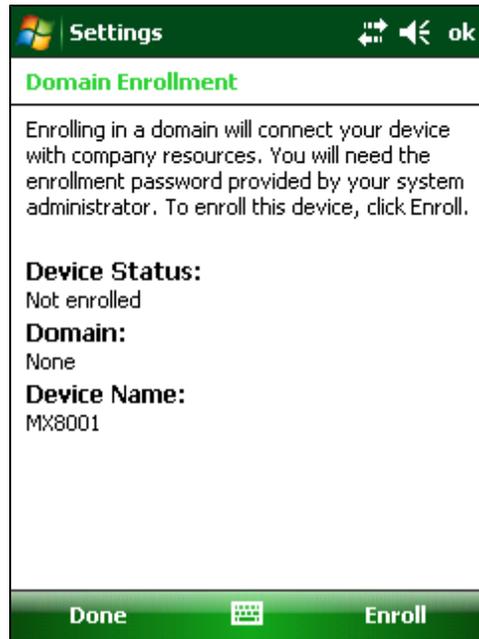


Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Domain Enroll

Start > Settings > Connections > Domain Enroll

Enroll in Active Directory.



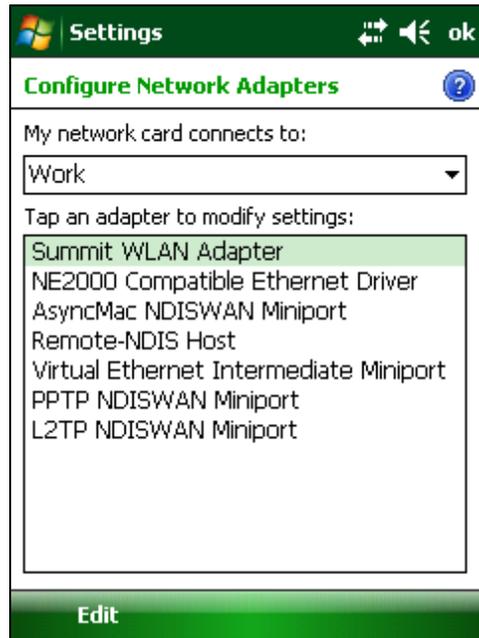
To begin enrollment, click on Enroll in the Status bar. Please contact your system administrator for the applicable information to complete the screens.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

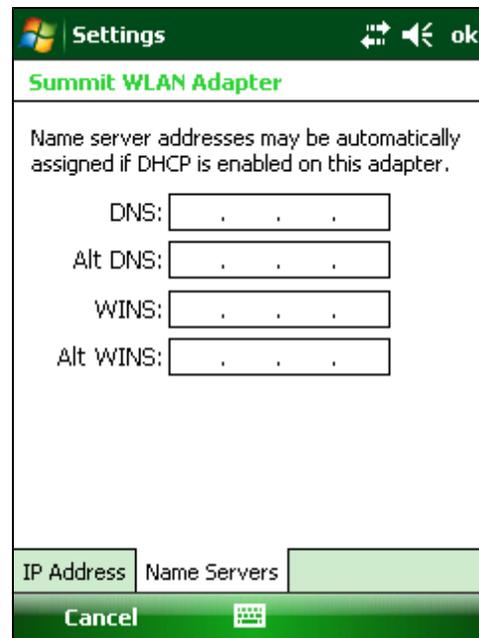
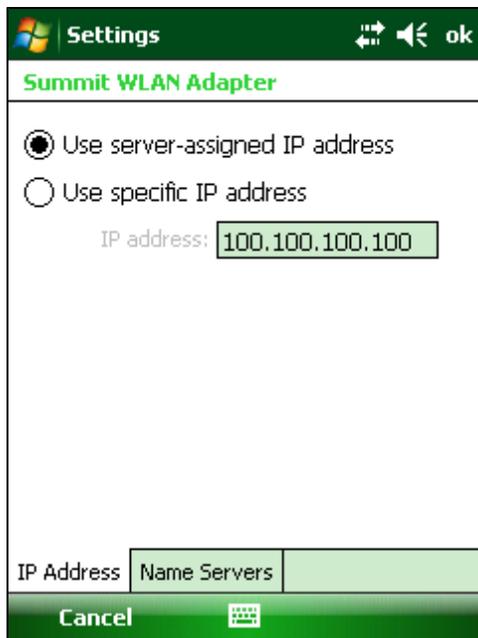
Wi-Fi (Network Adapters)

Start > Settings > Connections > Wi-Fi

When the Summit Configuration Utility is managing network connections, this panel displays a list of **network adapters**. The list is based on drivers installed in the registry whether the adapter is actually supported by the hardware or not.



To configure a network card, click on the adapter name. Enter the IP address (or select server assigned IP address) and the name server addresses.



Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Wi-Fi (Network Access)

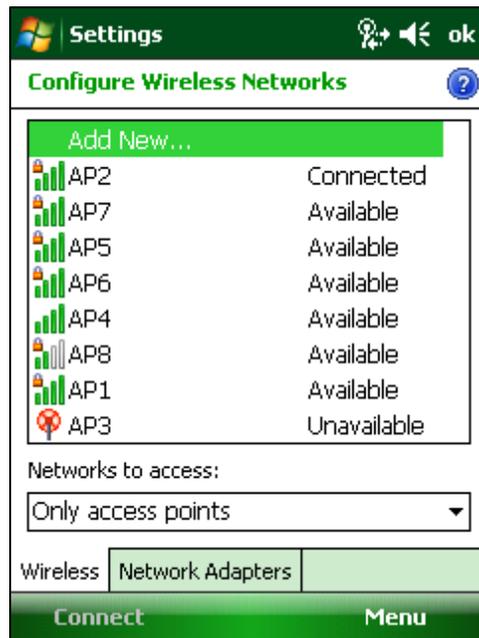
Start > Settings > Connections > Wi-Fi

The Wi-Fi icon is not always displayed. When the Summit Client Utility (SCU) is controlling wireless settings (Start > Settings > System > Wi-Fi), the Wi-Fi icon is not displayed in Connections.

When the Summit Client Utility is set for **Third Party Config**, the Wi-Fi icon is displayed.

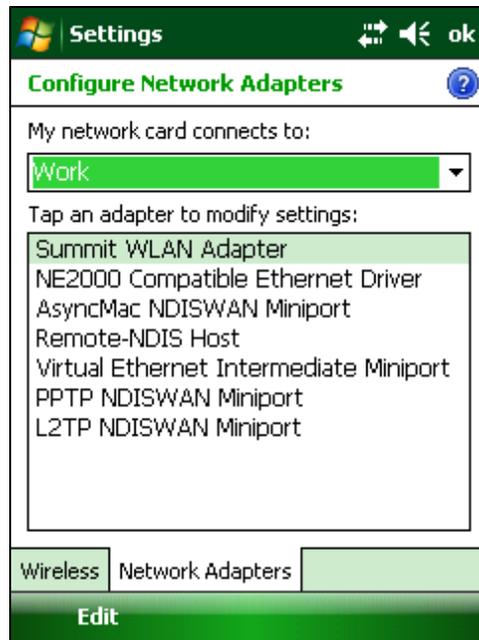
Wireless

For details on the [Wireless Manager](#), see [Wireless Network Configuration](#).



Network Adapters

Please see the previous [Network Adapters](#) section for more details.

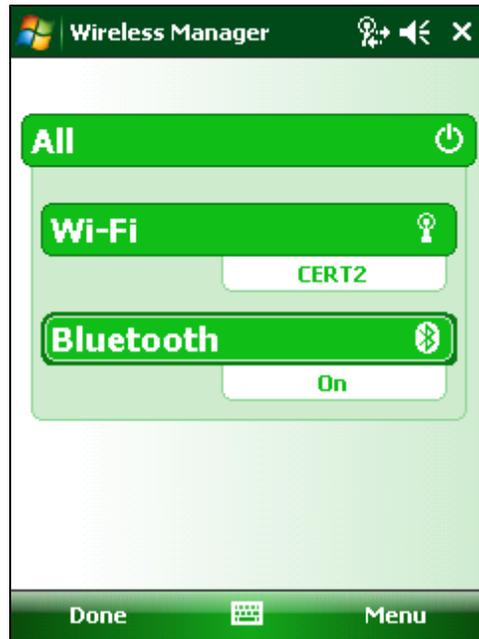


Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

Wireless Manager

Start > Settings > Connections > Wireless Manager

Provides information on the currently connected wireless network(s).



If more than one wireless device is being managed, the All bar is displayed. Tap the All bar to disable/enable all wireless devices at once.

Wi-Fi

If a Wi-Fi (802.11) radio is present, the Wi-Fi bar indicates the status of the Wi-Fi connection, such as:

Off	The Wi-Fi radio is off
On	The Wi-Fi radio is on (the default setting)
Unavailable	No Wi-Fi networks are available
Available	Wi-Fi networks are available but not connected
Connecting	The radio is connecting to a Wi-Fi network
SSID	The SSID of the connected Wi-Fi network when managed by Wireless Manager
Network Card	When the radio is connected and managed by the Summit Client Utility

If the Wi-Fi radio is Off, tapping the Wi-Fi bar turns the radio On. Once the radio is On, the status may cycle through other states such as Available and Connecting before reporting a connection status such as the SSID.

If the Wi-Fi radio is in any other state than Off, tapping the Wi-Fi bar turns the radio Off.

Bluetooth

If Bluetooth is present, the Bluetooth bar indicates the status of the connections, such as:

Off	The Bluetooth radio is off (the default setting)
On	The Bluetooth radio is on
Visible	The MX8 is discoverable

If the Bluetooth radio is Off, tapping the Bluetooth bar turns the radio On. Once the radio is On, it may cycle to Visible if the MX8 is discoverable.

If the Bluetooth radio is in any other state than Off, tapping the Bluetooth bar turns the radio Off.

Note: Tap Start > Help for context sensitive Windows Help when changing or viewing options. Tap the X icon in the top right corner to close Windows Help.

ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the MX8.

Requirement : ActiveSync (version 4.5 or higher for **Windows XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync/Windows Mobile Device Center for the PC is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync/Windows Mobile Device Center on your desktop computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 computer, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync version 4.5 or higher, you can synchronize information on your desktop computer with the MX8 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:

- Synchronize Microsoft Word and Microsoft Excel files between your mobile device and PC. Your files are automatically converted to the correct format.
- Back up and restore your 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.
- Select which information types are synchronized and control how much data is synchronized.

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 your desktop computer and your device.

If an information type is selected that does not exist on the MX8, the data appears to transfer, but it is ignored by the MX8 and not loaded

When installation of ActiveSync is complete on your 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 Install

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

Install ActiveSync on Desktop/Laptop

Install ActiveSync (or Windows Mobile Device Center) using the *Getting Started Disc*. The Getting Started screen should automatically display when the CD is inserted in the PC. If it does not, browse to the CD and click on **Start.exe**.

Select **Setup and Installation**. Click on ActiveSync to install ActiveSync on your PC.

Alternatively, you can go to the Microsoft Windows website and locate the ActiveSync download.

Follow the instructions in the ActiveSync Wizard.

Check that **Start > Programs > ActiveSync > Connections** has the correct connection selected. Refer to “Serial Connection” or “USB Connection”. Note that USB is the default connection type.

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

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

Serial Connection

Tap the **Start > Settings > ActiveSync > Connections** on the MX8. From the popup list, choose **57600 Default**

Note: The default is USB. Using serial ActiveSync at 115 Kb/s is not recommended.

This will set up the MX8 to use COM 1. Tap **ok** to save and exit

USB Connection

Tap the **Start > Settings > ActiveSync > Connections** on the MX8. From the popup list, choose **USB**.

This will set up the MX8 to use the USB configuration. Tap **ok** to save and exit.

Connect -- Initial Install Process

Connect the correct** cable to the PC (the host) and the MX8 (the client). The MX8 attempts to connect as soon as the cable connection is made.

See [Cables](#) for the initial ActiveSync Configuration:

** USB Client to PC/Laptop	MX8051CABLE
** Serial Client to PC/Laptop	MX8055CABLE

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

Synchronize Files

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.

MX8 and PC Partnership

- An ActiveSync partnership between the PC and MX8 has been established.
- Make sure the checkbox is checked for Synchronize all PCs using this connection (Start > Settings > ActiveSync > Connections).

Serial Port Transfer

- A PC with an available serial port. The PC must be running Windows XP or greater.
- "Allow connections to one of the following" is checked and COM1 (or other appropriate PC COM port) is selected from the list on the ActiveSync Connections Settings screen on the PC.
- For best results use the MX8 multipurpose RS232 and Power cable.

USB Transfer

- A PC with an available USB port. The PC must be running Windows XP or greater.
- "Allow USB connections" is checked on the ActiveSync Connections Settings screen on the PC.
- For best results use the MX8 multipurpose USB and Power cable.
- "Allow USB connection with this desktop computer" is checked.

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 using Windows 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).

Disconnect

USB Connection

- Disconnect the USB cable from the MX8.
- Tap the status bar icon in the lower right hand corner of the PC's 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.

Serial Connection

- Disconnect the RS232 cable from the MX8.
- Put the MX8 into Suspend by tapping the red Power button.
- Tap the status bar icon in the lower right hand corner of the PC's 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. ([Start > Settings > About > Device ID](#))

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 Help

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 MX8 is connected to a PC by a cable, disconnect the cable from the MX8 and reconnect it again.

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

[See Also: "Cold Boot and Loss of Host Re-connection"](#)

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

Solution 1: ActiveSync icon on the PC does not turn green after connecting USB cable from MX8.

1. Disconnect MX8 USB cable from PC.
2. Suspend/Resume the MX8.
3. In ActiveSync > File > Connection Settings on PC disable 'Allow USB Connections' and click OK.
4. Re-enable 'Allow USB Connections' on the PC and click OK.
5. Reconnect USB cable from MX8 to PC.

Solution 2: 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.

Configuring with HSM Connect

HSM Connect allows a user to view the MX8 screen remotely from a PC using an ActiveSync connection:

Requirement : ActiveSync (version 4.5 or higher for **Windows XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC are available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

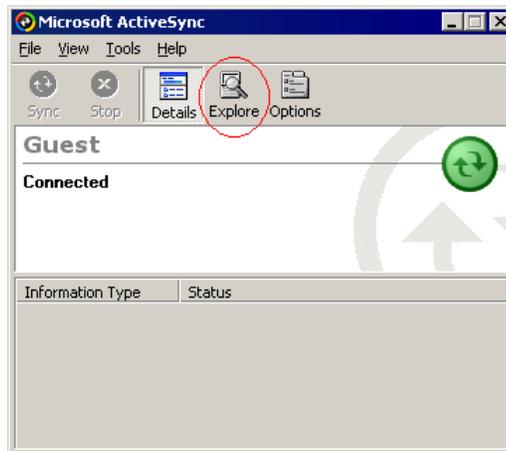
Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

ActiveSync is already installed on the MX8. HSM Connect is available for download from the *Getting Started Disc*. The MX8 is preconfigured to establish a USB ActiveSync connection to a PC when the proper cable is attached to the MX8 and the PC.

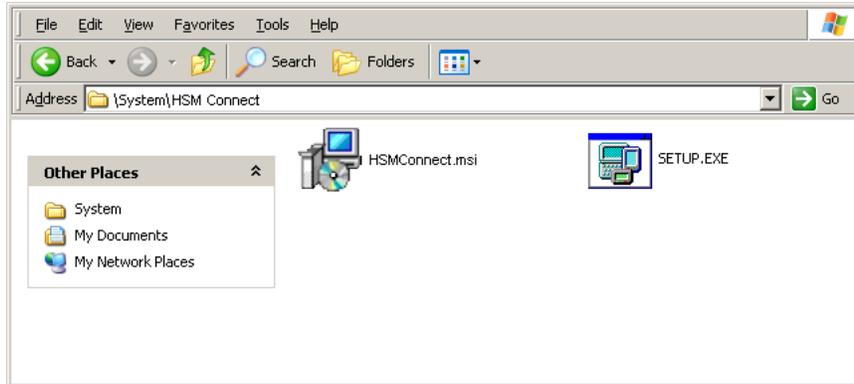
If the MX8 uses a serial port for ActiveSync, it will be necessary to configure the MX8 to use the serial port. Complete details on the proper cables and port configuration are included in [Initial Install](#).

Install HSM Connect

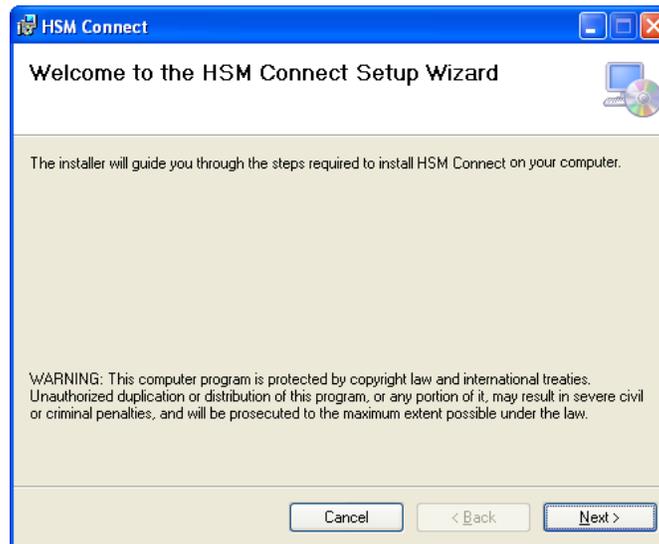
1. Install Microsoft ActiveSync on a PC with a USB port. For details, please see [Initial Install](#).
2. Power up the MX8.
3. Connect the MX8 to the PC using the proper connection cable. Once connected, the ActiveSync dialog box appears. If using the USB connection, the ActiveSync connection is automatically established. If using a serial connection, it is necessary to initiate the connection from the MX8.
4. Select "No" for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use HSM Connect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in ActiveSync Help.
5. When the ActiveSync screen appears, select Explore.



6. An explorer window is displayed for the MX8. Browse to the `\System\HSM Connect` folder. HSM Connect is available on the *Getting Started Disc*. Contact [Technical Assistance](#) for the files, if necessary.



7. Select and copy the HSMConnect.msi and Setup.exe files from the MX8 to the user PC. Note the location chosen for the files.
8. Close the ActiveSync explorer dialog box. Do not disconnect the MX8 ActiveSync connection.
9. Execute the Setup.exe file that was copied to the user PC. This setup program installs the HSMConnect utility.



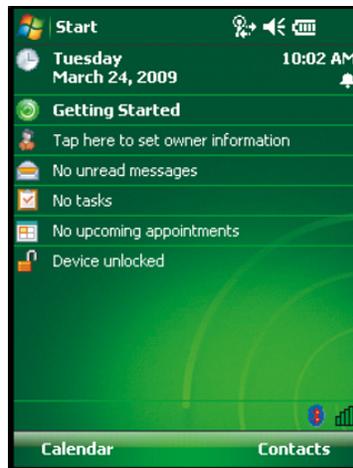
10. Follow the on screen installation prompts. The default installation directory is C:\Program Files\Honeywell Inc\HSM Connect.
11. When the installation is complete, create a desktop shortcut to the following file: C:\Program Files\Honeywell Inc\HSM Connect\HSMConnect.exe. If a different directory was selected during installation, please substitute the appropriate directory.
12. HSMConnect is now installed and ready to use.

Using HSM Connect

1. If an ActiveSync connection has not been established, connect the MX8 to the PC.
2. Double-click the HSMConnect icon that was created on the desktop.
3. HSM Connect launches.



4. Click the OK button to dismiss the About CERDisp dialog box on the desktop by clicking the OK button in the HSM Connect window on the PC desktop. The dialog box automatically times out and disappears after approximately 30 seconds.



5. The MX8 can now be configured from the HSMConnect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the MX8.
6. When the remote session is completed, terminate the HSMConnect program by selecting File > Exit or clicking on the X in the upper right hand corner to close the application, then disconnect the ActiveSync cable.

Note: After using HSM Connect, the MX8 cannot go into Suspend mode until after a warmboot. If using Power Management on a MX8, always warmboot the MX8 when finished using HSM Connect.

Chapter 5: Data Collection

This software component is the interface between data collection devices such as bar code scanners, or imagers, integrated into your MX8, bar code scanners externally connected to a COM port or bar code scanners wirelessly connected via Bluetooth to your MX8. This software component collects the data from the varied sources and presents it to applications on your MX8 in a transparent manner.

Note: When a HID enabled USB scanner is connected to the MX8 the scanned data is transmitted to the active window as keystroke messages. The data bypasses the data collection wedge. Any data handling to be applied to the scanned data, for example strip leading or trailing characters, must be programmed into the scan engine using configuration bar codes or handled by the application accepting the data.

Use the options on the control panels to set data collection keyboard wedge parameters, enable or disable allowed symbologies, set the active scanner port, and assign scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Parameters on the Main tab and the COM tab(s) apply to this device only.

Bar code manipulation parameter settings on the Data Options tab are applied to the incoming data resulting from successful bar code scans received by the MX8 for processing. The successful bar code scan data may be sent by an integrated scanner in the endcap, a wireless Bluetooth Handheld Scanner, or a tethered serial scanner.

Scanner configuration can be changed using the Data Collection settings panels or by the API functions. While the changed configuration is being read, the Scanner LED is solid amber. The scanner is not operational during the configuration update.

Bar Code Readers

Your MX8 may have any of the following integrated bar code readers (Start > Settings > System > Data Collection About):

- 1D Linear Imager, EV-15 (identified as Intermec)
- 2D Area Imager, 5300 (identified as HHP)
- Short Range Laser Scanner, 955I
- Base Laser Scanner, 955E
- Honeywell Laser Scanner, N43XX

Note: If the SPN number on the label on the back of your MX8 ends in Rev B, your device has an integrated N43XX scan engine. For example, SPN: MX8X9X9X9X9X9XX Rev B.

Note: Base Laser Scanner, 955E does not support aim mode. Any attempt to adjust the aiming beam using 955 programming bar codes will fail. The Base Laser scanner does not decode Codablock, Code93i or Telepen symbologies.

Return to Factory Default Settings

After scanning the scanner-engine-specific bar code to reset all scanner parameters to factory default settings (i.e., Reset All, Set Factory Defaults, Default Settings, etc.), the next step is to open the Data Collection settings panel. Tap ok and close the Data Collection panel. This action will synchronize all scanner formats for your device. Another option you can use to reset the Data Collection panel is to scan the LXEReset bar code (for Symbol and Hand Held Products scan engines) or the N43Reset bar code (for the Honeywell Laser Scanner N43XX) located in the *Integrated Scanner Programming Guide*. The MX8 will beep twice when a configuration bar code is successfully scanned.

Using Programming Bar Codes

Engine specific configuration bar codes are contained in the *Integrated Scanner Programming Guide*. They can be used to set or reset scan engine parameters by scanning a bar code, then saving the change. Honeywell, Symbol and Intermec scan engines can be programmed using programming bar codes. The MX8 will beep twice when a configuration bar code is successfully scanned.

Hand Held Products Imager

There are no configuration bar codes for this imager. Use the HHP Properties button on the Data Options tab and the Advanced button available on many of the individual Symbology Settings screens to configure the Hand Held Products Imager.

Data Processing Overview

Bar code data processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Symbology Settings panels. The steps are presented below in the order they are performed on the scanned data.

1. Scanned data is tested for a **code ID** and length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the bar code data is processed based on the settings for All.
 2. If the symbology is **disabled**, the scan is rejected.
 3. Strip **leading** data bytes unconditionally.
 4. Strip **trailing** data bytes unconditionally.
 5. Parse for, and strip if found, **Data Options** strings.
 6. Replace any **control characters** with string, as configured.
 7. Add **prefix** string to output buffer.
 8. If **Code ID** is *not* stripped, add saved **code ID** from above to output buffer.
 9. Add processed **data string** from above to output buffer.
 10. Add **suffix string** to output buffer.
 11. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
 12. 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).
 13. If key output is disabled, a windows message is broadcast to notify listening applications that data is available.
- The manipulated data is ready to be read by applications.

Main Tab

Start > Settings > System > Data Collection > Main tab

Factory Default Settings

Device 1	Disabled
Device 2	Internal
Device 3	Disabled
Keep Awake	Disabled
Send Key Messages	Enabled
Scan Mode - Continuous	Disabled
Scan Mode - Timeout between same symbol	1 second

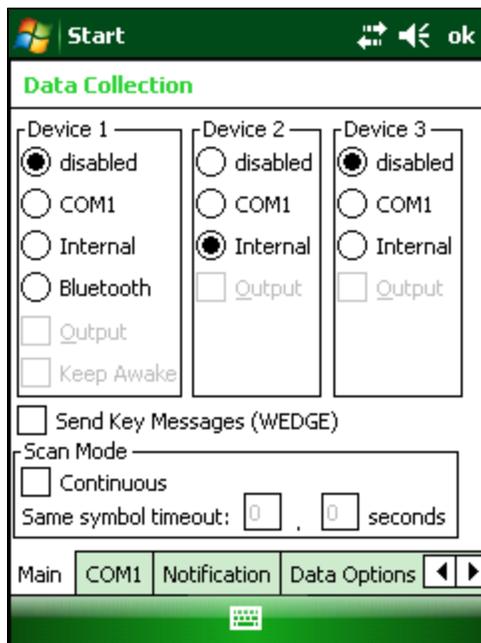
Device 1 – Internal. Radio button allows scanner input/output on Device 1 (scan key or trigger).

Device 2 – Output is enabled when COM1 is enabled on this port.

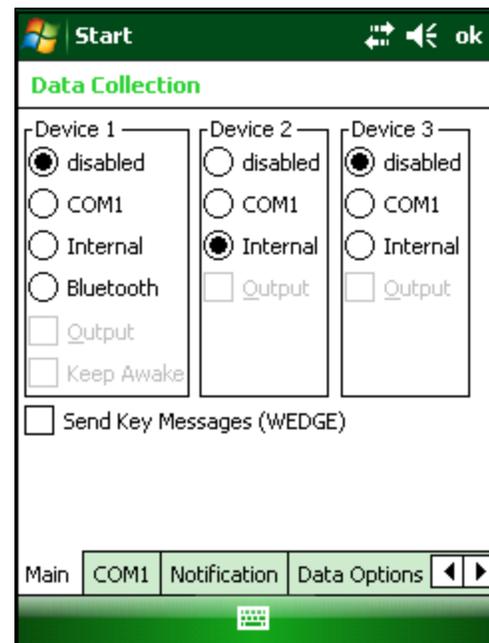
Device 3 – Output is enabled when COM1 is enabled on this port.

The Data Collection Wedge supports up to three concurrent data collection devices. For example, the internal scanner could be used to collect data at the same time a Bluetooth scanner is paired and/or a serial device is attached to COM1 (the MX8 must be in a desktop cradle to use a tethered scanner).

Note: Since Internal is the default setting for Device 2, a Bluetooth scanner can be paired with the Wedge using EZPair on Device 1 without disabling the internal scanner.



Device with integrated Symbol Scanner



Device with any other imager/scanner

Note: The Scan Mode (Continuous Scan) section is only present if the MX8 is equipped with a Symbol integrated scanner. Adjust the settings and tap ok to save the changes. The changes take effect immediately.

Continuous Scan Mode

Start > Settings > System > Data Collection > Main

Continuous scan mode is only available if the MX8 is equipped with a Symbol or Honeywell scanner. Continuous scan mode draws power from the main battery every time a scan read/decode sequence is performed.

Enabling Continuous Scan Mode will ensure the laser is always on and decoding. Do not scan decoder engine configuration bar codes when Continuous Scan Mode is on. Configuration bar codes do not decode when scanned while Continuous Mode is On.



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

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

If trigger mode, power mode, or timeout between same symbol parameters are changed using external configuration bar codes in the *Integrated Scanner Programming Guide*, the operating system automatically restores the parameters to their programmed settings upon a suspend/resume or cold boot and/or any change made in the Data Collection settings. The MX8 will beep twice when a configuration bar code is successfully scanned.

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

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

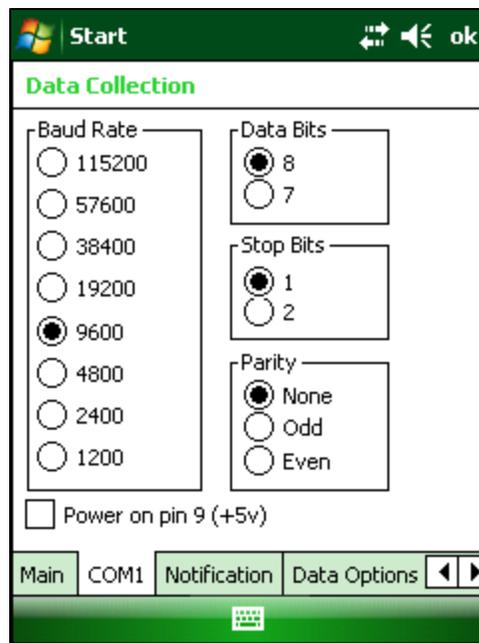
Switching to and from continuous and normal trigger modes is in effect after upon tapping the ok button and waiting for the amber scan LED to go out. A cold boot is not required or necessary.

COM1 Tab

Start > Settings > System > Data Collection > COM1 tab

Factory Default Settings

Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Power on pin 9	Disabled



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

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

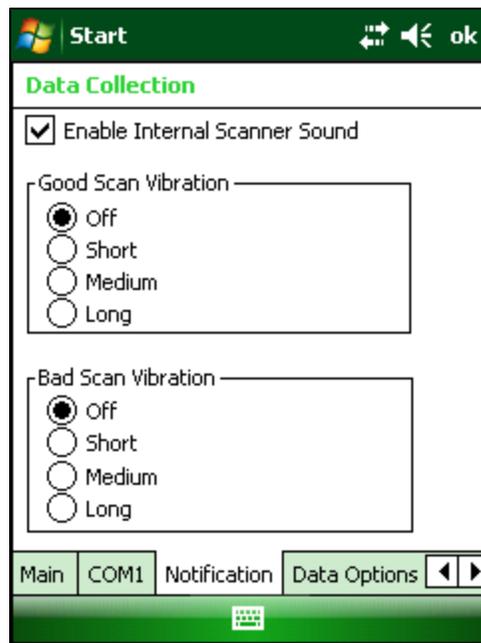
Note: COM1 does not support 5V switchable power on Pin 9 for tethered scanners.

Notification Tab

Start > Settings > System > Data Collection > Notification tab

Factory Default Settings

Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Off
Bad Scan Vibration	Off



This panel toggles internal scanner sounds on and off. Internal scanner sound, by default, is enabled.

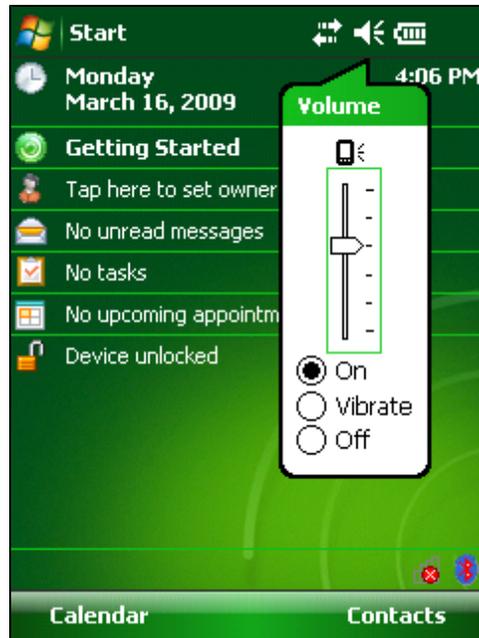
Vibration

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

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

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

Since the Data Collection Wedge uses the operating system interface to sound beeps, if the volume/vibrate icon is set to anything other than On, Wedge beeps do not sound. Wedge vibration is not affected by these settings.



Data Options Tab

Start > Settings > System > Data Collection > Data Options tab

Bar code manipulation parameter settings on this tab are applied to the incoming data resulting from successful bar code scans sent to the MX8 for processing.

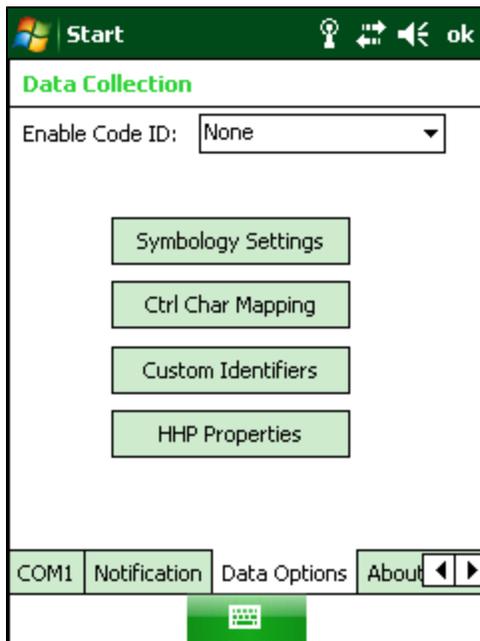
Note: The Data Options tab contains only those options available for one type of decoding engine.

The Data Options tab contains several options to control bar code processing. Options include:

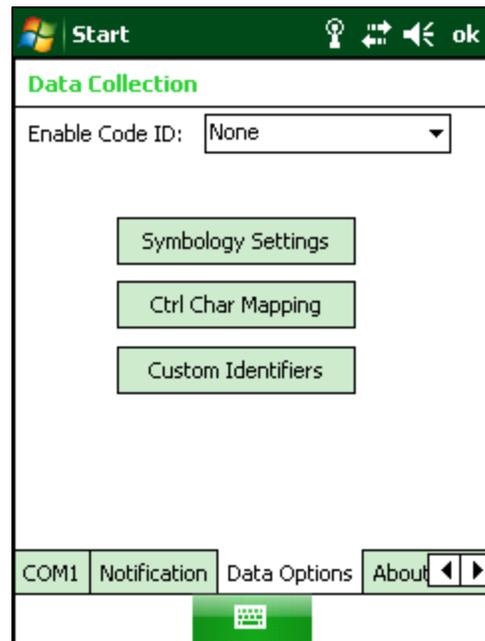
- Defining custom Code IDs
- Disable processing of specified bar code symbologies
- Rejecting bar code data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified bar code data strings
- Replacing control characters
- Adding a prefix and a suffix.

Factory Default Settings

Enable Code ID	None
----------------	------



MX8 with a Hand Held Products imager



MX8 with any other imager/scanner

Note: The HHP Properties button is only present if the MX8 is equipped with a Hand Held Products imager.

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

*HHP - Hand Held Products

For MX8 with Intermec or Symbol

Data Collection Wedge can only enable or disable the processing of a bar code inside the Wedge software.

Enabling or disabling a specific bar code symbology at the scanner/imager is done manually using the configuration bar code in the *Integrated Scanner Programming Guide*.

For MX8 with Hand Held Products

Data Collection Wedge enables or disables the bar code at the imager as well as enabling or disabling the bar code processing in the Wedge software.

Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of bar code 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 bar code 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 bar code. The combo box in the Symbology panel is loaded with the known AIM ID symbologies for that platform, plus any configured Custom code IDs.
Honeywell ID	Programs the internal scanner to transmit the Honeywell ID with each bar code. The combo box in the Symbology panel is populated with the known Honeywell ID symbologies for that platform, plus any configured Custom code IDs.
Symbol	Programs the internal scanner to transmit the Symbol ID with each bar code. The combo box in the Symbology panel is populated with the known Symbol ID symbologies for that platform, plus any configured Custom Code IDs.
HHP	Programs the internal scanner to transmit the HHP ID with each bar code. The combo box in the Symbology panel is populated with the known HHP ID symbologies for that platform, plus any custom Code IDs. HHP = Hand Held Products.
Custom	Does not change the scanner's Code ID transmission setting. The combo box in the Symbology 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 bar code data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e., treated as a Code ID).
- UPC/EAN Codes only: The Code ID for supplemental bar codes is not stripped.
- When Enable Code ID is set to AIM, Symbol or HHP, 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.
- Intermec and Symbol equipped devices are configured using configuration bar codes. When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 'JA1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID : JA1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- The external scanner operation cannot be controlled by the MX8 scanner driver; therefore, a 'good' beep may be sounded from the external scanner even if a bar code from an external scanner is rejected because of the configuration specified. The MX8 will still generate a 'bad' scan beep, to indicate the bar code has been rejected.

Buttons

Symbology Settings	Individually enable or disable a bar code from being scanned, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Barcode Data) add a prefix or suffix to a bar code before transmission.
Ctrl Char Mapping	Define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes.
Custom Identifiers	Defines an identifier that is at the beginning of bar code 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.
HHP Properties	Set properties for a Hand Held Products imager including centering, mode, range, AIM timer and light behavior. Note that the HHP Properties button is only present if the MX8 is equipped with a Hand Held Products imager.

Symbology Settings

Start > Settings > System > Data Collection > Symbology Settings button

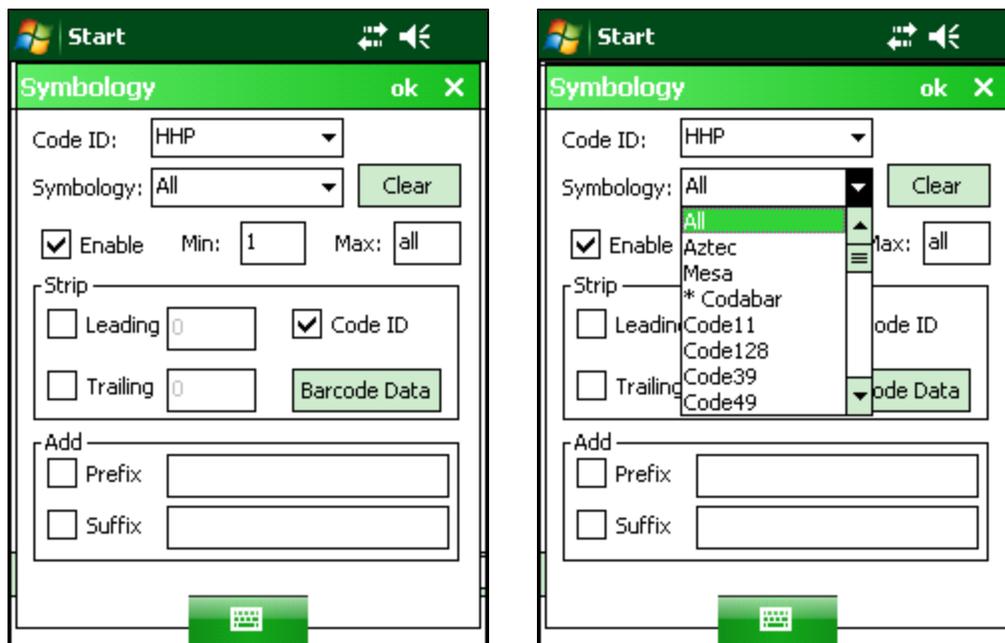
The Symbology selected in the Symbology drop down list defines the symbology for which the data is being configured. The features available on the Symbology panel include the ability to

- individually enable or disable a bar code from scanning,
- set the minimum and maximum size bar code to accept,
- strip Code ID,
- strip data from the beginning or end of a bar code,
- or (based on configurable Barcode Data) add a prefix or suffix to a bar code.

The Code ID drop down box only filters the available symbologies in the Symbology drop down box by the selected Code ID. This Code ID box does not enable or disable the Code ID as that function is controlled by the Enable Code ID box on the Data Options tab.

The Symbology drop down box contains all symbologies **supported by the device selected on the Main tab**. 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 ok is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop down list.



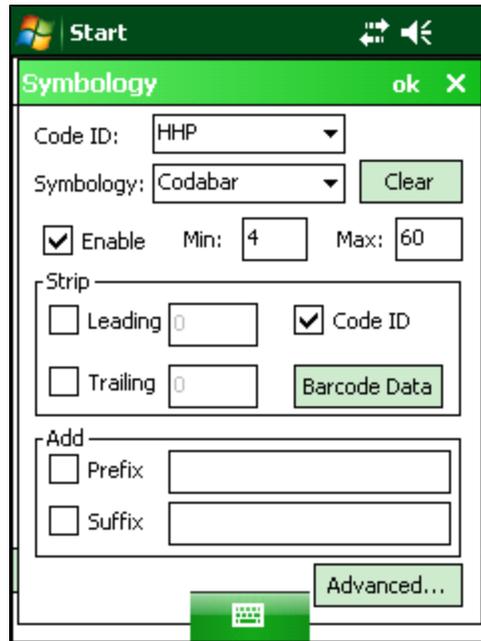
Clear Button

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. Click the Yes button and all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

Advanced Button

If there are advanced configuration options for the selected symbology, an Advanced button is displayed in the lower right corner of the panel. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.



Because the Hand Held Products imager does not support configuration bar codes, the Advanced function allows configuration parameters to be set for many of the supported bar codes.

Processing Order

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Data Options 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 Data Options tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

Enable, Min, Max

Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the bar code data for the type of ID specified in the Data Options tab – Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming bar code data, if the symbology is disabled, the bar code is rejected. Otherwise, the other settings in the dialog are applied and the bar code is processed.

If the symbology is disabled, all other fields on this dialog are dimmed.

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 bar code data (not including Code ID) must meet to be processed.

Any bar code scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

Max

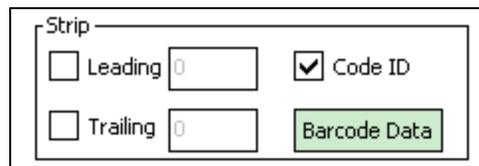
This field specifies the maximum length that the bar code data (not including Code ID) can be processed. Any bar code scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

Start > Settings > System > Data Collection > Symbology button

This group of controls determines what data is removed from the collected data before the data is buffered for the application. When 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.



The screenshot shows a control panel titled "Strip". It contains four elements: a checkbox labeled "Leading" followed by a text input field containing "0"; a checked checkbox labeled "Code ID"; a checkbox labeled "Trailing" followed by a text input field containing "0"; and a green button labeled "Barcode Data".

If the total number of characters being stripped is greater than the number of characters in the collected 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 collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

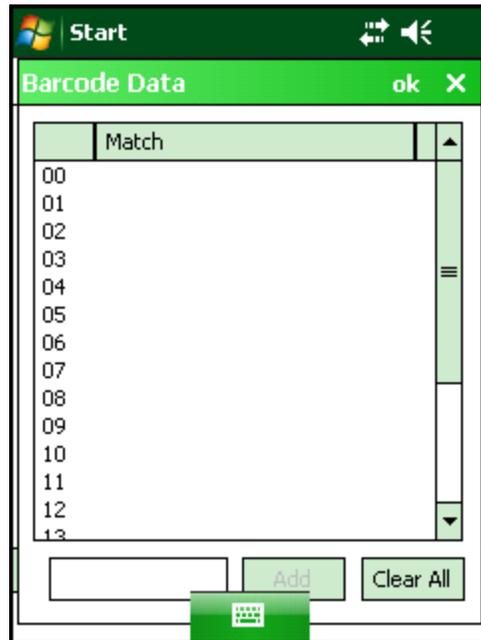
Code ID

Strips the Code ID based on the type code ID specified in the Enable Code ID field in the Data Options tab. By default, Code ID stripping is enabled for every symbology (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

Barcode Data Panel

Tap the Barcode Data button. This panel is used to strip data that matches the entry in the Match list from the bar code. 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 ok to store any additions, deletions or changes.

Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Click 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 click the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace . When Replace is clicked, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, clicking 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. Click the desired line item and then click 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.

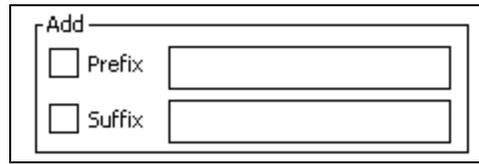
- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length bar code, a good beep will still be emitted, since bar code data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains **ABC** and **AB**, in that order, incoming data with **ABC** will match first, and the **AB** will have no effect.
- When a match between the first characters of the bar code and a string from the list is found, that string is stripped from the bar code 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 bar code data. The string **ABC*** strips off the prefix **ABC**. The string ***XYZ** will strip off the suffix **XYZ**. The string **ABC*XYZ** will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard **?** may be used to match any single character in the incoming data. For example, the data **AB?D** will match **ABCD**, **ABcD**, or **AB0D**, but not **ABDE**.
- The data collected is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the bar code data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the bar code 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



The image shows a control panel titled "Add" with a double-line border. Inside, there are two rows. The first row has a checkbox labeled "Prefix" followed by a rectangular text input field. The second row has a checkbox labeled "Suffix" followed by another rectangular text input field.

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.

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 bar code 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 "[Hat Encoding](#)" 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 bar code 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 bar code data is processed, the Suffix string is sent to the output buffer after the bar code 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.

Symbologies

Your MX8 may have any of the following integrated bar code readers:

- Intermec - 1D Linear Imager, EV-15
- HHP - 2D Area Imager, 5300
- Symbol - Short Range Laser Scanner, 955I
- Symbol - Base Laser Scanner, 955E
- Symbol - Multi-Range "LORAX" Laser, 1524ER
- Honeywell - Laser Scanner, N43XX

The Code ID drop-down box filters the available symbologies, in the Symbology drop down box, by the selected Code ID.

When a Honeywell scan engine is installed, AIM, Custom and Honeywell symbologies are displayed.

When a Hand Held Products imager scan engine is installed, AIM, Custom and HHP symbologies are displayed. HHP does not support Intermec or Symbol IDs.

When a Symbol scan engine is installed, AIM, Custom and Symbol symbologies are displayed. Symbol does not support Intermec, HHP IDs (Hand Held Products) or Honeywell IDs.

AIM Symbologies

Note: When the integrated scan engine is a EV-15, Honeywell or Symbol scan engine, AIM IDs apply, but Advanced properties do not.

EV-15 Engine	Symbol Engine	Honeywell Engine
All	All	All
Code39	Aztec	Codabar
EAN128	Codabar	Code 11
Code128	Code 128	Code 128
UPC/EAN	Code 39	Code 39
Codabar	UPC/EAN	Code 93
Code93	Code 49	EAN/UPC
Code11	Code 93	GS1 Databar
Interleaved 2 of 5	Data Matrix	Interleaved 2 of 5
MSI	Interleaved 2 of 5	Matrix 2 of 5
Discr2of5	MaxiCode	MSI
RSS14	MicroPDF	NEC 2 of 5
PDF417	PDF417	Plessey
Other	PosiCode	Str2of5
Plessey	QR Code	Telepen
QR	GS1 DataBar	Trioptic Code
Maxicode		China Post
DataMatrix		

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

HHP Symbologies

Advanced properties are available when an integrated Hand Held Products imager is installed in the MX8. Advanced properties are applicable regardless of the ID type selected (AIM or HHP).

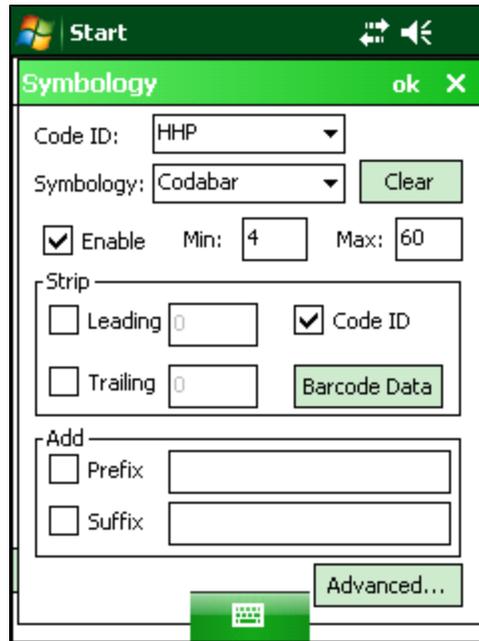
Not all HHP symbologies have Advanced options. Click the symbology link in the table below for the symbology Advanced options.

Symbology	
All	PDF417
Aztec	Plessey
BPO	Posicode
Codabar	Postnet
Codablock	QR
Code 11	RSS
Code32	Strt25
Code 39	Strt32
Code 49	Telepen
Code 93	TLC
Code 128	Trioptic39
Composite	UPCA
Coupon	UPCE0
DataMatrix	UPCE1
EAN8	CANPOST
EAN13	AUSPOST
EAN128	JapanPost
GenCode128	Planet
IATA25	DutchPost
IDTag	ChinaPost
Interleaved 2 of 5	Code16K
ISBT-1	Usps4cb
Matrix 2 of 5	Maxicode
Mesa	MicroPDF
MSI	OCR
Other	

The Data Collection Wedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

Advanced (Hand Held Products Only)

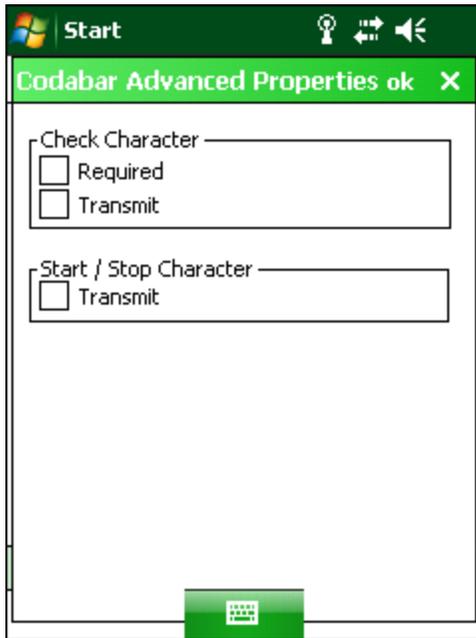
The Advanced button is only available if a Hand Held Products Imager is enabled. Because the Hand Held Products imager does not support configuration bar codes, the Advanced function allows configuration parameters to be set for many of the supported bar codes.



If there are advanced configuration options for the selected symbology, an Advanced button is displayed in the lower right corner of the panel. Not all bar code symbologies have configuration parameters so the Advanced button is not present for all symbologies.

The chart below lists the symbologies and advanced configuration parameters available for that symbology. If a symbology is not listed, it does not have any advanced configuration parameters.

Codabar



Check Character

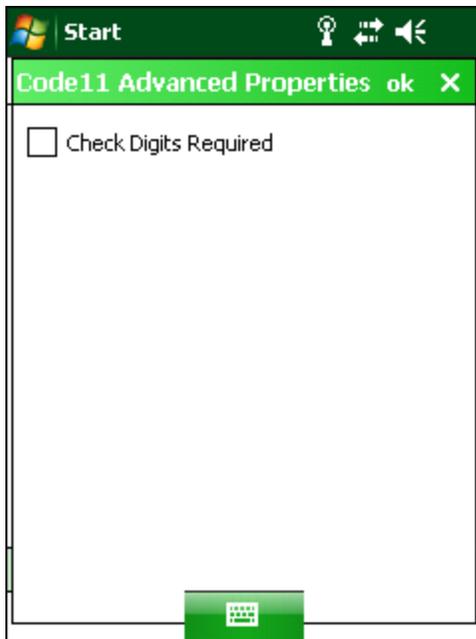
Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Start / Stop Character

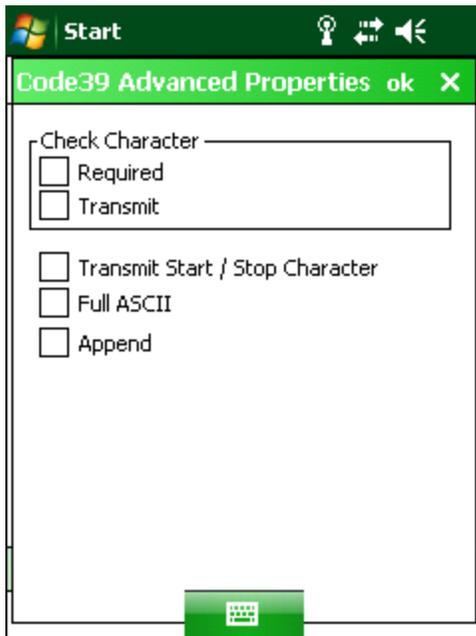
Transmit – When enabled, the start / stop characters are transmitted. Default is disabled.

Code 11



Check Digits Required – When enabled, only bar codes with two check digits are decoded. The default is disabled.

Code 39



Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Transmit Start / Stop Character – When enabled, the start / stop characters are transmitted. Default is disabled.

Full ASCII – When enabled, full ASCII interpretation is used. Default is disabled.

Append – When enabled, append and buffer codes that start with a space. Default is disabled.

EAN 8



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

Addenda

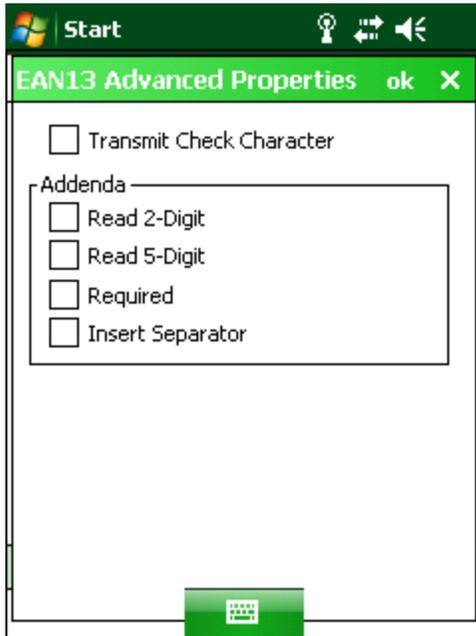
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

EAN 13



Transmit Check Character – When enabled, transmit the check character. Default is disabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

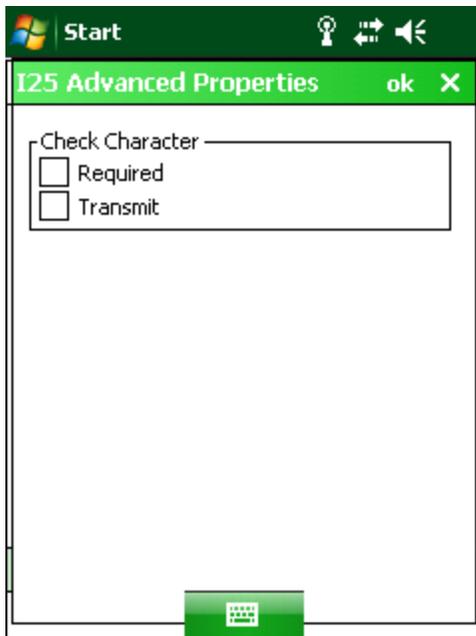
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

Note: A UPCA decoding algorithm will also decode EAN 13 labels. For correct operation, either disable the UPCA symbology when using EAN 13 labels or configure the UPCA settings to match the EAN 13 settings.

Interleaved 2 of 5

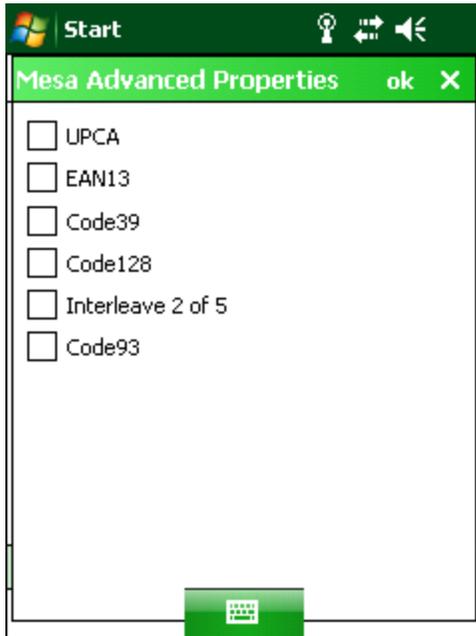


Check Character

Required – When enabled, the check character is required. Default is disabled.

Transmit – When enabled, the check character is transmitted. Default is disabled.

Mesa



UPCA – When enabled, decode UPCA Mesa. Default is disabled.

EAN13 – When enabled, decode EAN 13 Mesa. Default is disabled.

Code39 – When enabled, decode Code 39 Mesa. Default is disabled.

Code128 – When enabled, decode Code 128 Mesa. Default is disabled.

Interleaved 2 of 5 – When enabled, decode Interleaved 2 of 5 Mesa. Default is disabled.

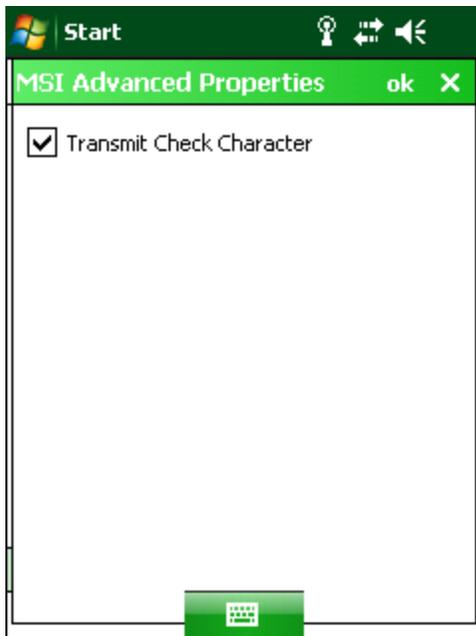
Code93 – When enabled, decode Code 93 Mesa. Default is disabled.

When the Mesa symbology is chosen on the [Symbology panel](#) (the Enable checkbox is checked) the Advanced button must be clicked and the desired Mesa Advanced Properties sub-symbology selected.

When Mesa is disabled on the Symbology panel (the Enable checkbox is cleared), click the Advanced button and uncheck all parameters or sub-symbologies, on the Mesa Advanced Properties panel.

Note: The root symbology (UPCA, EAN13, Code39, Code128, Interleaved 2 of 5 and/or Code 93) must be enabled before the matching enabled Mesa sub-symbology will decode.

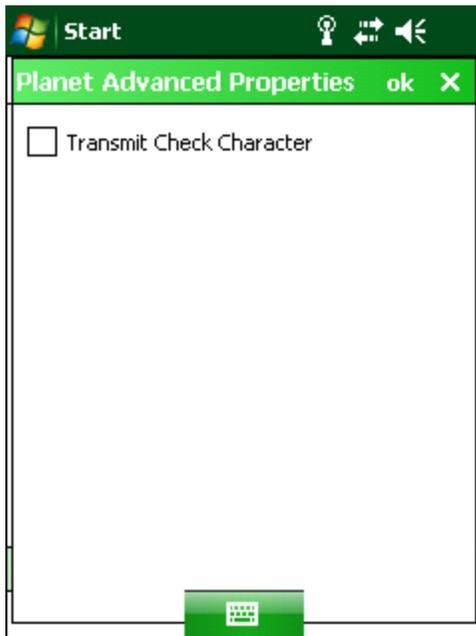
MSI Plessey



Transmit Check Character – When enabled, transmit the check character. Default is enabled.

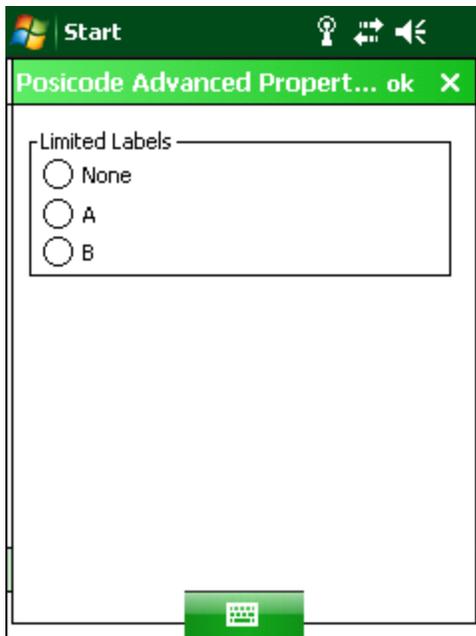
OCR [See Also: "OCR Symbology"](#)

Planet (Postal AlphaNumeric Encoding Technique)



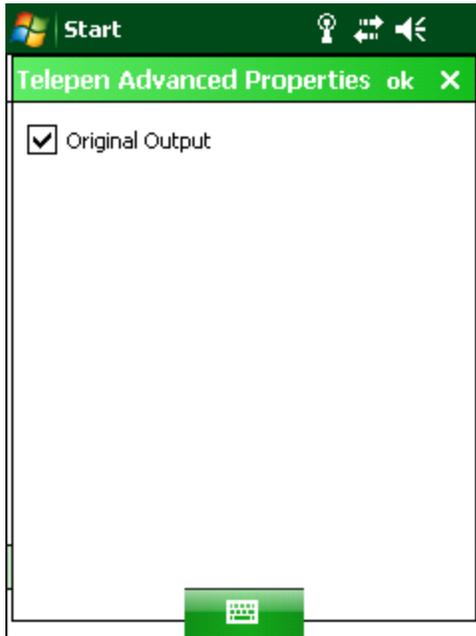
Transmit Check Character – When enabled, transmit the check character. Default is disabled.

Posicode



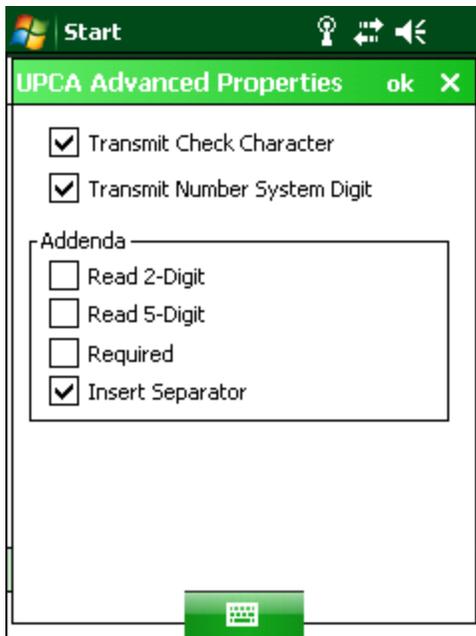
Limited Labels – Select the type of Posicode Limited labels:
None
A – Posicode Limited A
B – Posicode Limited B

Telepen



Original Output – When enabled, output is Original Telepen. When disabled, output is AIM. Default is enabled.

UPCA



Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit Number System Digit – When enabled, transmit the number system digit. Default is enabled.

Addenda

Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

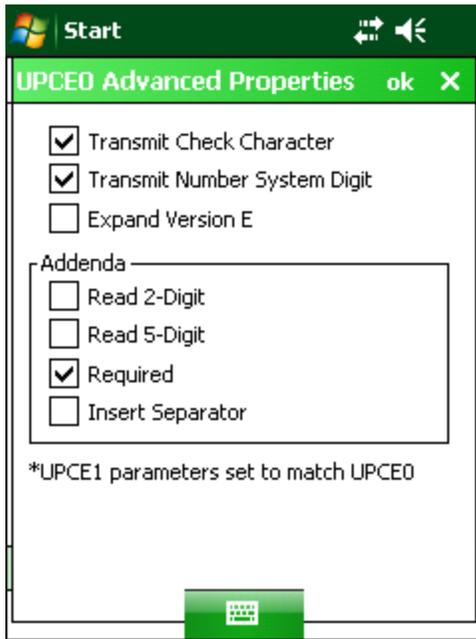
Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is disabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is enabled.

Note: An EAN 13 decoding algorithm will also decode UPCA labels. For correct operation, either disable the EAN 13 symbology when using UPCA labels or configure the EAN 13 settings to match the UPCA settings.

UPCE0



Note: The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Note: UPCE0 and UPCE1 are enabled as the same symbology at the scanner. Therefore, the only way for UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it is scanned by the imager but rejected by Data Collection Wedge.

Transmit Check Character – When enabled, transmit the check character. Default is enabled

Transmit number System Digit – When enabled, transmit the number system digit. Default is enabled.

Expand Version E – When enabled, expand version E to 12-digit UPCA format. Default is disabled.

Addenda

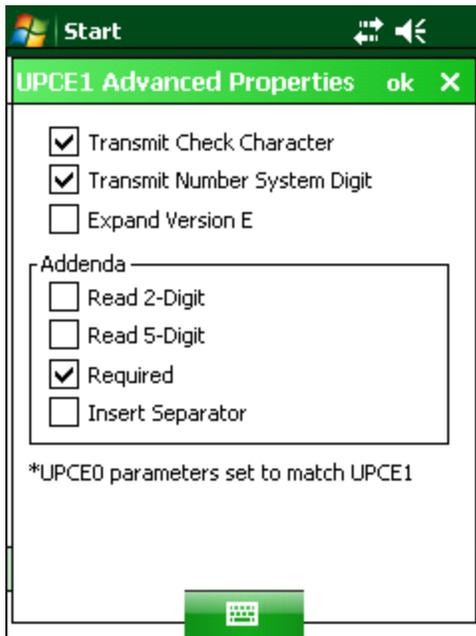
Read 2-Digit – When enabled, transmit the 2 digit addenda. Default is disabled.

Read 5-Digit – When enable, transmit the 5 digit addenda. Default is disabled.

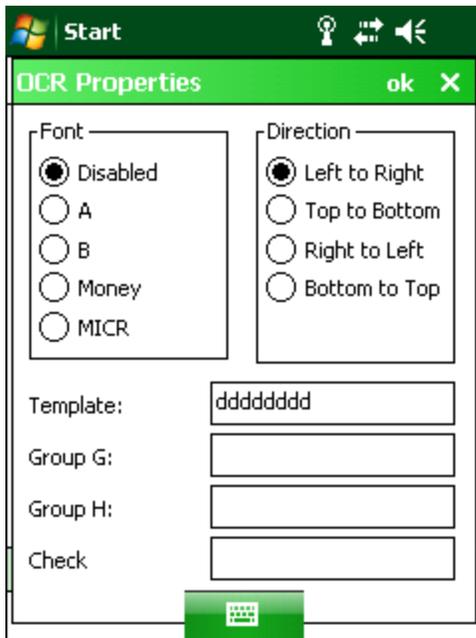
Required – When enabled, only transmit bar codes with a 2 or 5 digit addenda. Default is enabled.

Insert Separator – When enabled, insert a space between the code and addenda. Default is disabled.

UPCE1



OCR Symbology



Font – Font selection:

Disabled

A = OCR A

B = OCR B

Money = OCR Money

MICR = Magnetic Ink Character Recognition

Default is disabled.

Direction – Decoder reads OCR fonts in any direction, but setting direction parameter correctly can increase decoding speed:

Left to Right

Top to Bottom

Right to Left

Bottom to Top

Default is Left to Right.

Template – Template length must match the length of OCR string to be read.

Valid template selections are:

a - alphanumeric character (digit or letter)

c - check character

d - digits from 0 to 9

e - any character

g - any character specified in group G

h - any character specified in group H

l - alphabetic letter

r - delimits a row

t - delimits multiple templates

All characters are transmitted as is except for the selected template. Default is ddddddd.

Group G – Null terminated string defines the set of characters in group G. The default is null.

Group H – Null terminated string defines the set of characters in group H. The default is null.

Check – Enter the string constant 0123456789 for modulo10 checksums and the string constant 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ for modulo36 checksums.

The default is null.

OCR Template Examples

1. To read a combination of 6 alpha and numeric characters use the following template:
aaaaaa
2. To read the same string with a modulo 10 check digit in the 7th character position, use the following template:
aaaaaac
Then enter 0123456789 for the Check parameter.
3. To read either a string of 6 alphabetic letters OR a string of 8 numeric digits, use this template:
llllltddddddd
Note the use of the “t” to separate the first template from the second.
4. To read multiple rows of OCR data as shown below:
123450
ABCDEF
Either of the following templates could be used:
dddddrllllll or aaaaaaraaaaaa
Note the use of the “r” to define the position of the second row.

OCR Checksum Calculation

The following explains how the checksum is generated for the OCR bar code:

Modulo 10:

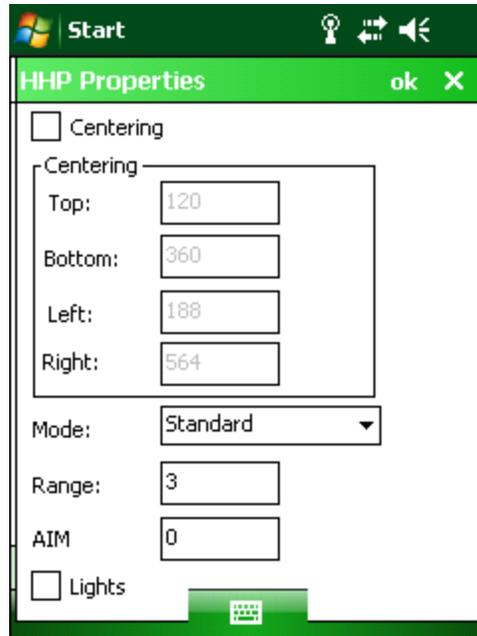
1. Add the characters in the string (not including the checksum character). Valid values are 0 – 9 for modulo 10.
2. Subtract 10 from the sum obtained above. Continue subtracting 10 until the remainder is less than 10.
3. The remainder obtained above is the checksum. Enter this digit in the checksum position.

Modulo 36

1. Add the characters in the string (not including the checksum character). Digit / Alpha values are defined as follows for modulo 36: 0 – 9 = 0 – 9; A = 10, B = 11, ... Z = 25
2. Subtract 36 from the sum obtained above. Continue subtracting 36 until the remainder is less than 36.
3. Subtract the remainder obtained above from 36. The value obtained is the checksum. Enter this character in the checksum position.

HHP Properties

When the MX8 is equipped with a Hand Held Products imager, this option is used to configure imager parameters.

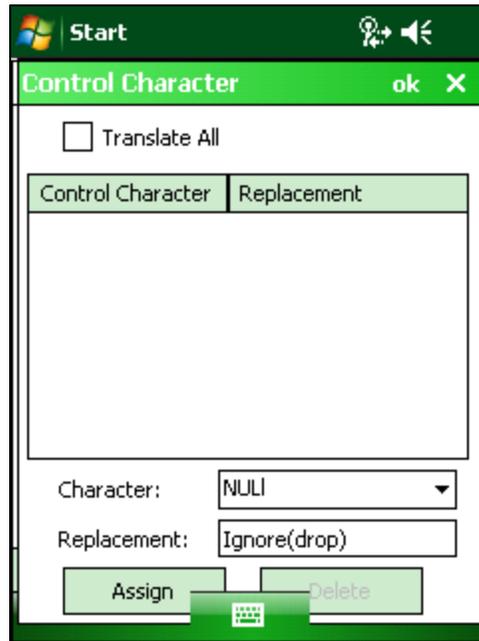


Option	Action
Centering	<p>The centering feature is used to allow the user to accurately scan a selected bar code among a group of bar codes that are located closely together. When centering is turned on, the imager will only decode bar codes that intersect the centering window defined by the user. The centering window must intersect the center of the bar code. The default centering settings define a 60 pixel square area in the center of the imager's field of view. The default is disabled. When enabled, the following parameters may be entered.</p> <p>Top Valid:0 – 239 Default: 120</p> <p>Bottom Valid:240 – 479 Default:360</p> <p>Left Valid:0 – 319 Default:188</p> <p>Right Valid:320 – 639 Default:564</p>
Mode	<p>In <i>Standard mode</i> the imager will decode both linear and 2-D symbologies.</p> <p>In <i>Aggressive Linear Decode mode</i> the imager will only read linear symbologies in this mode, but decoding these is faster and more accurate than Standard Mode.</p> <p>In <i>Quick Omni mode</i> the imager searches for a bar code in a reduced field located around the center of the image. Decoding is faster in this mode, but the user must center the aiming line over the bar code to be read. Both linear and 2-D symbologies can be read in this mode.</p> <p>The default is Standard.</p>

Option	Action
Range	<p>Set the linear range. Valid: 1 – 6 Default: 3 A value of 1 specifies that the linear range that is searched for a readable label is a tight vertical range near the aimer. A value of 6 specifies that the entire height of the image is to be searched.</p>
AIM	<p>Duration of the imager aim beam in 0.1 second increments. Valid: 0 – 50 (0 to 5 seconds) Default: 0</p>
Lights	<p>Specifies if the imager's lights and aimer should be left on during the entire decode process. The default is disabled. If disabled, the lights are turned on only during image capture, then turned off while the imager attempts to process and decode the bar code. If enabled, the aimer and lights remain turned on during the entire process. In Aggressive Linear Decode mode, set this parameter to enabled to improve the aimer visibility. See "Mode" above.</p>

Ctrl Char Mapping

The Ctrl Char Mapping button activates a dialog to define the operations the Data Collection Wedge performs on control characters (values less than 0x20) embedded in bar codes. 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.



Translate All

When Translate All is checked, unprintable ASCII characters (characters below 20H) in scanned bar codes are assigned to their appropriate CTRL code sequence when the bar codes 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 bar code 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 bar code are translated to their equivalent 'control' key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke. Any control code without a keystroke equivalent is dropped.
Character	This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names. When a character name is selected from the drop down box, the default text Ignore (drop) is shown and highlighted in the Replacement edit control. Ignore (drop) is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplay the default Ignore (drop) in the Replacement edit control.

Replacement	<p>The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.</p> <p>For example, if 'Carriage Return' is replaced by Line Feed (by specifying '^J' or '0x0A') in the configuration, the value 0x0d received in any scanned bar code (or defined in the prefix or suffix) will be replaced with the value 0x0a.</p> <p>The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.</p>
List Box	<p>The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.</p>
Delete	<p>This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.</p>

Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for bar codes that do not use the standard AIM or Symbol IDs or for bar codes that have data embedded at the beginning of the data that acts like a Code ID.

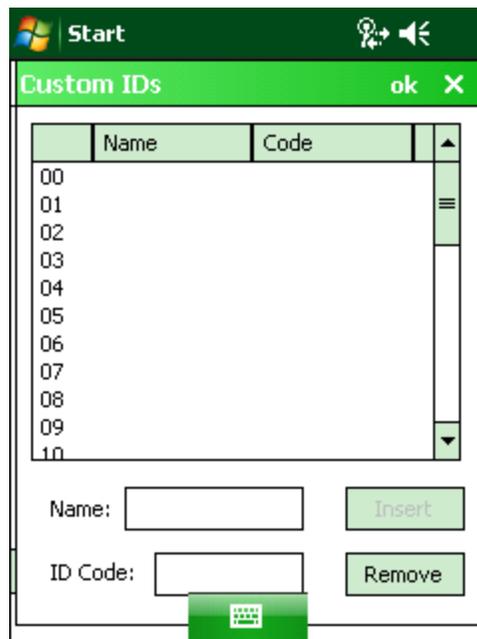
These are called “custom” Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless Enable Code ID is set to None. When the custom Code ID is found in a bar code, the configuration specified for the custom Code ID is applied to the bar code data. The dialog below allows 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).



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 bar code that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

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

Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the bar code data, prefix and suffix	ESCape	'Ignore (drop)'	0x1B in the bar code is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	'STX'	0x02 in a bar code 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 bar code 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 bar code 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 bar code is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	'\0x0A' or '\x0A'	Value 0x0C in a bar code is converted to text '\0x0A'

Bar Code Processing Examples

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

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

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

Bar Code 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]I044444567890987654321	< rejected > (too long)
I2/5]I044444567890123	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 bar codes 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 bar code data by the processing causes a bad scan beep on the same data.

Length Based Bar Code Stripping

Use this procedure to create symbology rules for two bar codes with the same symbology but with different discrete lengths. This procedure is not applicable for bar codes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired bar code ID.
- Next, a custom bar code symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

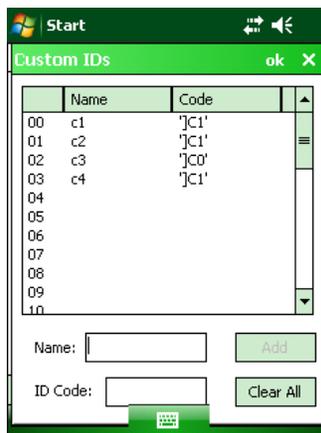
For the purposes of this example, the following sample bar code parameters will be used – EAN 128 and Code 128 bar codes. Some of the bar codes start with '00' and some start with '01'. The bar codes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character bar code is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

On the Data Options tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN 128 bar code and 0 for Code 128 bar code.

- c1 = Code = 'JC1'
- c2 = Code = 'JC1'
- c3 = Code = 'JC0' (24 character bar code is Code 128)
- c4 = Code = 'JC1'



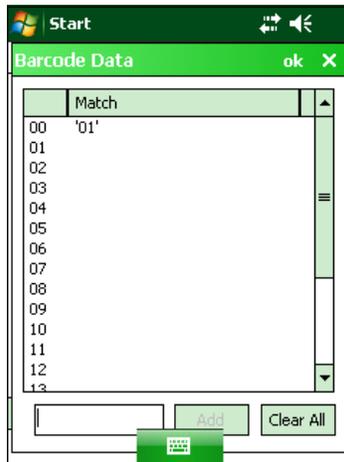
AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

Add the AIM custom symbologies. Refer to [Symbology Settings](#) for instruction.



Click the Barcode Data button. Click the Add button. Add the data for the match codes.



Refer to the previous section [Barcode Data Match List](#) for instruction. Scan a bar code and examine the result.

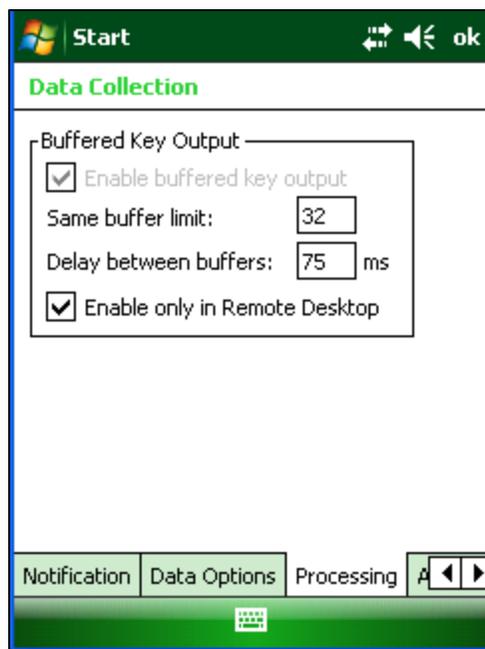
Processing Tab

The Processing tab contains a user configurable key delay that applies to scanned bar codes as they are input when Remote Desktop is the application with the input focus.

Factory Default Settings

Same buffer limit	32
Delay between buffers	75 ms
Only in Remote Desktop	Enabled

Note: Settings on this panel have no effect when RFTerm is the application with the input focus.



Same buffer limit

Specifies the maximum number of characters that the platform and network environment can process correctly without losing data. The default is 32.

Delay between buffers

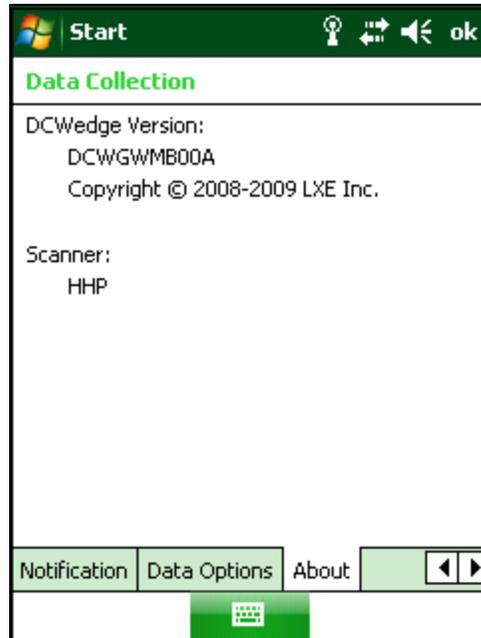
Specifies the number of milliseconds to delay after each character in the scanned bar code is processed as a keystroke. This value may need to be adjusted depending on the network traffic in the environment. The default value is 75 ms. Valid value is from 0 to 9999. A zero value is No Delay between characters.

Only in Remote Desktop

The delay specified in *Delay between buffers* is only applied when Remote Desktop is enabled and is the application with the input focus. When disabled, all keystrokes are delayed by the number of milliseconds specified in *Delay between buffers*.

About Tab

The About tab lists the version of the Data Collection Wedge (DCWedge) software and the type of scanner/imager installed in the MX8.



Valid scanner / imager types:

- HHP – Hand Held Products 5300 2D Imager
- Intermec – Intermec EV-15 Imager
- Symbol – Symbol SE955-I000WR
- N43XX Laser Scanner
- Blank – No scanner installed

Hat Encoding

Hat Encoded Characters Hex 00 through AD

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

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	~)
*	AA	~*
«	AB	~+
-	AC	~,
(soft hyphen)	AD	~ (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Hat Encoded Characters Hex AE through FF

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

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

Chapter 6: Launch Utility

Introduction

The launch utility on the MX8 has two functions:

- Process registry based Launch items
- Process [script based Launch items](#).

Registry Based Launch Items

Note: The Registry based Launch items (documented here) are processed before the Script Based Launch items.

The Launch utility can use registry entries to auto-launch Windows CAB files. These CAB files exist as separate files from the main installation image, and are copied to the terminal using ActiveSync, or using the optional SD card. The CAB files are copied into the folder System, which is the internal Flash drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key

HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist

The main subkey is any text, and is a description of the file. Then the values are added:

Value	Need	Data Type	Description
FileName	Required	String	Name of the CAB file, with full path (usually \System)
Installed	Required	DWORD	Starts as 0, changed to 1 when the CAB file is installed
FileCheck	Required	String	File name, with full path, of a file installed by the CAB file. If this file is not found, Launch assumes the CAB file is not installed or memory was lost.
Order	Optional	DWORD	Determines sequence of installation. Order=0 is installed first, order=99 is installed last.
Delay	Optional	DWORD	Delay, in seconds, after this item is installed and before the next one is installed. If the install fails (or is not found) the delay does not occur.
PCMCIA	Optional	DWORD	1=power up PCMCIA/CF slot after installation

The auto-launch process is as follows.

1. The launch utility opens the registry database and reads the list of CAB files to auto-launch.
2. 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.
3. 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.
4. This process repeats for the next entry in the registry, until all registry entries are analyzed.

Notes:

- To force execution every time, use a **FileCheck** of “**dummy**”, which is never found, forcing the item to execute. If an **AUTOEXEC.BAT** file is found, the terminal runs it by default.
- For persist keys specifying **.EXE** or **.BAT** files, the executing process is started, and then **Launch** continues, leaving the loading process to run independently.
- For other persist keys (including **.CAB** files), **Launch** waits 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 are installed in the same pass, but not in a predictable sequence.
- The **Delay** field is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to **0** if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.
- The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots must be started after this file is loaded. By default, the PCMCIA slots are off on power up, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default radio drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.
- Note that the auto-launch process can also launch batch files (***.BAT**), executable files (***.EXE**), registry setting files (***.REG**), or sound files (***.WAV**). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Launch Startup options

The Launch utility uses registry entries to enable or disable startup options. These flags are located in the registry key:

HKEY_LOCAL_MACHINE\Software\LXE\Launch

These can be configured using RegEdit. The options are as follows:

Value	Ship Default	LTK Default	Description
LaunchPSM	1	0	Execute the Persist keys
JumpStart	1	0	Look for and execute JumpStart scripts
LaunchStart	1	0	Execute any auto-install files in \System\Startup
TimeService	0	0	Launches the GrabTime utility as a service, so that the time and date are periodically automatically updated.

It can often be useful to disable these as necessary, to troubleshoot system startup.

Example

The following example loads and launches RFTerm.

```
;; ----- RFTerm support
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
"FileName"="\System\RFTERM.CAB"
"Installed"=dword:0
"FileCheck"="\WINDOWS\LXE\RFTERM.EXE"
"Order"=dword:11
;; run the app after it has loaded and client device is ready
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
"FileName"="\WINDOWS\LXE\RFTERM.EXE"
"Installed"=dword:0
"FileCheck"="ALWAYSEXEC"
"Order"=dword:40
"Delay"=dword:1
```

Script Based Launch Items

Note: The Script Based Launch items (documented here) are processed after the [Registry Based Launch items](#) (documented earlier).

The Enhanced (script based) portion of the Launch utility provides several features:

- Launch .CAB file
- Run .EXE file
- Run .EXE file using specified parameters
- Run .BAT file
- Process .REG file
- Copy file, with or without overwriting of existing file
- Delete file
- Create directory
- Remove directory
- Add / Update a registry field
- Delete a registry field
- Add a registry subkey
- Delete a registry key
- Display an on-screen message; message requires OK to continue
- Conditional commands, based on existence of file or folder
- Conditional commands, based on terminal type
- End block of conditional commands
- Create a shortcut
- Perform a cold boot (Restart is not useful in this context)

The script developer has the option of pausing script file execution until the current action completes, or continuing script file processing. The script developer is also able to pause for a specified number of milliseconds between commands.

The utility also processes .REG files, using the same format as the legacy Launch Utility. It does this by calling the RegLoad utility. It can also process .BAT files, by calling the Command Prompt utility.

This utility allows the user to configure separate processing for Restart and Cold Boot.

- By default, Enhanced Launch processes both registry entries and scripts, if present. There are registry settings to enable/disable processing of both types of files.
- Script files may have the extension .CLD (for cold boot). With this extension, they may be clicked to execute from the File Explorer. When clicked directly, the extensions do not matter (a script ending in .CLD does not have to be preceded by a cold boot).

Enhanced Launch Utility Use

The Enhanced Launch Utility can be used at OS startup to execute commands from a script file or to launch programs. The user can configure scripts or registry entries for different operation after Cold Boot and Restart. Use of scripts and registry entries is documented in the following sections.

File Names

From a Cold Boot it looks for **JmpStart.cld**. The Launch program can also be run manually. Unless it is given a file as part of the command line it tries to run Launch.txt. The script file may be in ASCII or Unicode.

When trying to find a script file, Launch looks in the following locations (in sequence):

- root directory of the Flash (\System\Launch.xxx)
- root directory of the SD card (\SD Card\Launch.xxx).

In addition, a script file can be written (with a .cld extension), and can be double-clicked to run from the File Explorer.

Command line structure

Each command takes up one line. Every command uses the format:

```
COMMAND, PARAMETER1, PARAMETER2, ...etc.
```

Parameters are separated by a single comma. If a parameter requires a comma within it, the whole parameter must be enclosed in quote marks (""). Extra spaces are ignored between the comma and the next parameter.

For Example

To delete a file called Ive, got, commas, in, my, name.txt, use the command

```
delete,"Ive, got, commas, in, my, name.txt".
```

Enclosing quotes are used to allow commas inside a parameter, but are removed prior to executing the command. Thus, delete,deleteme.txt is the same as delete,"deleteme.txt". If a parameter requires a quote mark within it, the whole parameter must first be enclosed within quote marks, and the required quote mark is represented by two quote marks (""). For example, to place the message This is how you display "quote marks" on the screen, use the command

```
message,This is a heading,"This is how you display ""quote marks""".
```

The case of a command is ignored, so delete is the same as DELETE and DeLeTe.

Comments

Any line that starts with a semicolon (;), a slash (/) or an asterisk (*) is treated as a comment, and ignored by Launch.

Launch also ignores any extra parameters (more than the required number) in a command. It is not recommended that comments be placed at the end of lines as any future changes could render your script files incompatible.

Blank lines are also ignored.

Commands Supported by Launch

Copy	ElselFfile	IfFile	Mkdir
Delete	Endf	IfTerm	Rmdir
DelRegData	EndIfFile	Launch	SetRegData
DelRegKey	EndIfTerm	LaunchCmd	SetRegKey
ElselF	FCopy	Message	Shortcut

The commands supported by Launch are detailed below. Square brackets indicate that a parameter is optional. Characters in italics represent a variable, and not a literal.

Copy

Description

Copies a file but does not overwrite an existing file.

Syntax

Copy, *source-file*, *destination-file*

Parameters

source-file: The file to be copied, including its path

destination-file: The destination path and filename

Example

```
copy, \Storage Card\MyData.dat, \Temp\MyData.dat
```

Notes

If the destination file already exists, it is not overwritten, and no error is given.

If the source file is blank, a zero-byte file is created.

Delete

Description

Deletes the specified file.

Syntax

Delete, *source-file*

Parameters

source-file: The file to be deleted, including its path

Example

```
delete, \Temp\MyData.dat
```

DelRegData

Description

Deletes a specified registry data field.

Syntax

```
Delregdata, key, subkey, field
```

Parameters

key: The abbreviated major registry key where you want to delete a field. Can be one of:

- **cr** or **hkcr** (HKEY_CLASSES_ROOT)
- **cu** or **hkcu** (HKEY_CURRENT_USER)
- **lm** or **hklm** (HKEY_LOCAL_MACHINE).

The case of *key* doesn't matter

subkey: The subkey that holds the field you want to delete.

field: The field that you want to delete.

Example

```
delregdata, LM, Software\WidgetsPlc\OurApp, AppName
```

Notes

An error isn't displayed if you specify a non-existent field, but is displayed if you specify a non-existent key or subkey.

DelRegKey

Description

Deletes a specified registry subkey.

Syntax

```
DelRegKey, key, subkey
```

Parameters

key: The abbreviated major registry key where you want to delete the subkey. Can be one of:

- **cr** or **hkcr** (HKEY_CLASSES_ROOT)
- **cu** or **hkcu** (HKEY_CURRENT_USER)
- **lm** or **hklm** (HKEY_LOCAL_MACHINE).

The case of *key* doesn't matter

subkey: The subkey you want to delete.

Example

```
delregkey, LM, Software\WidgetsPlc\OurApp
```

Notes

Deletes the specified subkey and all of its contents (if any).

ElseIf

Description

Begins conditional command block, executed only if the previous IF command was FALSE.

Syntax

```
ElseIf
```

Parameters

None

Example

See [IfFile](#) , below

Notes

Results are unpredictable if not paired properly with **If...** command.

ElseIfFile

Description

Begins conditional command block executed only if the file specified in the previous IfFile does not exist.

Syntax

```
ElseIfFile
```

Parameters

None

Example

See [IfFile](#) , below

Notes

Results are unpredictable if not paired properly with **IfFile** command.

EndIf

Description

Ends conditional command block begun with the previous IF command.

Syntax

```
EndIf
```

Parameters

None

Example

See [IfFile](#), below

Notes

Results are unpredictable if not paired properly with **If...** command.

EndIfFile

Description

Ends conditional command block begun with the previous IF command.

Syntax

```
EndIfFile
```

Parameters

None

Example

See [IfFile](#) , below

Notes

Results are unpredictable if not paired properly with **IfFile** command.

EndIfTerm

Description

Ends conditional command block executed only if the terminal type specified in **IfTerm** matches.

Syntax

```
EndIfTerm
```

Parameters

None

Example

See [IfTerm](#) , below

Notes

Results are unpredictable if not paired properly with **IfTerm** command.

FCopy

Description

Copies a file, overwriting any existing file.

Syntax

fcopy, *source-file*, *destination-file*

Parameters

source-file: The file to be copied, including its path

destination-file: The destination path and filename

Example

```
fcopy, \Storage Card\MyData.dat, \Temp\MyData.dat
```

Notes

If the destination file already exists it is overwritten.

If the source file is blank, a zero-byte file is created.

IfFile

Description

Begins the conditional execution of a block of commands only if the specified file exists.

Syntax

```
IfFile, file
```

Parameters

file: The path and filename to determine if the commands should be executed

Example

```
IfFile, \System\MyData.dat  
    any number of commands, executed if file exists  
ElseIfFile  
    any number of commands, executed if file does not exist  
EndIfFile
```

Notes

If the file already exists the commands are executed.

This test does not care if file is a file or directory.

Nesting is supported.

IfTerm

Description

Begins the conditional execution of a block of commands only if the terminal matches the specified terminal type.

Syntax

```
IfTerm, terminal
```

Parameters

terminal: The terminal type to determine if the commands should be executed

Example

```
IfTerm, MX3X  
    any number of commands  
EndIfTerm
```

Notes

If the terminal type is identical (not case-dependent) the commands are executed.

Nesting with **IfFile** is supported. Nesting with **IfTerm** is meaningless.

Launch

Description

Runs a program.

Syntax

```
Launch, program, wait-code
```

Parameters

program: The full path and filename of the program to be run.

wait-code Tells Launch how to behave when the program is running.

w(ait) causes Launch to stop processing the script until the program has finished executing.

c(ontinue) makes Launch continue processing the script while the program is executing.

Example

```
launch, \Windows\Calc.exe, w
```

Notes

This differs from **LaunchCmd** in that **Launch** has no parameters.

LaunchCmd

Description

Runs a program with arguments.

Syntax

Launchcmd, *program*, *arguments*, *wait-code*

Parameters

program: The full path and filename of the program to be run.
wait-code Tells Launch how to behave when the program is running.
w(ait) causes Launch to stop processing the script until the program has finished executing.
c(ontinue) makes Launch continue processing the script while the program is executing.
arguments: The command line arguments for program.

Example

```
launchcmd, \Windows\Pword.exe, \My Documents\Doc1.doc, w
```

Notes

This differs from **Launch** in that **LaunchCmd** allows parameters.

Message

Description

Displays a message on the screen.

Syntax

Message, *message-title*, *message-body*

Parameters

message-title: A heading for the message. Can be left empty.
message-body: The main body of the message. To display a message over multiple lines, use the \n character combination at the end of each line. To display a single backslash use two together (\\).

Example

```
message, This is a message, "This is the first line, \nand this is the second"
```

Notes

Displaying a message pauses the execution of the script file until the message is OK'd. This is displayed with a modal dialog.

Mkdir

Description

Creates a directory.

Syntax

Mkdir, *dir*

Parameters

dir: The full path and name of the directory to be created.

Example

```
mkdir, \Program Files\MyApp
```

Notes

A new directory cannot be created if its parent directory doesn't exist.

For example, to create a directory called *MyApp* with a subdirectory called *SubDir1*, use **mkdir, MyApp** followed by **mkdir, MyApp\SubDir1**.

Rmdir

Description

Removes a directory.

Syntax

Rmdir, *dir*

Parameters

dir: The full path and name of the directory to be removed.

Example

```
rmdir, \Program Files\MyApp
```

Notes

A directory cannot be removed if it contains files or subdirectories.

SetRegData

Description

Adds or updates a data field in the registry.

Syntax

```
Setregdata, key, subkey, type, field, data[, data2][, data3]...
```

Parameters

<i>key</i> :	The abbreviated major registry key where you want to create/update the subkey. Can be one of: <ul style="list-style-type: none">• cr or hkcr (HKEY_CLASSES_ROOT)• cu or hkcu (HKEY_CURRENT_USER)• lm or hklm (HKEY_LOCAL_MACHINE).
<i>subkey</i> :	The case of <i>key</i> doesn't matter The subkey you want to create/update a field in.
<i>type</i> :	The data type of the field you wish to create/update. Can be s (for string value), dd (for decimal value), dx (for hexadecimal value) or b (for binary value). The case of <i>type</i> doesn't matter. If you're altering an existing field, <i>type</i> can be different from the current type
<i>field</i> :	The name of the new field to be created/updated.
<i>data</i> :	The value of the field being created. This depends on the <i>type</i> of field. Binary fields can have many values (up to 2000 bytes). In this case the data field holds the number of bytes in the binary field, and each byte is given as a subsequent parameter in hexadecimal (<i>data2</i> , <i>data3</i> etc.).

Example

```
Setregdata, LM, WidgetsPlc\Info, s, AppName, The Widget Program
```

```
Setregdata, LM, WidgetsPlc\Info, dx, HexField, FA5B
```

```
Setregdata, LM, WidgetsPlc\Info, b, 5, d3, 62, 58, f1, 9c
```

SetRegKey

Description

Adds a sub key to the registry.

Syntax

```
Setregkey, key, subkey
```

Parameters

key: The abbreviated major registry key where you want to create the subkey. Can be one of:

- **cr** or **hkcr** (HKEY_CLASSES_ROOT)
- **cu** or **hkcu** (HKEY_CURRENT_USER)
- **lm** or **hklm** (HKEY_LOCAL_MACHINE).

The case of *key* doesn't matter

subkey: The subkey you want to create.

Example

```
Setregkey, LM, Software\MyApp
```

Notes

Attempting to create a key that already exists does not cause an error.

Shortcut

Description

Creates a shortcut.

Syntax

`Shortcut, name, target`

Parameters

name: The path and name of the shortcut file. The file name must end in .lnk for Windows CE to recognize it as a shortcut.

target: The target of the shortcut. If the target has a space in it quote marks must be used (see Command Line Structure section and example below).

Example

```
shortcut, \Program Files\Widget.lnk, """"\My App\Widget.exe""""
```

Notes

No validation is performed on target to be sure it is executable.

Launch Error Messages

Launch displays a message if it encounters an error during the processing of a script. It is possible to get cascading error messages, as Launch does not stop processing the script if it encounters an error. An example of this would be a failure creating a directory causing the failure of all files copied to that directory.

Here is a list of the possible error messages that could be given:

Error Message	Given by	Description
Bad wait code wait-code	Launch LaunchCmd	The wait-code wasn't recognized
Directory Creation Failed error-code	MkDir	There was a problem encountered creating the directory
Directory Removal Failed error-code	Rmdir	There was a problem encountered removing the directory
Error reading script file	-	An error occurred reading the script file.
File Copy Failed error-code	Copy Fcopy	There was a problem encountered copying the file
File Delete Failed error-code	Delete	There was a problem encountered deleting the file
Invalid Command: command	-	The command wasn't recognized
Invalid Data Length data	SetRegData	Tried to set more than 2000 byte values in a binary field
Invalid Data Type type	SetRegData	The value of the type parameter is invalid
Invalid decimal data data	SetRegData	The data field doesn't contain decimal data
Invalid hex data data	SetRegData	The data field doesn't contain hexadecimal data
Invalid Registry Key key	DelRegData DelRegKey SetRegData DelRegKey	The key parameter to the command has not been recognized
Parms: Invalid Create Directory	Mkdir	Not enough parameters were supplied.
Parms: Invalid Create Registry Key	SetRegKey	Not enough parameters were supplied.
Parms: Invalid Create Shortcut	Shortcut	Not enough parameters were supplied.
Parms: Invalid Delete Registry Data	DelRegData	Not enough parameters were supplied.
Parms: Invalid Delete Registry Key	DelRegKey	Not enough parameters were supplied.
Parms: Invalid File Copy	Copy Fcopy	Not enough parameters were supplied.
Parms: Invalid File Delete	Delete	Not enough parameters were supplied.
Parms: Invalid Program Name	Launch LaunchCmd	Not enough parameters were supplied.
Parms: Invalid Remove Directory	Rmdir	Not enough parameters were supplied.

Error Message	Given by	Description
Parms: Invalid Set Registry Data	SetRegData	Not enough parameters were supplied.
Parms: Invalid User Message	Message	Not enough parameters were supplied.
Program Launch couldn't get ExitCode error-code	Launch LaunchCmd	There was a problem getting the exit status of the program.
Program Launch Failed error-code	Launch LaunchCmd	There was a problem executing the program.
Registry Key Create Failed error-code	SetRegKey	There was a problem creating the registry key given.
Registry Key Delete Failed error-code	DelRegKey	There was a problem deleting the registry key given.
Registry Value Delete Failed error-code	DelRegData	There was a problem deleting the registry data. Most likely a bad subkey.
Registry Value Set Failed error-code	SetRegData	There was a problem setting the registry data. Most likely a bad subkey.
Shortcut Creation Failed error-code	Shortcut	There was a problem encountered creating the shortcut.
Unable to open file script-file	-	There was a problem opening the script-file. This message is only displayed when manually running Launch.

Example Script File

```
iffile, \System\applock.cab
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \System\applock.cab", w
launch, \Windows\applockprep.exe, c
endiffile
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \System\wedge.cab", w
iffile, \System\summit.cab
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \System\summit.cab", w
endiffile
iffile, \System\RFTerm.cab
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \System\RFTerm.cab", w
endiffile
iffile, \System\Java.cab
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \System\Java.cab", w
launchcmd, \Windows\wceload.exe, "/noaskdest /noui \Windows\Jeode.cab", w
endiffile
launch, \System\regrest.exe, w
coldboot
```



Chapter 7: Wireless Network Configuration

Introduction

The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates or an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Security Options Supported are

- [None](#)
- [WEP](#)
- [LEAP](#)
- [WPA-PSK](#)
- [WPA/LEAP](#)
- [PEAP-MSCHAP](#)
- [PEAP-GTC](#)
- [EAP-TLS](#)
- [EAP-FAST](#)

Complete configuration options are detailed in the [Summit Client Utility](#).

Important Notes

	It is important that all dates are correct on the MX8 and host 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 software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance for details.
	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, perform a Suspend/Resume on the MX8.

Summit Client Utility

Note: When making changes to profile or global parameters, tap the power key to place the MX8 in Suspend. When the MX8 resumes from suspend the parameters are applied. The MX8 can be resumed by tapping the power key or the touch screen or by pressing any key.

Access:

Start > Settings > System > Wi-Fi or

Summit Tray Icon (if present)

The [Main Tab](#) provides information, admin login and active profile selection.

Profile specific parameters are found on the [Profile Tab](#). The parameters on this tab can be set to unique values for each profile. This tab was labeled Config in early versions of the SCU.

The [Status Tab](#) contains information on the current connection.

The [Diags Tab](#) provides utilities to troubleshoot the radio.

Global parameters are found on the [Global Tab](#). The values for these parameters apply to all profiles. This tab was labeled Global Settings in early versions of the SCU.

Help

Help is available by clicking the ? icon in the title bar on most Summit Client Utility (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 accessed 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 radio 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

Click the icon to launch the SCU.

Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Using Windows Mobile Wireless Manager

Best practice is to use the [Summit Client Utility](#) to manage wireless connectivity.

However, if desired, Windows Mobile includes the Wireless Manager utility to manage wireless network connections in place of the Summit Client Utility.

To use the Windows Mobile Wireless Manager, first open the Summit Client Utility.

1. Select **ThirdPartyConfig** in the Active Profile drop down box on the [Main tab](#).
2. A message appears that means a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Suspend/Resume the MX8.

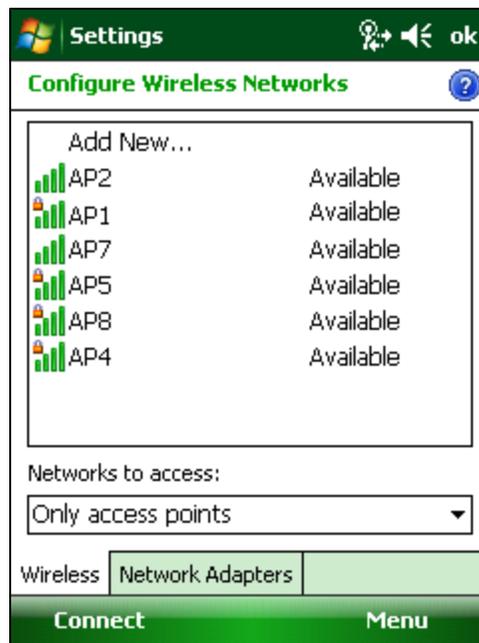
Access the Wireless Manager utility by tapping the radio icon at the top of the screen or tapping:

Start > Settings > Connections > Wi-Fi

If the Wi-Fi icon is not present in the Connections panel, return to the Summit Client Utility and select **ThirdPartyConfig**.

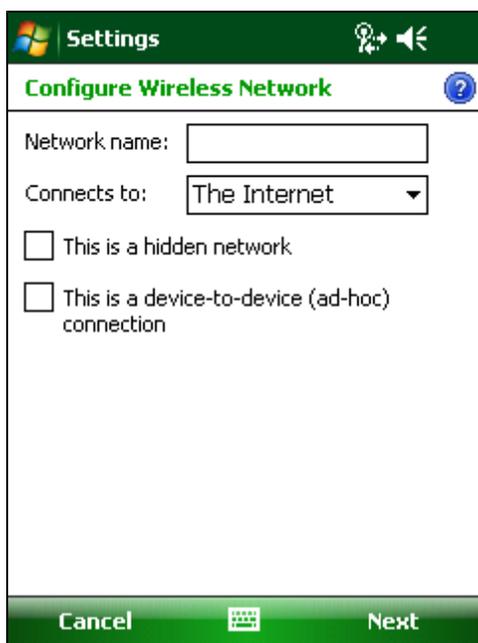
Create a New Network Connection

Click on the Wi-Fi icon. A list of available networks is displayed.



If the desired network is not displayed, tap **Add New**.

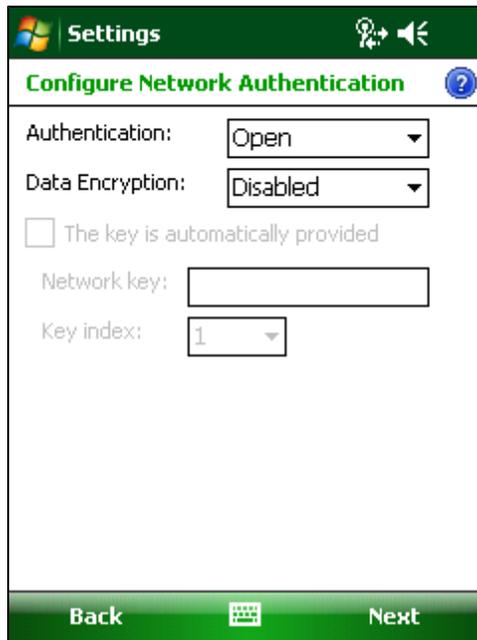
If the desired network is displayed in the list, tap the network name.



Enter the SSID of the desired network in the **Network name** text box. Be sure to check the *This is a hidden network* checkbox for a non-broadcast SSID.

In the **Connects to** box, select **The Internet** if the MX8 connects directly to the Internet, select **Work** if the MX8 connects to a network (even if the network provides an Internet connection).

Tap **Next**.



Please refer to the Windows Mobile help screens or online documentation for configuring wireless security using the Windows Mobile Wireless Manager.

Note: Tap **Start > Help** for context sensitive Windows Help when changing or viewing options. Tap the **X** icon in the top right corner to close Windows Help.

Edit a Network Connection

Double tap the network name to edit the configuration or tap the network name and tap **Connect** to connect to the network. Network configuration screens are the same as displayed in the previous section.

Switch Control to SCU

1. To switch back to SCU control, select any other profile except **ThirdPartyConfig** in the SCU Active Config drop down list on the [Main tab](#).
2. A message appears that means a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Cold boot the MX8.

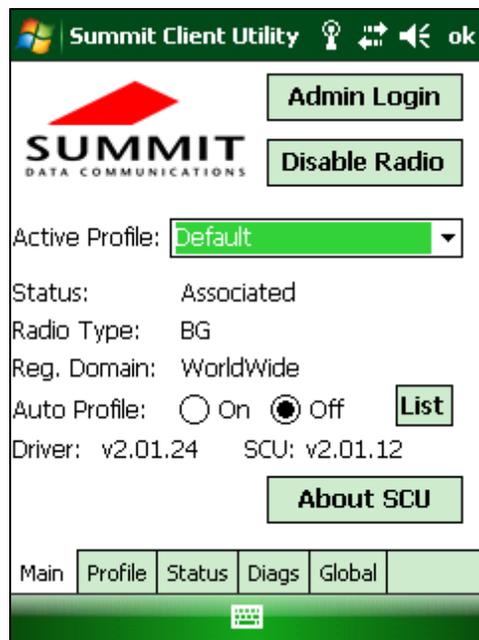
Radio control is passed to the Summit Client Utility.

Main Tab

Start > Settings > System > Wi-Fi > Main tab

Factory Default Settings

Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	Varies by location



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

- SCU (Summit Client Utility) version.
- Driver version.
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11 a/b/g radio).
- Regulatory Domain is preset to either Worldwide or a location specific domain (FCC, ETSI, KCC or TELEC).
- Copyright Information can be accessed by tapping the About SCU button.
- Active Config profile / Active Profile name.
- Status of the client (Down, Associated, Authenticated, etc).

The **Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Always perform a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named "ThirdPartyConfig" is chosen as the active profile, the Summit Client Utility passes radio control to Windows Zero Config for configuration of all client and security settings for the network module.

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

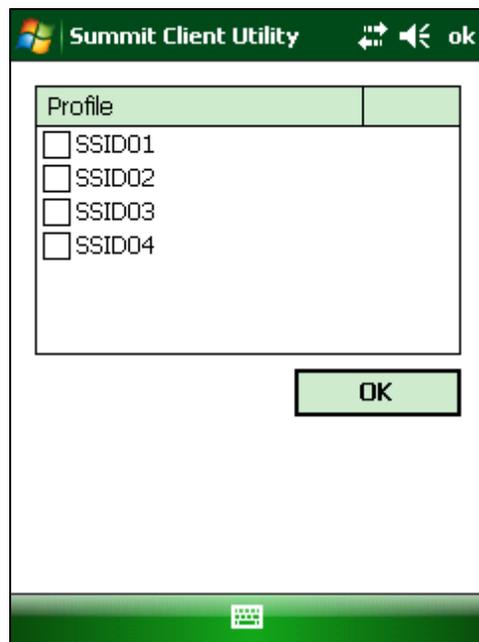
The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the **Admin Logout** button or exit the SCU without tapping the **Admin Logout** button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the **List** button.



The Auto Profile selection screen displays all currently configured profiles. Click on the checkbox for any profiles that are to be included in Auto Profile selection then click ok to save.

To enable Auto Profile, click the **On** button on the **Main** tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

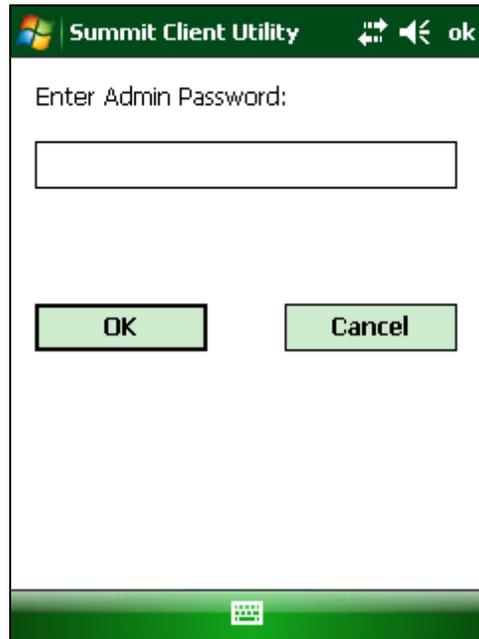
- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is clicked to turn off Auto Profile.

Note: Do not include any profiles with an [Ad Hoc Radio Mode](#) in this listing.

Admin Login

To login to Administrator mode, tap the **Admin Login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the **Admin Logout** button, or the **OK** button to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.



Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the [Global](#) tab.

The end-user can:

- Turn the radio on or off on the [Main](#) tab.
- Select an active Profile on the [Main](#) tab.
- View the current parameter settings for the profiles on the [Profile](#) tab.
- View the global parameter settings on the [Global](#) tab.
- View the current connection details on the [Status](#) tab.
- View radio status, software versions and regulatory domain on the [Main](#) tab.
- Access additional troubleshooting features on the [Diags](#) tab.

After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the [Profile](#) tab.
- Edit global parameters on the [Global](#) tab.
- Enable/disable the Summit tray icon in the taskbar.

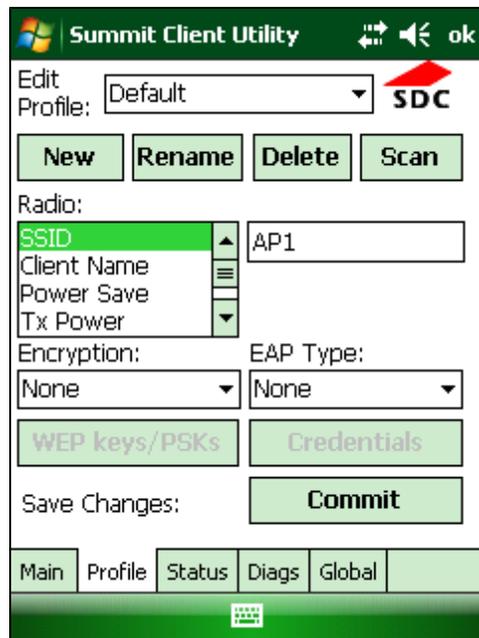
Profile Tab

Start > Settings > System > Wi-Fi > Profile tab

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

Factory Default Settings

Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters for default
Auth Type	Open
EAP Type	None
Encryption	None



When logged in as an Admin (see [Admin Login](#)), use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Buttons

Button	Function															
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.															
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.															
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.															
New	Creates a new profile with the default settings (see Profile 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.															
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.															
Scan	<p>Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers.</p> <p>If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.</p> <div data-bbox="685 932 1065 1440" data-label="Image"> <table border="1"> <thead> <tr> <th>SSID</th> <th>RSSI</th> <th>Secure</th> </tr> </thead> <tbody> <tr> <td>Net4</td> <td>-47</td> <td>true</td> </tr> <tr> <td>Net2</td> <td>-48</td> <td>true</td> </tr> <tr> <td>Net1</td> <td>-51</td> <td>true</td> </tr> <tr> <td>Net3</td> <td>-51</td> <td>false</td> </tr> </tbody> </table> </div> <p>If you are logged in as an Admin, tap an SSID in the list and tap the Configure button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as “_1” if a profile with the SSID as its name exists already).</p>	SSID	RSSI	Secure	Net4	-47	true	Net2	-48	true	Net1	-51	true	Net3	-51	false
SSID	RSSI	Secure														
Net4	-47	true														
Net2	-48	true														
Net1	-51	true														
Net3	-51	false														
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.															

Note: *Unsaved Changes* – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

Important – The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g., Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. <i>Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.</i>
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the MX8. <i>Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.</i>

Parameter	Default	Explanation
Radio Mode	BG radio: BG Rates Full Or A radio: BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) ABG Rates Full (All A rates and all B and G rates with A rates preferred) BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) Ad Hoc (when connecting to another client device instead of an AP) Default: BG Rates Full (for 802.11b/g radios) BGA Rates Full (for 802.11a/b/g radio) Note: <i>BG radio only – Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.</i>

It is important the **Radio Mode** parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the MX8 may only connect to APs set for G rates and not those set for B and G rates.

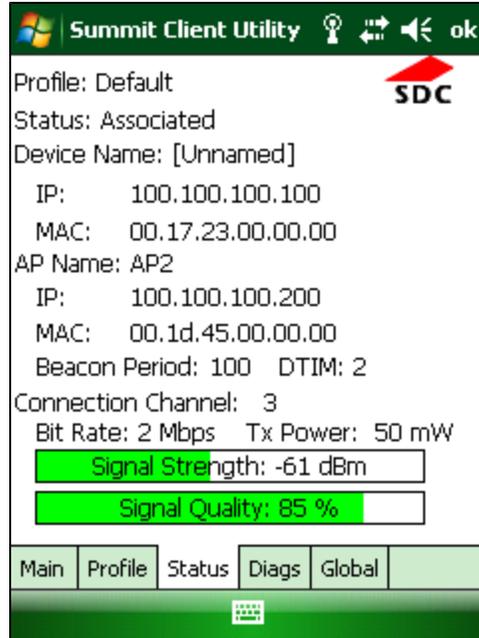
The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	Radio Mode
A Main and BG Main	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Contact [Technical Assistance](#) if you have questions about the antenna(s) installed on your MX8.

Status Tab

Start > Settings > System > Wi-Fi > Status tab



This screen provides information on the radio:

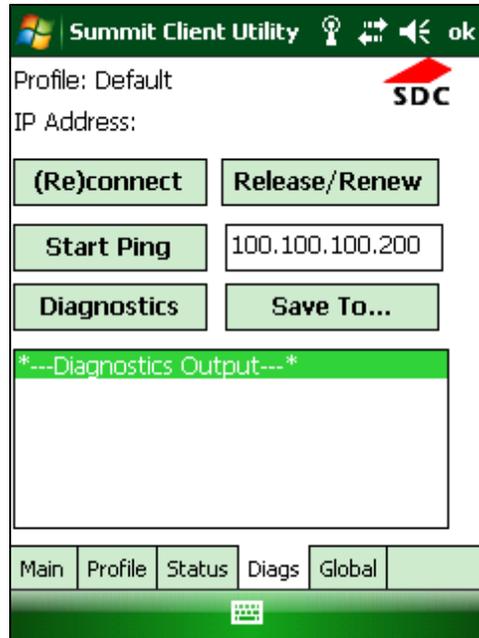
- The profile being used
- The status of the radio card (down, associated, authenticated, etc.)
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic
- Bit rate in Mbit.
- Current transmit power in mW
- Beacon period – the time between AP beacons in kilomicroseconds. (one kilomicrosecond = 1,024 microseconds)
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab

Start > Settings > System > Wi-Fi > Diags tab



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To...** – Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can be viewed using an application such as WordPad.

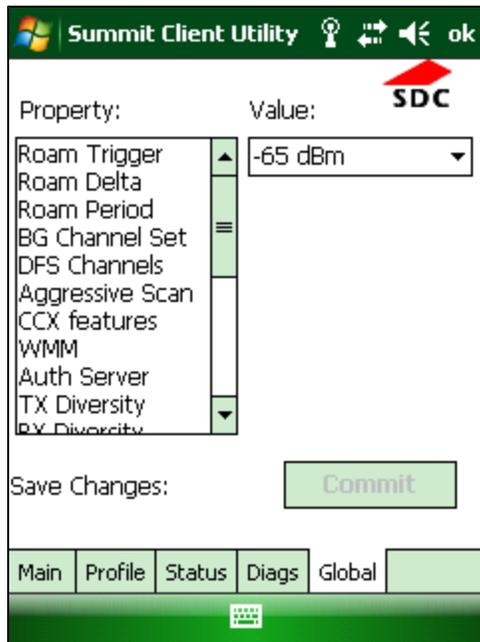
Global Tab

Start > Settings > System > Wi-Fi > Global tab

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

Factory Default Settings

Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full
DFS Channels	Off
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	BG: Off A: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	BG: On A: Main Only
RX Diversity	BG: On-Start on Main A: Main Only
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms



Custom Parameter Option

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

Global Parameters

Parameter	Default	Function
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom .
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom .
Roam Period	BG: 10 sec. A: 5 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom .
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) Custom .
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off. <i>Note: Not supported (always off) in some releases.</i>
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX or CCX Features	BG: Off A: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number.

Parameter	Default	Function
		Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off Default value cannot be changed.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP, CHAP, EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information is cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK <i>Note: This change does not take effect until after a Suspend/Resume cycle.</i>
WAPI	Off	Default is Off and dimmed (cannot be changed).
TX Diversity	BG: On A: Main Only	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).

The options for the TX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	TX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On
BG Main and BG Aux	On

Contact [Technical Assistance](#) if you have questions about the antenna(s) installed on your MX8.

Parameter	Default	Function
RX Diversity	BG: On-Start on Main A: Main Only	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).

The options for the RX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	RX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On-start on Main
BG Main and BG Aux	On-start on Main

Contact [Technical Assistance](#) if you have questions about the antenna(s) installed on your MX8.

Parameter	Default	Function
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.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.

Parameter	Default	Function
Certs Path	System	<p>A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Make sure the Windows folder path exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out.</p> <p>Options are: none.</p> <p>For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.</p>
Ping Payload	32 bytes	<p>Maximum amount of data to be transmitted on a ping.</p> <p>Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.</p>
Ping Timeout ms	5000	<p>The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout.</p> <p>Options are: Any number between 0 and 30000 ms.</p>
Ping Delay ms	1000	<p>The amount of time, in milliseconds, between each ping after a Start Ping button tap.</p> <p>Options are: Any number between 0 and 30000 ms.</p>

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

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers these choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

How to: Use Stored Credentials

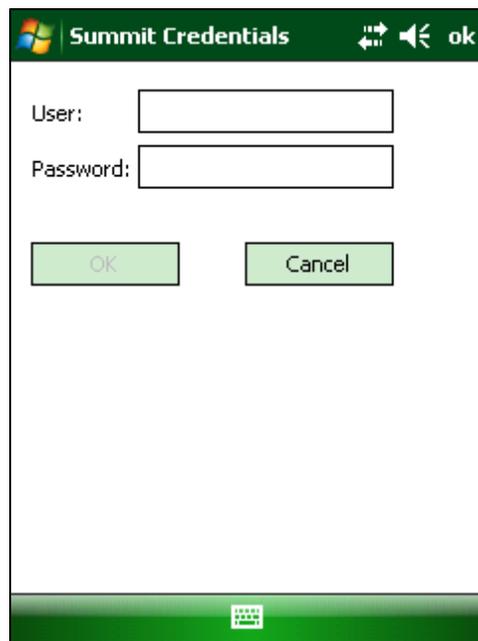
1. After completing the other entries in the profile, click on the **Credentials** button.
2. Enter the Username and Password on the Credentials screen and click **the OK** button.
3. Click the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Click the **OK** button then the **Commit** button.
12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: See [Configuring the Profile](#) for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Click the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Click the **OK** button.



10. 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.
11. The sign-on screen is displayed after a reboot.

Note: See [Configuring the Profile](#) for more details.

If a user enters invalid credentials and clicks **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the **Cancel** button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the **Reconnect** button on the [Diags Tab](#) is clicked or
- the profile is modified and the **Commit** button is clicked.

Windows Certificate Store vs. Certs Path

Note: It is important that all [dates are correct](#) on the MX8 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see [Generating a User Certificate](#).
- To import the user certificate into the Windows certificate store, see [Installing a User Certificate](#).
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

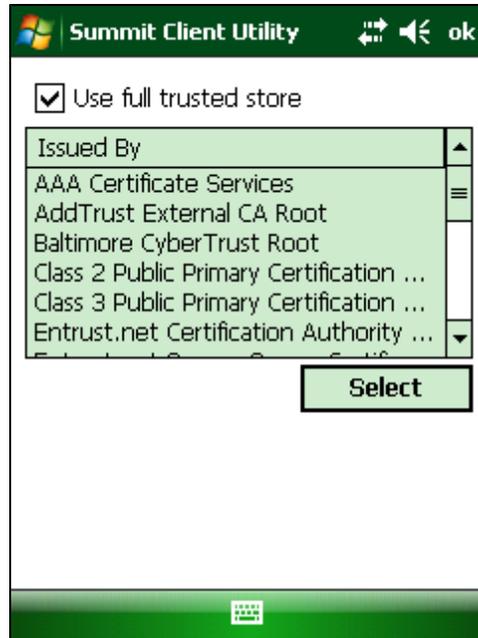
Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. See [Generating a Root CA Certificate](#) and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the CA Cert textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. See [Generating a Root CA Certificate](#) and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See [Installing a Root CA Certificate](#).
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate click on the **Browse (...)** button.



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

Configuring the Profile

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

- On the [Main Tab](#), click the [Admin Login](#) button and enter the password.
- Edit the default profile with the parameters for your network. Select the Default profile from the pull down menu.
- Make any desired parameter changes as described in the applicable following section determined by network security type and click the **Commit** button to save the changes.

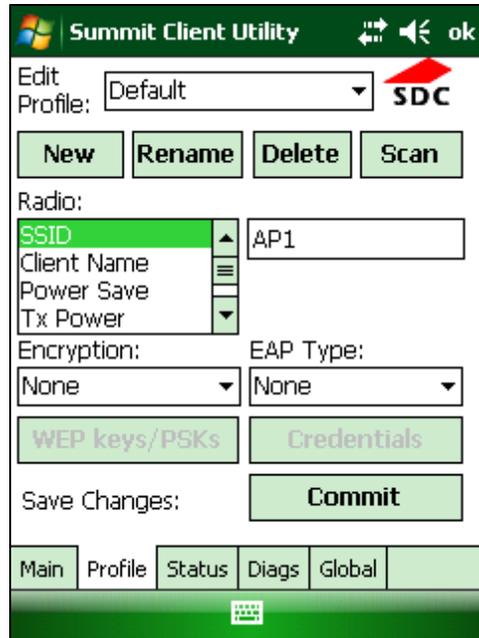
IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **None**
- Set **Auth Type** to **Open**



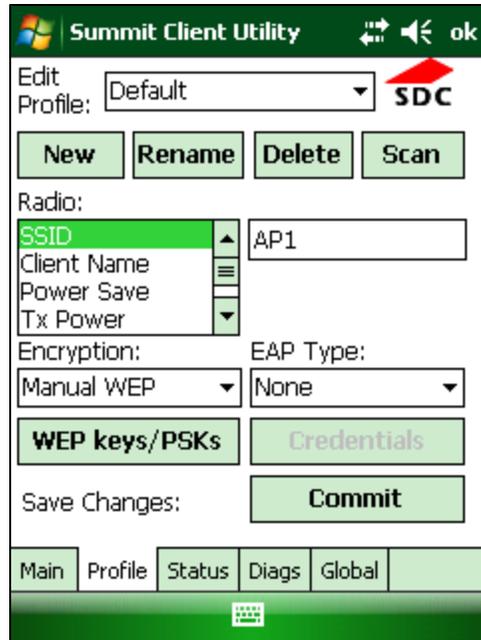
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

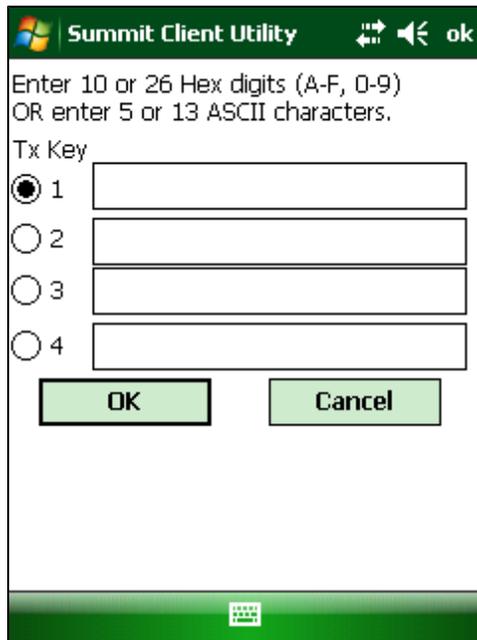
WEP

To connect using WEP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WEP** or **Manual WEP** (depending on SCU version)
- Set **Auth Type** to **Open**



Click the **WEP keys/PSKs** button.



Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click **OK**.

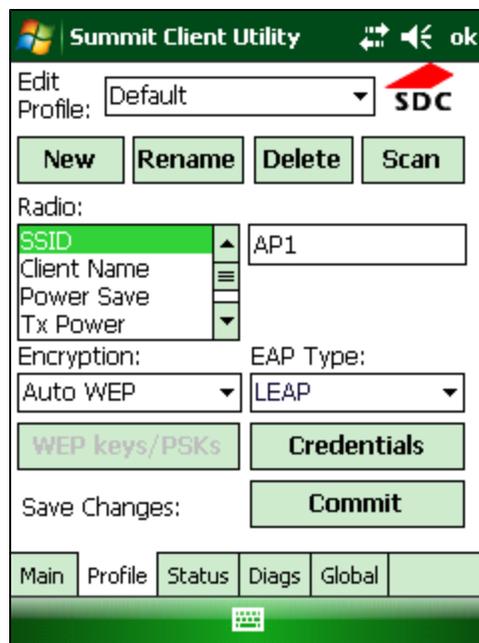
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

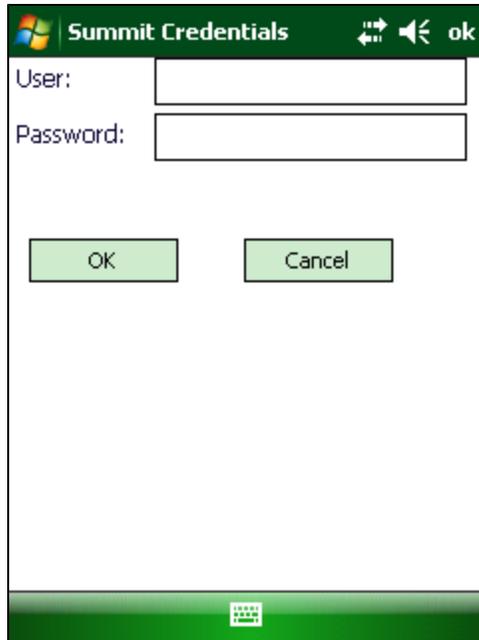
To use LEAP (without WPA), make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WEP EAP** or **Auto WEP** (depending on SCU version)
- Set **Auth Type** as follows:
 - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
 - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
 - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.



See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

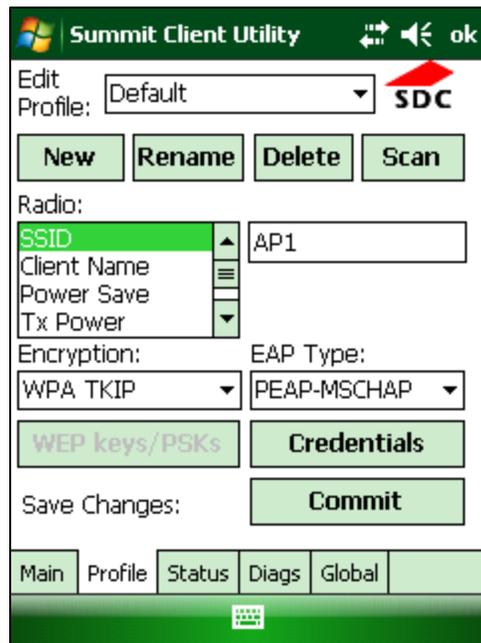
Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-MSCHAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

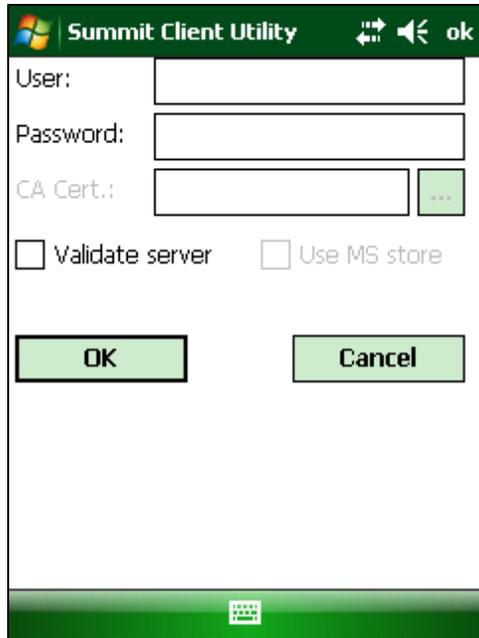


See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

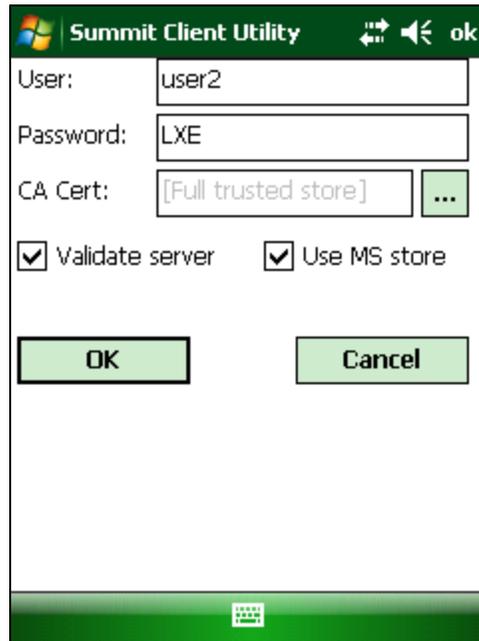
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the [Main Tab](#).

See [Windows Certificate Store vs. Certs Path](#) for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store** box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-GTC**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

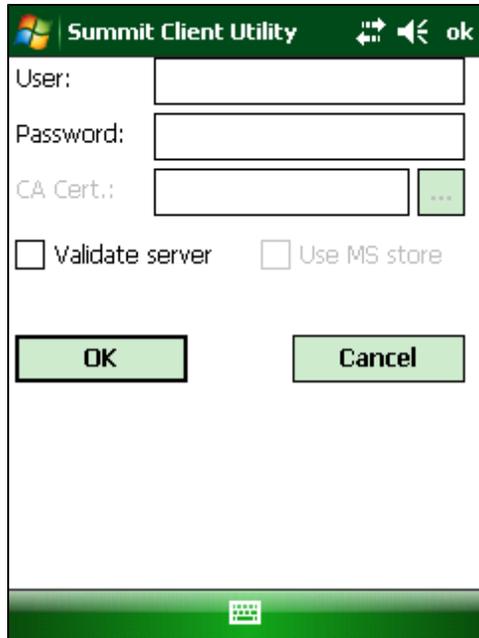
The screenshot shows the Summit Client Utility interface. At the top, it says "Summit Client Utility" with a Windows logo on the left and navigation icons on the right. Below the title bar, there is a dropdown menu for "Edit Profile:" set to "Default". To the right of this dropdown is a red arrow pointing to the text "SDC". Below the dropdown are four buttons: "New", "Rename", "Delete", and "Scan". Under the "Radio:" section, there is a list of options: "SSID", "Client Name", "Power Save", and "Tx Power". The "SSID" option is selected and highlighted in green, and its value is "AP1". Below the radio options, there are two dropdown menus: "Encryption:" set to "WPA TKIP" and "EAP Type:" set to "PEAP-GTC". Below these are two buttons: "WEP keys/PSKs" and "Credentials". At the bottom of the main configuration area, there is a "Save Changes:" label and a "Commit" button. At the very bottom, there is a navigation bar with buttons for "Main", "Profile", "Status", "Diags", and "Global".

See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

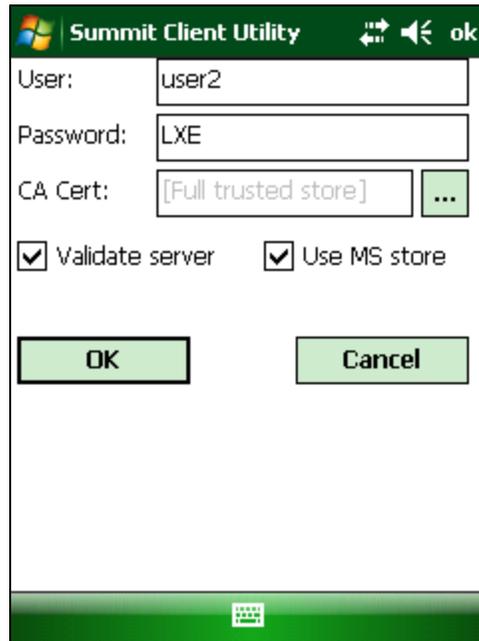
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the [Main Tab](#).

See [Windows Certificate Store vs. Certs Path](#) for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store box** unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

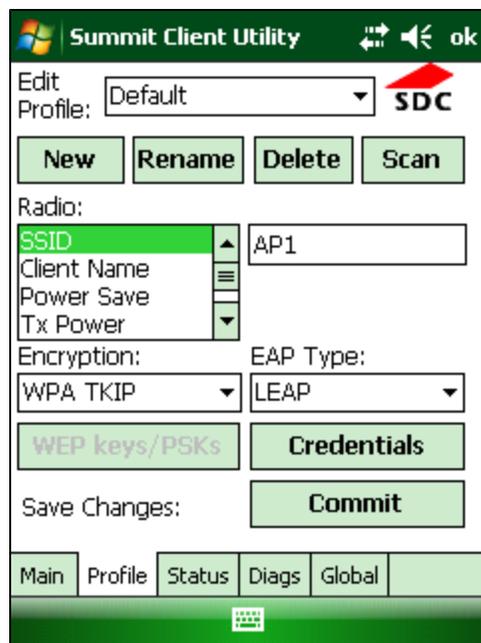
Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

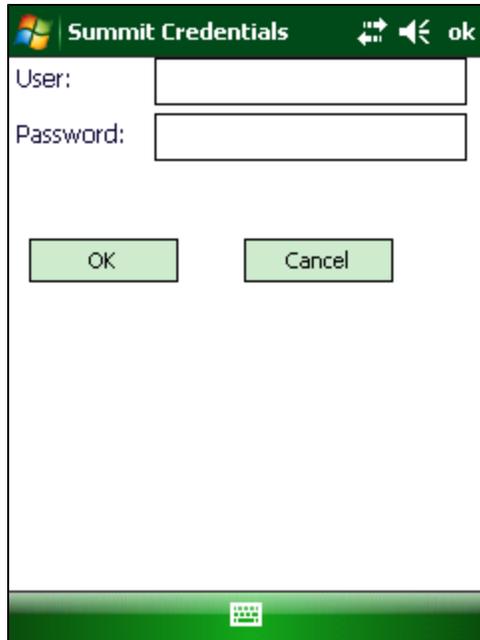
To use WPA/LEAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** as follows:
 - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
 - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
 - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.



See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

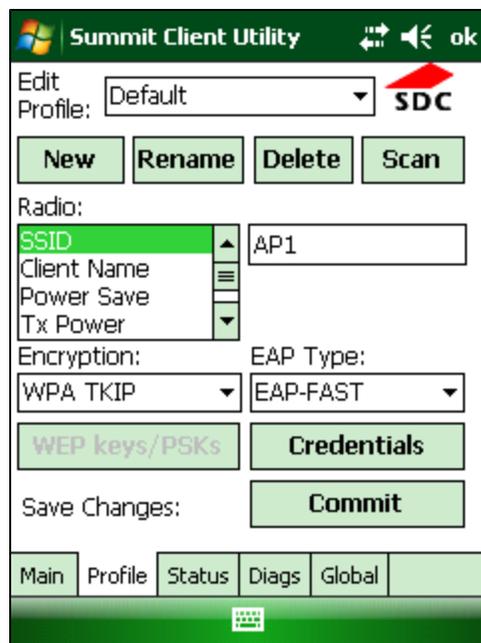
EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-FAST**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the MX8.



For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the MX8. The same username/password must be used to authenticate each time. See the note below for more details.

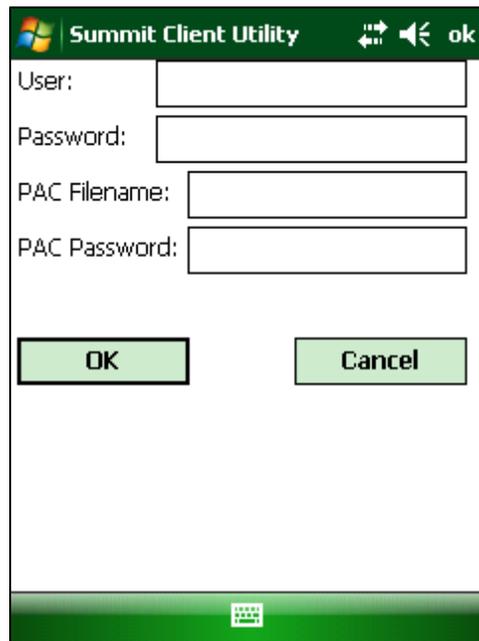
For manual PAC provisioning, the PAC filename and Password must be entered.

See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

Click on the **Credentials** button.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



To use Sign-On credentials:

- Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.

To use Stored Credentials:

- Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
- Enter the password.

To use Automatic PAC Provisioning:

- No additional entries are required.

To use manual PAC Provisioning:

- Enter the PAC Filename and PAC Password.
- The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.

Tap **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-TLS**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

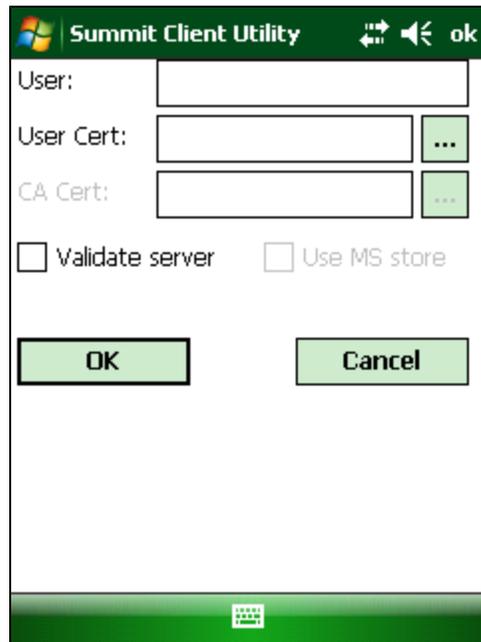
The screenshot shows the Summit Client Utility interface. At the top, it says "Summit Client Utility" with a Windows logo on the left and navigation icons on the right. Below the title bar, there is a dropdown menu for "Edit Profile:" set to "Default". To the right of this dropdown is a red arrow pointing to the text "SDC". Below the dropdown are four buttons: "New", "Rename", "Delete", and "Scan". Under the "Radio:" section, there is a list of options: "SSID", "Client Name", "Power Save", and "Tx Power". The "SSID" option is selected and highlighted in green, and its value is "AP1". Below the radio options, there are two dropdown menus: "Encryption:" set to "WPA TKIP" and "EAP Type:" set to "EAP-TLS". Below these are two buttons: "WEP keys/PSKs" and "Credentials". At the bottom of the main configuration area, there is a "Save Changes:" label and a "Commit" button. At the very bottom, there is a navigation bar with buttons for "Main", "Profile", "Status", "Diags", and "Global".

See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

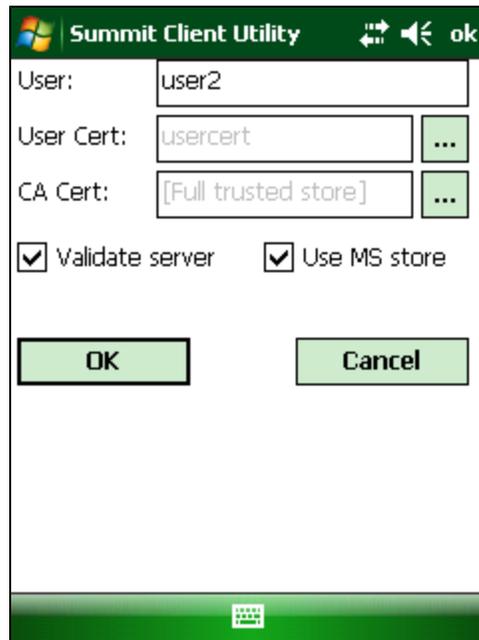
Select a user certificate from the Windows certificate store. Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the User Cert box.

Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions to [generate](#) and [install](#) the user certificate.

See [Windows Certificate Store vs. Certs Path](#) for more information on CA certificate storage.

Check the **Validate server** checkbox.



If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The MX8 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

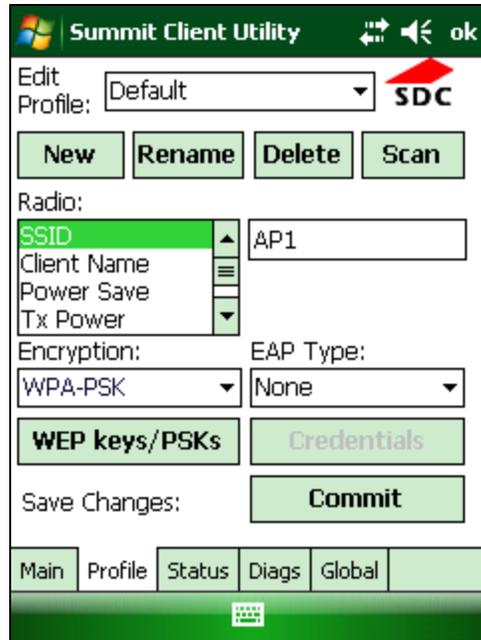
See [Certificates](#) for information on generating a Root CA certificate or a User certificate.

Note: The date must be properly set on the device to authenticate a certificate.

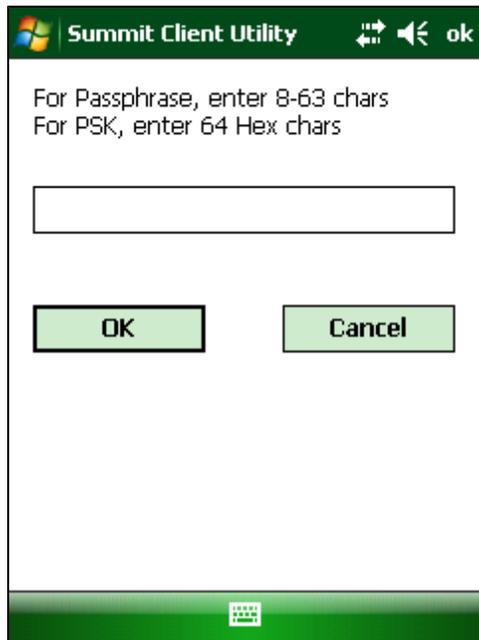
WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WPA PSK** or **WPA2 PSK**
- Set **Auth Type** to **Open**



Click the **WEP keys/PSKs** button.



This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and Suspend/Resume. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Please refer to the Security Primer to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the MX8 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Quick Start

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. [Generate a Root CA Certificate](#) and download it to a PC.
2. Connect the MX8 to the desktop PC using ActiveSync and copy the certificate to the MX8\System folder.
3. [Install the Root CA Certificate](#).

User Certificates are necessary for EAP-TLS

1. [Generate a User Certificate](#) and download it to a PC.
2. Install the User Certificate on the PC.
3. [Export the User Certificate](#) as a .PFX file.
4. Connect the MX8 to the desktop PC using ActiveSync and copy the certificate to the MX8\System folder.
5. [Install the User Certificate](#).
6. After installation, perform a Suspend/Resume.
7. [Verify installation](#).

Generating a Root CA Certificate

*Note: It is important that all **dates are correct** on the MX8 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the 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.



Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Click the **Download a CA certificate, certificate chain or CRL** link.

Make sure the correct root CA certificate is selected in the list box.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

A dropdown menu with a blue header containing the text 'Current'. The rest of the menu is empty.

Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.



Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

[Install](#) the certificate on the MX8.

Installing a Root CA Certificate

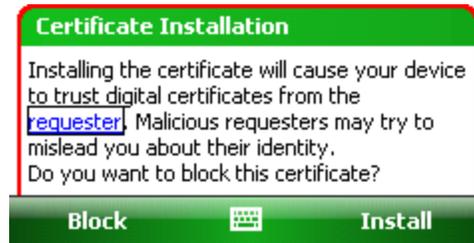
Note: This section is used only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

Copy the certificate file to the MX8. The certificate file has a .CER extension. Locate the file and tap it.

A certificate installation warning is displayed.



Tap **More**.



Tap **Install** to continue the installation. An installation successful message is displayed.

You can view any installed user certificates by selecting **Start > Settings > System** and tapping the **Certificates** icon.

Installed root certificates are displayed on the **Root** tab.

Generating a User Certificate

The easiest way to get the user certificate is to use the browser on a PC to navigate to the Certificate Authority. 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.



This process saves a user certificate file. There is no separate private key file as used on Windows CE devices.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Click the **Request a certificate** link.

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

Click on the **User Certificate** link.

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit:

[More Options >>](#)

Click on the **Submit** button. If there is a message box asking if you want to confirm the request, click **Yes**. The User Certificate is issued.

Certificate Issued

The certificate you requested was issued to you.



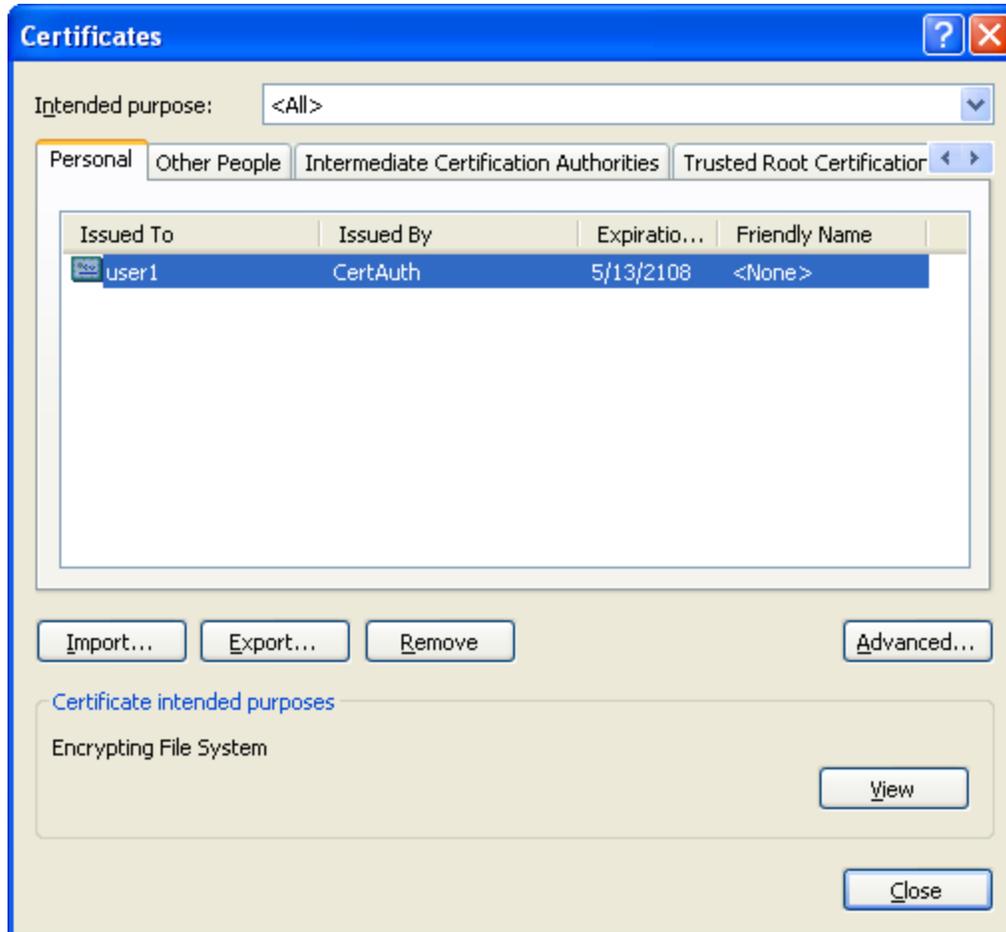
[Install this certificate](#)

Install the user certificate on the requesting computer by clicking the **Install this certificate** link. Export the certificate as described below.

Exporting a User Certificate

Start Internet Explore on the PC that requested the certificate.

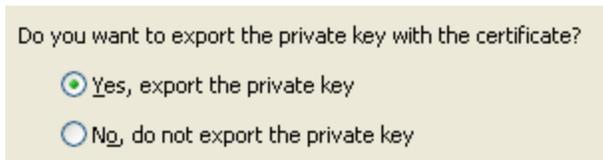
Select **Tools > Internet Options > Content** and click the **Certificates** button.



Make sure the **Personal** tab is selected. Highlight the certificate and click the **Export** button.

The Certificate Export Wizard is started.

Select **Yes, export the private key** and click Next.

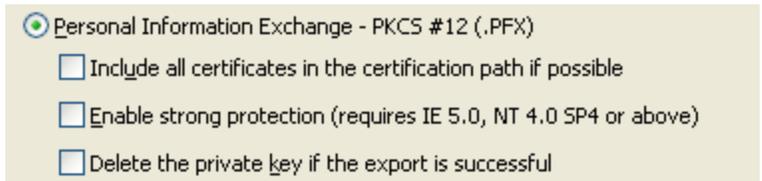


Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

Uncheck **Enable strong protection** and check **Next**.
The certificate type must be PKCS #12 (.PFX).



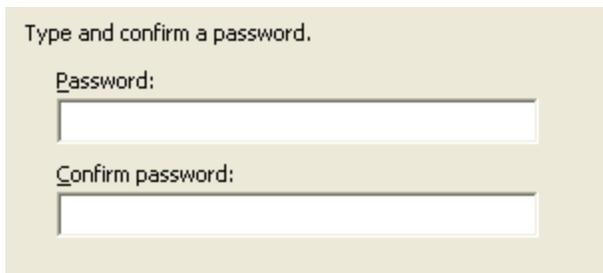
Personal Information Exchange - PKCS #12 (.PFX)

Include all certificates in the certification path if possible

Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

Delete the private key if the export is successful

When the private key is exported, you must enter the password, confirm the password and click **Next**. Be sure to remember the password as it is needed when installing the certificate.



Type and confirm a password.

Password:

Confirm password:

Supply the file name for the certificate. Use the **Browse** button to select the folder where you wish to store the certificate. The certificate is saved with a .PFX extension.



File name:

Browse...

Click Finish. and OK to close the Successful Export message.

Locate the User Certificate in the specified location. Copy to the MX8. [Install](#) the user certificate.

Installing a User Certificate

After [generating](#) and [exporting](#) the user certificate, copy it from the PC to the MX8. Copy the certificate to a location on the MX8, such as a storage card or the \System folder.

Locate the certificate file (it has a .PFX extension) and tap on it. You are prompted for the password that was assigned when the certificate was exported.



Enter the password and tap **Done**. A message is displayed that the certificate installation was successful.

You can view any installed user certificates by selecting **Start > Settings > System** and tapping the **Certificates** icon.



Installed user certificates are displayed on the **Personal** tab.



Chapter 8: Keymaps

Remember : “Sticky” keys are also known as “second” function keys. Ctrl, Alt, Shft, Blue and Orange keys are “sticky keys”. Sticky keys do not need to be held down before pressing the next (or desired) key. It is valid to use combined modifiers on specific keys.

The key mapping in this section relates to the physical keypad. See the Input Panel for the Virtual (or Soft) Keypad used with the stylus.

32 key Numeric-Alpha Keymap

- The following [keypad](#) keymap is used on an MX8 that is NOT running a Terminal Emulator. Honeywell terminal emulators use a separate keymap.
- When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shft sticky key or the Caps key sequence (Blue+Tab) for upper case alphabetic characters.
- Pressing the Alph key forces “Alpha” mode for the 2,3,4,5,6,7,8, and 9 keys. The 1 and 0 keys continue to place a 1 and 0 into the text field.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alph key to toggle between Alpha and Numeric mode.
- When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.
- Pressing the Power key when in any sticky mode (Blue, Orange, Shift, etc) either turns the device On (when Off) or places it in Suspend (when On).
- For those keymaps that require remapping (MAP), keys can be remapped using the Buttons Panel (Start > Settings > Personal > Buttons).

To get this Key / Function	Press these Keys in this Order		
Power / Suspend	Power		
Field Exit (default is VK_PAUSE) MAP = Mappable	Blue (MAP)	Shft (MAP)	Diamond #1
=	Orange	Shft (MAP)	Diamond#2 Default is Mappable
(Blue	Shft (MAP)	Diamond#2 Default is Mappable
!	Orange	Shft (MAP)	Diamond#3 Default is Mappable
)	Blue	Shft (MAP)	Diamond#3 Default is Mappable
Volume Adjust Mode	Orange	Scan	Up Arrow Down Arrow
Display Backlight Brightness Adjust Mode	Blue	Scan	Up Arrow Down Arrow

To get this Key / Function	Press these Keys in this Order		
Toggle Alpha Mode	Alph		
Toggle Blue Mode	Blue		
Toggle Orange Mode	Orange		
Toggle Shift Mode	Shft		
Alt Mode	Alt		
Control Mode	Ctrl		
Esc	Blue	Alt	
Space	Spc		
Enter	Enter		
Scan Mode	Scan		
CapsLock (Toggle)	Blue	Tab	
Back Space	Orange	Spc	
Tab	Tab		
Back Tab	Orange	Tab	
Up Arrow	Up Arrow		
Down Arrow	Down Arrow		
Right Arrow	Blue	Up Arrow	
Left Arrow	Blue	Down Arrow	
Insert	Orange	Ctrl	
Delete	Del		
Home	Shft	Down Arrow	
End	Shft	Up Arrow	
Page Up	Orange	Up Arrow	
Page Down	Orange	Down Arrow	
F1	F1		
F2	F2		
F3	F3		
F4	F4		
F5	F5		
F6	Orange	F1	
F7	Orange	F2	
F8	Orange	F3	
F9	Orange	F4	
F10	Orange	F5	

To get this Key / Function	Press these Keys in this Order		
F11	Blue	F1	
F12	Blue	F2	
F13	Blue	F3	
F14	Blue	F4	
F15	Blue	F5	
F16	Shft	F1	
F17	Shft	F2	
F18	Shft	F3	
F19	Shft	F4	
F20	Shft	F5	
F21	Shft	Orange	F1
F22	Shft	Orange	F2
F23	Shft	Orange	F3
F24	Shft	Orange	F4
a	Alpha	2	
b	Alpha	22	
c	Alpha	222	
d	Alpha	3	
e	Alpha	33	
f	Alpha	333	
g	Alpha	4	
h	Alpha	44	
i	Alpha	444	
j	Alpha	5	
k	Alpha	55	
l	Alpha	555	
m	Alpha	6	
n	Alpha	66	
o	Alpha	666	
p	Alpha	7	
q	Alpha	77	
r	Alpha	777	
s	Alpha	7777	
t	Alpha	8	

To get this Key / Function	Press these Keys in this Order		
u	Alpha	88	
v	Alpha	888	
w	Alpha	9	
x	Alpha	99	
y	Alpha	999	
z	Alpha	9999	
A	Shft	Alpha	2
B	Shft	Alpha	22
C	Shft	Alpha	222
D	Shft	Alpha	3
E	Shft	Alpha	33
F	Shft	Alpha	333
G	Shft	Alpha	4
H	Shft	Alpha	44
I	Shft	Alpha	444
J	Shft	Alpha	5
K	Shft	Alpha	55
L	Shft	Alpha	555
M	Shft	Alpha	6
N	Shft	Alpha	66
O	Shft	Alpha	666
P	Shft	Alpha	7
Q	Shft	Alpha	77
R	Shft	Alpha	777
S	Shft	Alpha	7777
T	Shft	Alpha	8
U	Shft	Alpha	88
V	Shft	Alpha	888
W	Shft	Alpha	9
X	Shft	Alpha	99
Y	Shft	Alpha	999
Z	Shft	Alpha	9999
1	1		
2	2		

To get this Key / Function	Press these Keys in this Order		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
0	0		
. (period)	Orange	DEL	
<	Blue	7	
[Blue	2	
[Orange	2	
]	Blue	3	
]	Orange	3	
>	Blue	8	
=	Orange	Diamond#2	
{	Blue	4	
}	Blue	5	
/	Blue	1	
-	Blue	Spc	
+	Blue	Del	
* (asterisk)	Orange	Diamond#1	
* (asterisk)	Shft	8	
: (colon)	Orange	0 (zero)	
; (semicolon)	Blue	0 (zero)	
?	Orange	8	
` (accent)	Blue	6	
_ (underscore)	Orange	7	
, (comma)	Orange	6	
' (apostrophe)	Orange	Alph	
~ (tilde)	Blue	9	
\	Orange	1	
	Orange	Alt	
"	Blue	Alph	

To get this Key / Function	Press these Keys in this Order		
!	Orange	Diamond#3	
!	Shft	1	
@	Orange	5	
@	Shft	2	
#	Orange	4	
#	Shft	3	
\$	Orange	9	
\$	Shft	4	
%	Shft	5	
^	Blue	Ctrl	
^	Shft	6	
&	Shft	7	
(Blue	Diamond#2	
(Shft	9	
)	Blue	Diamond#3	
)	Shft	0 (zero)	

32 key Alpha-Mode Keymap

- The following [keypad](#) keymap is used on an MX8 that is NOT running a Terminal Emulator. Honeywell terminal emulators use a separate keymap.
- When using a sequence of keys that require an alpha key, first press the Alph key. Use the Shft sticky key for upper case alphabetic characters.
- Tapping the Power key when in any sticky mode (Blue, Orange, Shift, etc) either turns the device On (when Off) or places it in Suspend (when active).
- Pressing the Alph key locks the keypad into alpha mode. Pressing Alph a second time toggles alpha mode off.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alph key to toggle between Alpha and Numeric mode.
- Since letters are mapped to Alt, Ctl, Shft, these modifiers must be pressed before Alph. For example, for Alt T, press Alt, then Alph, then Alt again.
- When using a sequence of keys that do not include the Alph key but does include a sticky key, press the sticky key first then the rest of the key sequence.
- For those keymaps that require remapping (MAP), keys can be remapped using the Buttons Panel (Start > Settings > Personal > Buttons).

To get this Key / Function	Press these Keys in this Order		
Power / Suspend	Power		
Field Exit (default is VK_PAUSE) MAP = Mappable	Blue (MAP)	Shft (MAP)	Diamond #1
=	Orange	Shft (MAP)	Diamond#2 Default is Mappable
(Blue	Shft (MAP)	Diamond#2 Default is Mappable
!	Orange	Shft (MAP)	Diamond#3 Default is Mappable
)	Blue	Shft (MAP)	Diamond#3 Default is Mappable
Volume Adjust Mode	Orange	Scan	Up Arrow Down Arrow
Display Backlight Brightness Adjust Mode	Blue	Scan	Up Arrow Down Arrow
Toggle Alpha Mode	Alph		
Toggle Blue Mode	Blue		
Toggle Orange Mode	Orange		
Toggle Shift Mode	Shft		
Alt Mode	Alt		
Control Mode	Ctrl		

To get this Key / Function	Press these Keys in this Order		
Esc	Blue	Alt	
Space	Spc		
Enter	Enter		
Scan Mode	Scan		
CapsLock (Toggle)	Blue	Shft	
Uppercase Alpha	Shft		
Back Space	Orange	Spc	
Tab	Tab		
Back Tab	Orange	Tab	
Up Arrow	Up Arrow		
Down Arrow	Down Arrow		
Right Arrow	Blue	Up Arrow	
Left Arrow	Blue	Down Arrow	
Insert	Orange	Ctrl	
Delete	Del		
Home	Shft	Down Arrow	
End	Shft	Up Arrow	
Page Up	Orange	Up Arrow	
Page Up	Orange	8	
Page Down	Orange	7	
Page Down	Orange	Down Arrow	
F1	F1		
F2	F2		
F3	F3		
F4	F4		
F5	F5		
F6	Orange	F1	
F7	Orange	F2	
F8	Orange	F3	
F9	Orange	F4	
F10	Orange	F5	
F11	Blue	F1	
F11	Blue	1	
F12	Blue	F2	

To get this Key / Function	Press these Keys in this Order		
F12	Blue	2	
F13	Blue	F3	
F13	Blue	3	
F14	Blue	F4	
F14	Blue	4	
F15	Blue	F5	
F15	Blue	5	
F16	Shft	F1	
F17	Shft	F2	
F18	Shft	F3	
F19	Shft	F4	
F20	Shft	F5	
F21	Shft	Orange	F1
F22	Shft	Orange	F2
F23	Shft	Orange	F3
F24	Shft	Orange	F4
a	Alpha	F3	
b	Alpha	F4	
c	Alpha	F2	
d	Alpha	F5	
e	Alpha	F1	
f	Alpha	Diamond 1	
g	Alpha	Down Arrow	
h	Alpha	Up Arrow	
i	Alpha	Tab	
j	Alpha	Shft	
k	Alpha	1	
l	Alpha	2	
m	Alpha	3	
n	Alpha	4	
o	Alpha	5	
p	Alpha	6	
q	Alpha	7	
r	Alpha	8	

To get this Key / Function	Press these Keys in this Order		
s	Alpha	9	
t	Alpha	Alt	
u	Alpha	0 (zero)	
v	Alpha	Spc	
w	Alpha	Ctl	
x	Alpha	Del	
y	Alpha	Diamond 2	
z	Alpha	Diamond 3	
A	Shft	Alpha	F3
B	Shft	Alpha	F4
C	Shft	Alpha	F2
D	Shft	Alpha	F5
E	Shft	Alpha	F1
F	Shft	Alpha	Diamond 1
G	Shft	Alpha	Down Arrow
H	Shft	Alpha	Up Arrow
I	Shft	Alpha	Tab
J	Shft	Alpha	Shft
K	Shft	Alpha	1
L	Shft	Alpha	2
M	Shft	Alpha	3
N	Shft	Alpha	4
O	Shft	Alpha	5
P	Shft	Alpha	6
Q	Shft	Alpha	7
R	Shft	Alpha	8
S	Shft	Alpha	9
T	Shft	Alpha	Alt
U	Shft	Alpha	0 (zero)
V	Shft	Alpha	Spc
W	Shft	Alpha	Ctl
X	Shft	Alpha	Del
Y	Shft	Alpha	Diamond 2
Z	Shft	Alpha	Diamond 3

To get this Key / Function	Press these Keys in this Order		
1	1		
2	2		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
0	0 (zero)		
. (period)	Orange	Diamond 3	
<	Blue	7	
[Blue	2	
]	Orange	3	
>	Blue	8	
=	Orange	Del	
{	Orange	4	
}	Orange	5	
/	Orange	Alph	
-	Orange	Spc	
+	Orange	9	
* (asterisk)	Orange	0 (zero)	
* (asterisk)	Shft	8	
: (colon)	Blue	Diamond 3	
; (semicolon)	Blue	0 (zero)	
?	Orange	Diamond 1	
` (accent)	Blue	6	
_ (underscore)	Blue	Diamond 2	
, (comma)	Orange	Diamond 2	
' (apostrophe)	Orange	1	
~ (tilde)	Blue	9	
\	Blue	Diamond 1	
	Orange	Alt	
"	Blue	Alph	

To get this Key / Function	Press these Keys in this Order		
!	Shft	1	
@	Shft	2	
#	Shft	3	
\$	Shft	4	
%	Shft	5	
^	Shft	6	
&	Shft	7	
(Shft	9	
)	Shft	0 (zero)	

Chapter 9: Technical Specifications

Processor	Marvell Xscale PXA-27X CPU operating at 520 MHz. Turbo mode switching is supported. 32 bit CPU (with on-chip cache)
Memory	128 MB SDRAM 128 MB Strata Flash 20 MB available for programs and data
Mass Storage	Removable Mini SD Card. 128MB
Operating System	Microsoft® Windows® Mobile® 6.1
Radio Modules	802.11 a/b/g radio / Bluetooth
Scanner options	Integrated. No Scanner Intermec EV-15 Linear Imager Hand Held Products 5300 SF 2D Imager Symbol 955I (Short Range) Symbol 955E (Base Laser) Honeywell Laser Scanner, N43XX
Display technology	Transmissive Color LCD with Touchscreen. Customer Configurable Display. LED Backlighting Type - LCD – Active Transmissive Color / LED Backlight Resolution - 320 (Vertical) x 240 (Horizontal) pixels Size - 1/4 VGA portrait Diagonal Viewing Area - 2.8 in (7.12cm) Dot Pitch - 60 (W)um X 180 (H) um Dot Size - 180 um X 180 um Color Scale - 256 colors
External Connectors / Interface	20 pin Multi function I/O connector. Provides cabled connection to external devices such as an audio headset, USB/power connection, RS-232/power connection.
Main Battery	Li-Ion battery pack 3.7V 2.3000mAh. In-Unit and External Re-Chargeable
Backup Battery (CMOS)	Internal Nickel Metal Hydride (Ni-MH) 2.4V max. Automatically charges from main battery during normal operation. Requires AC power for re-charging. Memory operational for 5 minutes when main battery is depleted. Minimum life expectancy is 2 years.

Dimensions and Weight

Dimension	
Length	7.58" 19.2 cm
Width at Display Width at handgrip	2.84" 7.2 cm 2.45" 6.2 cm
Depth at Scanner Depth at Battery	1.72" 4.36.1 cm 1.52" 3.86 cm
Weight	
Unit with network card, battery, SE955 scanner and handle	1 lbs 458g
Unit with network card, battery, SE955 scanner and handstrap	0.84 lbs 385g
Battery	2.8 oz 80g
Network Card	0.35 oz 9.9g
Mini SD Flash Card	0.035 oz 1g

Environmental Specifications

Operating Temperature	14°F to 122°F (-10°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
ESD	8 KV air, 4kV direct contact
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Water and Dust	IEC 60529 compliant to IP54
Vibration	Based on MIL Std 810D

Network Card Specifications

Summit 802.11 b/g

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	50 mW max.
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	Same as MX8 Operating Temperature
Storage Temperature	Same as MX8 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Summit 802.11 a/b/g

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC : 1-11, 36, 40, 44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44, 48
Operating Temperature	Same as MX8 Operating Temperature
Storage Temperature	Same as MX8 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 feet (10 meters) line of sight
Operating Frequency	2.402 – 2.480 GHz
Bluetooth Version	2.0 + EDR

Pinout I/O Port

Pin No	Pin Description
1	UART_TXD
2	UART_RTS
3	UART_RXD
4	UART_CTS
5	GND
6	USBC_D+
7	USBC_VBUS
8	HS_OUT
9	HS_SLEEVE
10	HS_DETECT
11 to 13	DC_GND
14	UART_DTR
15	UART_DSR
16	USBC_D-
17	HS_MIC
18 to 20	DC_IN

AC Wall Adapter

Feature	Specification
Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Current Fuse
Input Voltage	100VAC min – 240 VAC max
Input Frequency	50 - 60 Hz
Input Connector	North American wall plug, no ground
Output Connector	AC wall adapter has a 5.5mm barrel connector. This connects to the cables which transition power to the 20 pin D connector.
Output Voltage	+5V, regulated
Output Current	0 Amps min, 3 Amps max
Operating Temperature	32 F to 100° F / -0° C to 40° C The AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.
Storage Temperature	-40° F to 180° F / -40° C to 80° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)



Chapter 10: Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select **Support > Contact Service and Repair** to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT

SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

The duration of the limited warranty for the MX8 is 1 year.

The duration of the limited warranty for the MX8 Desktop Cradle is 1 year.

The duration of the limited warranty for the MX8 Passive Vehicle Cradle is 1 year.

The duration of the limited warranty for the MX8 Battery Charger is 1 year.

The duration of the limited warranty for the MX8 3000mAh Li-Ion Battery is 6 months.

The duration of the limited warranty for the MX8 Charging Multi-Dock is 1 year.

The duration of the limited warranty for the MX8 AC power supply and cables is 1 year.

The duration of the limited warranty for the MX8 cables (USB, Serial, Communication, Power) is 1 year.

The duration of the limited warranty for the MX8 fabric accessories (e.g., belt, case, holster) is 90 days.



Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
www.honeywellaidc.com

E-EQ-MX8WMRG
Rev J
10/12