MC3200 INTEGRATOR GUIDE

MN000887A03-A Dec 2018

Copyrights

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your contact for further information.

Trademarks

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
A01 Rev. A	6/2014	Initial release.
A02 Rev. A	3/2018	Update approved cleanser active ingredients.
A03 Rev. A	12/2018	Add boot to accessory list.

Contents

About This Guide

This guide provides information about using the MC32N0 Series of mobile computers and accessories.

Note: Screens and windows pictured in this guide are samples and can differ from actual screens.

MC32N0 Series Documentation Set

The documentation set for the MC32N0 Series provides information for specific user needs, and includes:

- *MC32N0 Quick Start Guide* - describes how to get the device up and running.
- *MC32N0 Regulatory Guide* - provides required regulatory information.
- *MC32N0 User Guide* - describes how to use the device.
- *MC32N0 Integrator Guide* - describes how to set up the device and accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
MC32N0–G Standard	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	512 MB RAM / 2 GB Flash	Imager or laser scanner	Windows CE 7.0
MC32N0–G Premium	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	1 GB RAM / 4 GB Flash	Imager or laser scanner, Interactive Sensor Technology (IST)	Android-based, Android Open-Source Project 4.1.1 or Windows CE 7.0
MC32N0–R Standard	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	512 MB RAM / 2 GB Flash	Laser scanner	Windows CE 7.0
MC32N0–R Premium	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	1 GB RAM / 4 GB Flash	Laser scanner, IST	Android-based, Android Open-Source Project 4.1.1 or Windows CE 7.0

Table continued…

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
MC32N0–S Standard	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	512 MB RAM / 2 GB Flash	Imager or laser scanner	Windows CE 7.0
MC32N0–S Premium	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	3.0” color	1 GB RAM / 4 GB Flash	Imager or laser scanner, IST	Android-based, Android Open-Source Project 4.1.1 or Windows CE 7.0

Software Versions for Android

To determine the current software versions touch > **About device**.

- **Serial number** – Displays the serial number.
- **Model number** – Displays the model number.
- **Android version** – Displays the operating system version.
- **Kernel version** – Displays the kernel version number.
- **Build number** – Displays the software build number.

Software Versions for WinCE

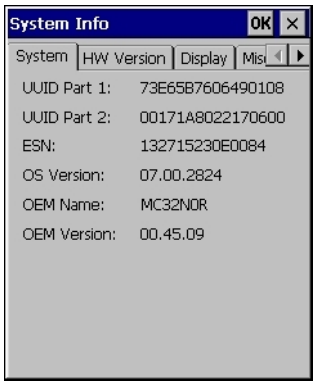
This guide covers various software configurations and references are made to operating system or software versions for:

- OEM version
- BTExplorer version
- Fusion version.

OEM Version

To determine the OEM software version tap **Start** > **Settings** > **Control Panel** > **System Info** icon > **System** tab.

Figure 1: System Info – OEM Version



BTExplorer Software

Note: StoneStreet Bluetooth stack has to be enabled to see version number.

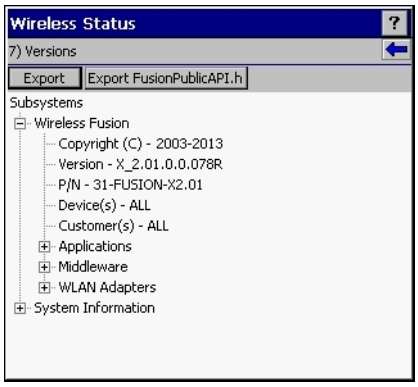
To determine the BTExplorer software version tap **BTExplorer** icon > **Show BTExplorer** > **File** > **About**.

Figure 2: BTExplorer Version

Fusion Software

To determine the Fusion software version tap **Wireless Strength** icon > **Wireless Status** > **Versions**.

Figure 3: Fusion Version



Chapter Descriptions

Topics covered in this guide are as follows:

- *Getting Started on page 19* provides information on getting the MC32N0 up and running for the first time.
- *Accessories on page 29* describes the available accessories and how to use them with the MC32N0.
- *USB Communication on page 55* describes how to connect the MC32N0 to a host computer using USB.
- *DataWedge Configuration on page 57* describes how to use and configure the DataWedge application.
- *Administrator Utilities on page 87* provides information for using the suite of administrative tools for configuring the MC32N0.
- *Settings for Android Devices on page 107* provides the settings for configuring the MC32N0 with Android.
- *Application Deployment for Android Devices on page 117* provides information for developing and managing applications with Android.

- *Synchronization on page 129* provides instructions on installing ActiveSync, setting up a partnership and synchronizing information between the MC32N0 and a host computer.
- *Settings for WinCE Devices on page 135* provides the settings for configuring the MC32N0 with WinCE.
- *Application Deployment for Windows CE on page 145* provides information for developing and managing applications with WinCE.
- *Maintenance and Troubleshooting on page 159* includes instructions on cleaning and storing the MC32N0, and provides troubleshooting solutions for potential problems during MC32N0 operation.
- *Technical Specifications on page 169* provides the technical specifications for the MC32N0.

Notational Conventions

The following conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Icons on a screen.
- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, lists that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set. These icons and their associated meanings are described below.

Warning: The word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.

Caution: The word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.

Note: NOTE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is located on the screen. There is no warning level associated with a note.

Related Documents

- *MC32N0 Quick Start Guide*, p/n MN000215Axx
- *MC32N0 Regulatory Guide*, p/n MN000216Axx
- *MC32N0 User Guide*, p/n MN000886Axx

For the latest version of this guide and all guides, go to: *http://www.zebra.com/support*.

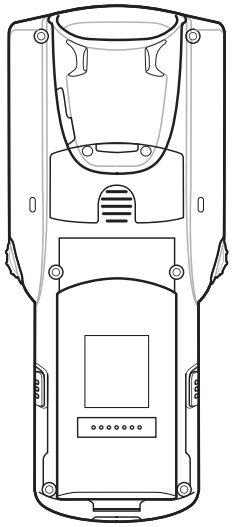
Service Information

If you have a problem with your equipment, contact Zebra Support Center for your region. Contact information is available at: *http://www.zebra.com/support*.

When contacting the Zebra Support Center, please have the following information available:

- Serial number of the unit (found on manufacturing label)
- Model number or product name (found on manufacturing label)
- Software type and version number

Figure 4: Manufacturing Label Location



Zebra responds to calls by email or telephone within the time limits set forth in support agreements.

If your problem cannot be solved by the Zebra Support Center, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your product from a Zebra business partner, contact that business partner for support.

Chapter 1

Getting Started

This chapter provides information for getting the device up and running for the first time.

Setup

To start using the MC32N0 for the first time:

- Install a microSD card (optional)
- Install the battery
- Charge the MC32N0
- Power on the MC32N0.

Installing a microSD Card

The microSD card slot provides secondary non-volatile storage. The slot is located under the battery pack. Refer to the documentation provided with the card for more information, and follow the manufacturer's recommendations for use.

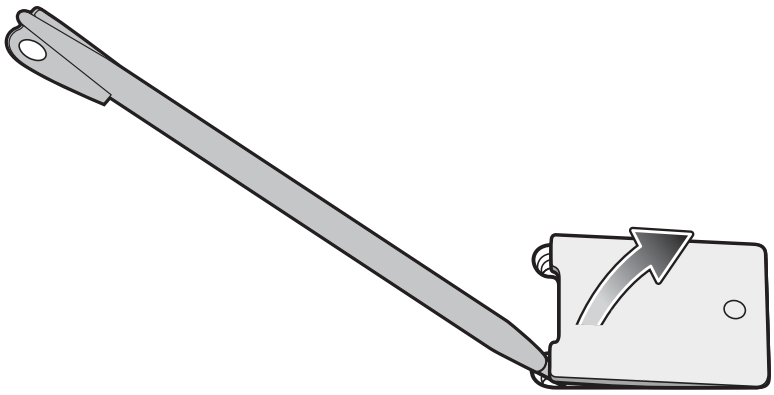
Caution: Follow proper electrostatic discharge (ESD) precautions to avoid damaging the microSD card. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

Note: On Android devices, after installing the microSD card, the device will automatically reset. This ensures proper reading of the file content on the microSD card.

Procedure:

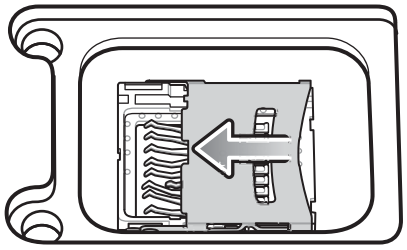
1 Remove the microSD card cover.

Figure 5: Remove microSD Card Cover



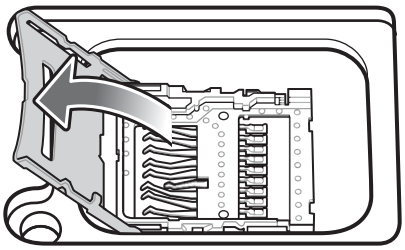
2 Slide the microSD card holder down to unlock.

Figure 6: Unlock microSD Card Holder



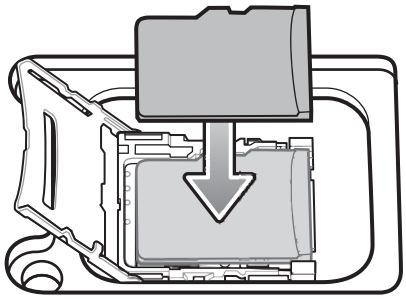
3 Lift the microSD card holder.

Figure 7: Lift microSD Card Holder



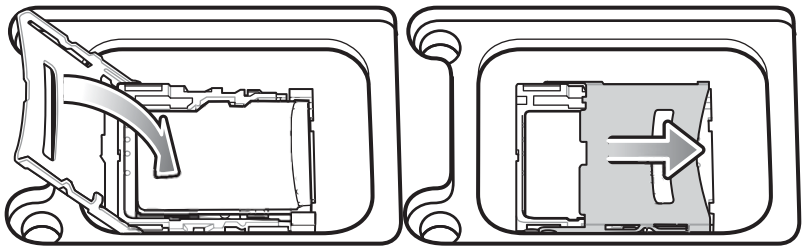
4 Place the microSD card into the contact area.

Figure 8: Install microSD Card



5 Close the microSD card holder and slide the microSD card holder up to lock.

Figure 9: Lock microSD Card Holder



6 Replace the microSD card cover and ensure that it is installed properly.

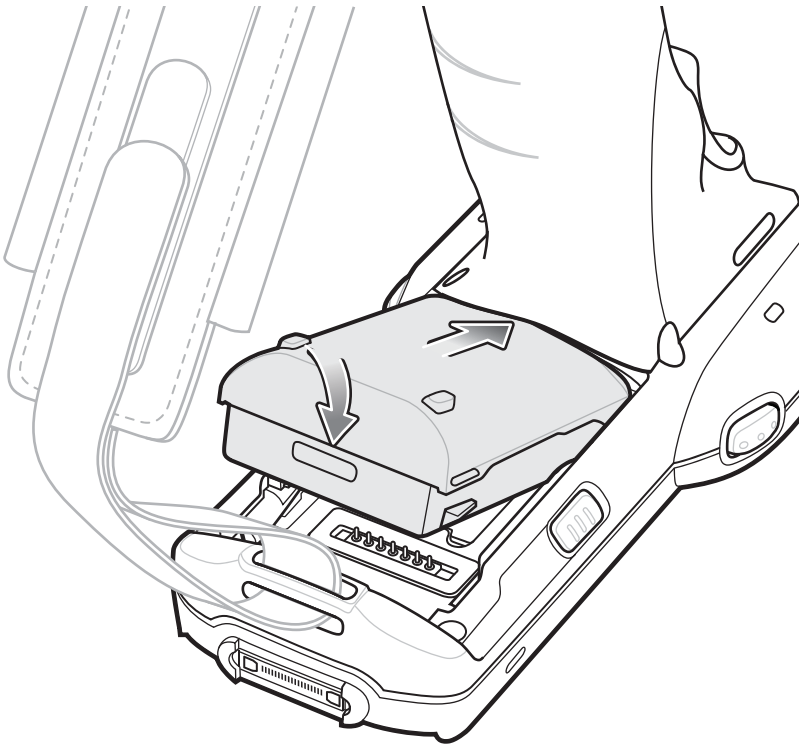
Installing the MC32N0-G Battery

To install the battery:

Procedure:

1 Align the battery into the battery compartment.

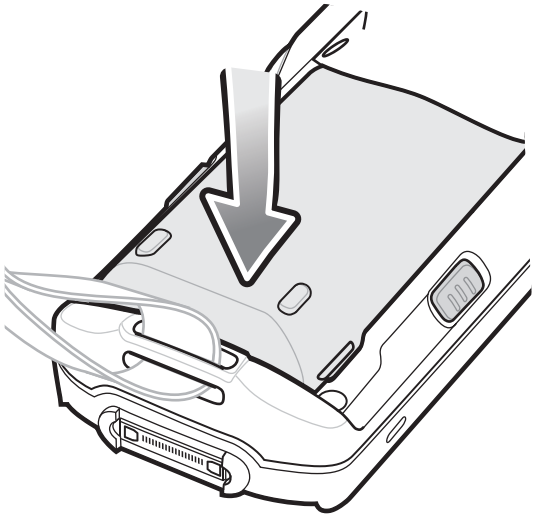
Figure 10: Inserting the Battery



2 Rotate the bottom of the bottom into the battery compartment.

3 Press battery down firmly. Ensure that both battery release buttons on the sides of the MC32N0 return to the home position.

Figure 11: Press Battery Down



4 Press the Power button to turn on the device.

5 On WinCE device with Rev B software, after boot up the calibration screen appears. Using the stylus, touch the targets as they appear on the screen.

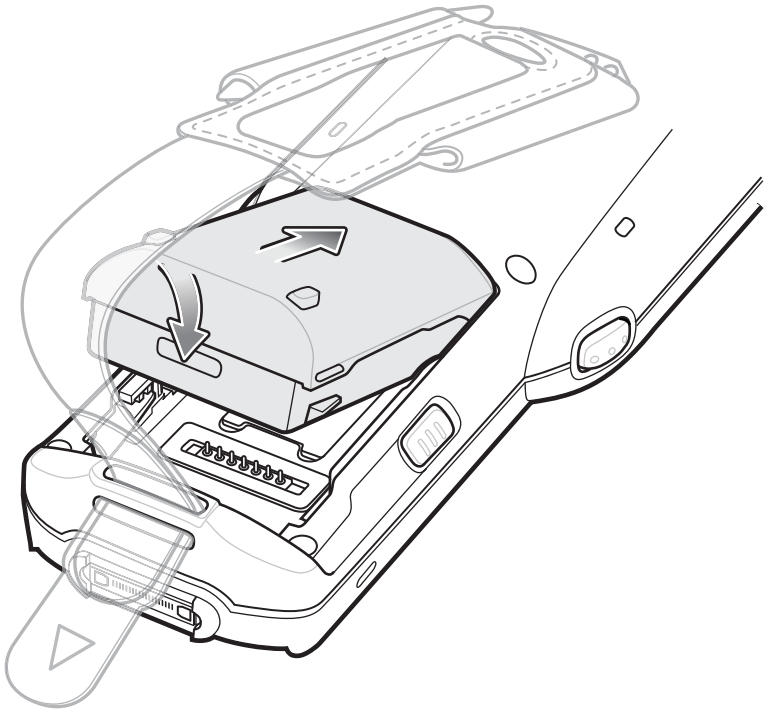
Installing the MC32N0–R/S Battery

Procedure:

1 Loosen the handstrap.

2 Align the top of the battery into the battery compartment.

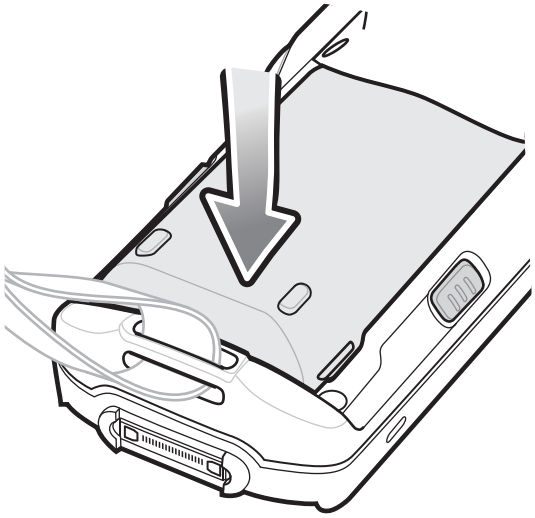
Figure 12: Inserting the Battery



3 Rotate the bottom of the bottom into the battery compartment.

4 Press battery down firmly. Ensure that both battery release buttons on the sides of the MC32N0 return to the home position.

Figure 13: Press Battery Down



5 Tighten the handstrap.

6 Press the Power button to turn on the device.

7 On WinCE device with Rev B software, after boot up the calibration screen appears. Using the stylus, touch the targets as they appear on the screen.

Charging the Battery

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

Use the mobile computer cradles, cables and spare battery chargers to charge the mobile computer main battery.

The main battery can be charged before insertion into the mobile computer or after it is installed. There are two main batteries for the MC32N0, the Standard Battery (1X) and the Extended Life Battery (2X). The standard capacity battery ships from the factory in all MC32N0-R configurations. The Extended Life Battery ships from the factory in all MC32N0-S and MC32N0-G configurations. To install an Extended Life Battery in the MC32N0-R configurations, purchase an Extended Life Battery. Use one of the spare battery chargers to charge the main battery (out of the mobile computer) or one of the cradles to charge the main battery while it is installed in the mobile computer.

Before using the mobile computer for the first time, fully charge the main battery until the amber Charge LED Indicator remains lit (see *Table 1: LED Charge Indicators on page 23* for charge status indications). The Standard Battery fully charges in less than five hours and the Extended Life Battery fully charges in less than eight hours.

The MC32N0 retains data in memory for at least five minutes when the mobile computer's main battery is removed or fully discharged.

When the main battery reaches a very low battery state, the battery retains data in memory for at least 36 hours.

Batteries must be charged within the 0° to +40° C (32° to 104° F) ambient temperature range.

The following accessories can be used to charge batteries:

- Cradles (and a power supply):
  - Single Slot Serial/USB Cradle with Battery Adapter
  - Four Slot Cradles.
- Cables (and a power supply):
  - USB Client Charge Cable
  - Serial (RS232) Charge Cable.
- Spare Battery Chargers (and a power supply):
  - Four Slot Spare Battery Charger
  - Universal Battery Charger (UBC) Adapter with Battery Adapter.

To charge the mobile computer using the cradles:

1. Insert the mobile computer into a cradle. See *Accessories on page 29* for accessory setup.

2. The mobile computer starts to charge automatically. The amber Charge LED Indicator indicates the charge status. See the table below for charging indications.

To charge the mobile computer using the cables:

1. Connect the MC32N0 Communication/Charge Cable to the appropriate power source and connect to the mobile computer. See *Accessories on page 29* for accessory setup.

2. The mobile computer starts to charge automatically. The amber Charge LED Indicator indicates the charge status.

Table 1: LED Charge Indicators

Status	Indications
Off	MC32N0 is not charging.

Table continued…

Status	Indications
	MC32N0 is not inserted correctly in the cradle. MC32N0 is not connected to a power source. Charger or cradle is not powered.
Slow Blinking Amber	MC32N0 is charging.
Solid Amber	Charging complete. Note: When the battery is initially inserted in the mobile computer, the amber LED flashes once if the battery power is low.
Fast Blinking Amber	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).

Charging Temperature

Charge batteries in ambient temperatures from 0 °C to 40 °C (32 °F to 104 °F) or up to 45 °C (113 °F) as reported by the battery. To view the battery temperature on Android devices, touch the **Battery Info** icon on the Home screen or touch  >  **About device** > **Battery Information**.

Note that charging is intelligently controlled by the MC32N0. To accomplish this, for small periods of time, the MC32N0 or accessory alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC32N0 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

Charging Spare Batteries

See *Accessories on page 29* for information on using accessories to charge spare batteries.

Resetting the Android Device

There are two reset functions, soft reset and hard reset.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

Procedure:

1 Press and hold the Power button until the menu appears.
2 Touch **Reset**.
3 The device reboots.

Performing a Hard Reset

Note: All un-saved data is lost after performing a Hard Reset.

Perform a Hard Reset if the device stops responding. To perform a Hard Reset:

Procedure:

1 Simultaneously press the Power button, 1 and 9 keys.

2 The device reboots.

Performing an Enterprise Reset

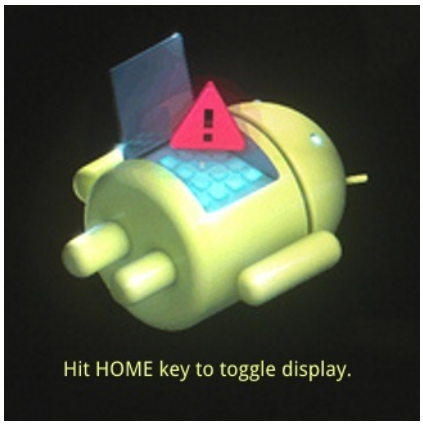
An Enterprise Reset erases all data in the `/cache` and `/data` partitions and clears all device settings, except those in the `/enterprise` partition.

Before performing an Enterprise Reset, copy all applications and the key remap configuration file that you want to persist after the reset into the `/enterprise/usr/persist` folder.

Procedure:

1 Download the Enterprise Reset file from the Zebra web site, http://www.zebra.com/support.
2 Copy the `M32N0JXXRExxxxxxx.zip` file to the root directory of the microSD card. See *USB Communication on page 55*.
3 Press and hold the Power button until the menu appears.
4 Touch **Reset**.
5 On the MC32N0–G device, press and hold the Trigger button or on the MC32N0–R/S devices, press and hold the Right Scan button..
6 When the Recovery Mode screen appears, release the button.

Figure 14: Recovery Mode Screen



7 Press ⌂. The System Recovery screen appears.

Figure 15: System Recovery Screen

8 Use the navigation keys to navigate to the **apply update from sdcard** option.
9 Press Enter.

10 Use the navigation keys to navigate to the `M32N0JXXRExxxxx.zip` file.

11 Press Enter. The Enterprise Reset occurs and then the device resets.

Performing a Factory Reset

A Factory Reset erases all data in the /cache, /data and /enterprise partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See *Updating the MC32N0 System on page 121* for more information.

Procedure:

1 Download the Factory Reset file from the Zebra web site, http://www.zebra.com/support.

2 Copy the `M32N0JXXRFxxxxxxx.zip` file to the root directory of the microSD card. See *USB Communication on page 55*.

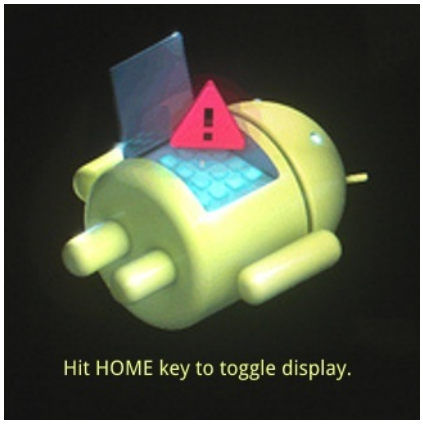
3 Press and hold the Power button until the menu appears.

4 Touch **Reset**.

5 On the MC32N0–G device, press and hold the Trigger button or on the MC32N0–R/S devices, press and hold the Right Scan button..

6 When the Recovery Mode screen appears release the button.

Figure 16: Recovery Mode Screen



7 Press ⌂.

Figure 17: System Recovery Screen

8 Use the navigation keys to navigate to the **apply update from sdcard** option.

9 Press Enter.

10 Use the navigation keys to navigate to the `M32N0JXXRFxxxxxxx.zip` file.

11 Press the Enter. The Factory Reset occurs and then the device resets.

Resetting the WinCE Device

If the MC32N0 stops responding to input, reset it. There are two reset functions, warm boot and cold boot. A warm boot restarts the MC32N0 by closing all running programs. All data that is not saved is lost.

A cold boot also restarts the MC32N0, but erases all stored records and entries from RAM. In addition it returns formats, preferences and other settings to the factory default settings.

Perform a warm boot first. If the MC32N0 still does not respond, perform a cold boot.

Performing a Warm Boot

Procedure:

1 Press the Power button for five seconds.

Caution: Files that remain open during a warm boot may not be retained.

2 As soon as the MC32N0 starts to boot release the Power button.

Figure 18: Splash Screen (Warm Boot)

Performing a Cold Boot

A cold boot restarts the mobile computer and erases all user stored records and entries from RAM. Never perform a cold boot unless a warm boot does not solve the problem.

Note:

Cold boot resets the mobile computer, to the default settings. All added applications and all stored data are removed. Do not cold boot without administrator approval.

Note:

The Real-time clock (RTC) default time is set to 1/1/2013 12:00 AM and is retained after a cold boot. After boot up, the MC32N0 saves the system time in persistent storage (Application folder) every 60 minutes.

If the RTC time resets to the default value due to power lost, the MC32N0 restores the time from the file in persistence storage (Application folder). The RTC file is deleted during OSUpdate procedure.

Procedure:

1 Simultaneously press and then release the 1, 9 and Power keys. Do not hold down any other keys or buttons. As the mobile computer initializes, the splash window appears.

Figure 19: Splash Screen (Cold Boot)

2 Calibrate the touch screen.

Chapter 2

Accessories

This chapter provides information for using the accessories for the device.

MC32N0 Accessories

The table below lists the accessories available for the MC32N0.

Table 2: MC32N0 Accessories

Accessory	Part Number	Description
Cradles		
Single Slot Serial /USB Cradle	CRD3000-1001RR	Charges the MC32N0 main battery and a spare battery, and synchronizes the MC32N0 with a host computer through either a serial or USB connection.
Four Slot Ethernet Cradle	CRD3X01-4001ER	Charges up to four MC32N0s and provides Ethernet communications.
Four Slot Charge Only Cradle	CHS3000-4001CR	Charges up to four MC32N0s.
Chargers		
Four Slot Spare Battery Charger	SAC7X00-4000CR	Charges up to four MC32N0 spare batteries.
Battery Adapter	ADP-MC32–CUP0-01	Allows for charging of MC32N0 batteries in the Four Slot Spare Battery Charger, Single Slot USB cradle and UBC Adapter (Single-pack).
	ADP-MC32–CUP0-04	(4–pack).
Universal Battery Charger (UBC) Base	UBC2000-I500DES	Charges up to four MC32N0 spare batteries. Requires UBC Adapter and Battery Adapter.
MC3XXX Universal Battery Charger (UBC) Adapter	21-32665-45AR	Charges a single MC32N0 battery. Requires Battery Adapter. Use in conjunction with the UBC Base to charge multiple batteries.
Power Supply for Single Slot Serial/USB Cradle	PWRS-14000–148R	Provides power to the Single Slot Serial/USB cradle.
Power Supply for Four Slot Cradles	PWRS-14000-241R	Provides power to the Four Slot Charge Only and Ethernet cradles.
Power Supply for Four Slot battery Charger	PWRS-14000–242R	Provides power to the Four Slot Spare Battery Charger.

Table continued…

Accessory	Part Number	Description
Power Supply for Charging Cables	PWRS-14000-249R	Provides power to the Charge Only cable, RS232 Charge cable and USB Client Charge cable.
US AC Line Cord	23844-00-00R	Provides power to 3–wire power supplies PWRS-14000–148R and PWRS-14000–241R.
International AC Line Cord	50–16000–271R 50–16000–218R 50–16000–219R 50–16000–220R 50–16000–221R 50–16000–256R 50–16000–257R 50–16000–669R 50–16000–671R 50–16000–672R 50–16000–678R 50–16000–727R	Provides power to 3–wire power supplies PWRS-14000–148R and PWRS-14000–241R.
US AC Line Cord	50-16000-182R	Provides power to the 2-wire power supply PWRS-14000–249R.
International AC Line Cord	50–16000–255R 50–16000–664R 50–16000–666R 50–16000–670R	Provides power to the 2-wire power supply PWRS-14000–249R.
DC Line Cord	50–16002–029R	Provides power from power supply to the Four Slot Charge Only cradle and Four Slot Ethernet cradle.
Cables		
Charge Only Cable	25-70103-03R	Provides power to the MC32N0. Requires power supply PWRS-14000–249R.
USB Client Charge Cable	25-67868-03R	Provides USB client communication capabilities and charges the MC32N0.
RS232 Charge Cable	25-67866-03R	Provides RS232 communication capabilities and charges the MC32N0.
Vehicle Charge Cable	VCA3000–01R	Changes the MC32N0 using a vehicle's cigarette lighter.
Zebra Printer Cable	25-91513-01R	Provides printer specific communication capabilities.
Single Slot Cradle RS232 Cable	25-63852-01R	Provides serial host communication through the Single Slot Serial/USB cradle.

Table continued…

Accessory	Part Number	Description
Single Slot Cradle USB Cable	25-68596-01R	Provides USB communication through the Single Slot Serial/USB cradle.
Headset Adapter Cable	25-124411-02R	Connects an RCH51 headset to the MC32N0. Contains 2.5 mm jack with unique locking screw.
Miscellaneous		
Magnetic Stripe Reader	MSR3000–100R	Reads magnetic stripe cards.
Cradle Modem Kit	KT-MC3000SERMO-DEMR	Provides modem connectivity to the Single Slot Serial/USB cradle. Kit includes Modem Dongle and Modem Adapter Cable. **Note:** Not supported on Android devices.
2740 mAh Battery	BTRY-MC32–01–01	Replacement standard capacity (1X) battery.
	BTRY-MC32–01–10	Replacement standard capacity (1X) battery (10–pack).
4800 mAh Battery	BTRY-MC32–02–01	Replacement extended capacity (2X) battery.
	BTRY-MC32–02–10	Replacement extended capacity (2X) battery (10–pack).
Replacement Tether	KT-73440–01R	Replacement non-elastic tether for MC32N0–R and MC32N0–S (3–pack).
MC32XX-R/S Stylus and Tether Kit	11-43912-03R	Replacement stylus and tether kit (3-pack).
MC32N0–G Stylus and Tether	KT-81680–03R	Replacement stylus and tether for MC32N0–G (3-pack).
	KT-81680-50R	Replacement stylus and tether for MC32N0–G (50-pack).
MC32N0-G Handstrap Button	KT-97258-01R	Replacement button for MC32N0-G handstrap (250-pack).
MC32N0-G Handstrap	SG-MC3123242-01R	Replacement handstrap for MC32N0-G.
MC32N0-G Handstrap	SG-MC3123342-01R	Replacement handstrap for MC32N0-G (5–pack).
MC32N0-R/S Handstrap	SG-MC3123243-01R	Replacement handstrap for MC32N0-R and MC32N0-S.
Plastic Holster	8710-050005-01R	Provides a clip on holder for the MC32N0-R and MC32N0- S.
Fabric Holster	11–69293–01R	Provides a soft, clip on holder and a shoulder strap for the MC32N0-R and MC32N0- S
Fabric Holster	SG-MC3021212–01R	Provides a soft, clip on holder and a shoulder strap for the MC32N0–G.
Shoulder Strap	58–40000–007R	Universal shoulder strap.
Belt	11-08062-02R	Belt for fabric holster.

Table continued…

Accessory	Part Number	Description
MC32N0–G Rubber Boot	11-72959-04R	Provides additional protection for both the MC32N0–G laser and imager configurations.
MC32N0-S Rubber Boot	11-70899-04R	Provides additional protection for both the MC32N0–S laser and imager configurations.
MC32N0–R Rubber Boot	11–72096–04R	Provides additional protection for the MC32N0–R.
MC32 Rubber Boot for Turret Cup	11–72097–04R	Provides additional protection for the MC32N0–R (turret cup).
Mounting Bracket	KT-136648–01	Used to mount four slot cradles onto a wall.

Battery Adapter

Use the Battery Adapter with the Single Slot Serial/USB Cradle and the Four Slot Battery Charger to allow charging of the MC32N0 batteries.

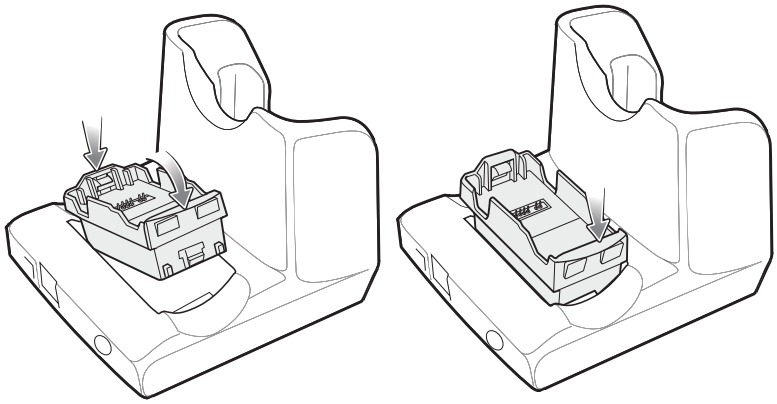
Installing the Battery Adapter

When and where to use: The Battery Adapter is required to charge MC32N0 batteries in the Single Slot Serial/USB cradle, the Four Slot Battery Charger or the UBC Adapter.

Procedure:

1 Remove power from the cradle or charger.
2 Insert the end of the Battery Adapter into the battery slot.
3 Rotate the Battery Adapter down into the battery slot.

Figure 20: Battery Adapter in Single Slot Serial/USB Cradle



Note:

On the Four Slot Battery Charger, install the Battery Adapter into the two front slots before installing into the two rear slots.

If charing both MC3200 and MC3100 batteries in the charger, install the MC3200 battery adapter in the back slots and install the MC3100 batteries in the front slots.

Figure 21: Battery Adapter in Four Slot Battery Charger

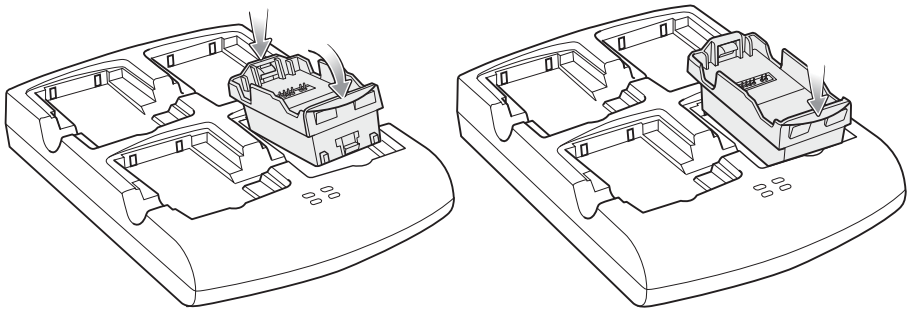
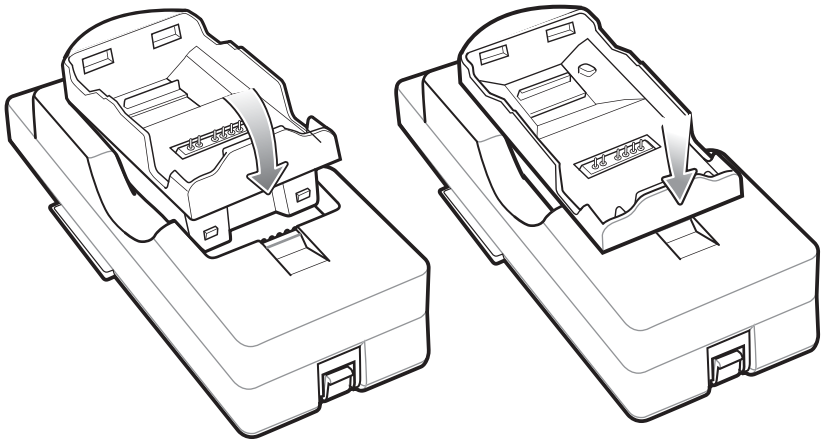


Figure 22: Battery Adapter in UBC Adapter



4 Press the Battery Adapter down to ensure that it is properly seated.

5 Reconnect power.

Removing the Battery Adapter

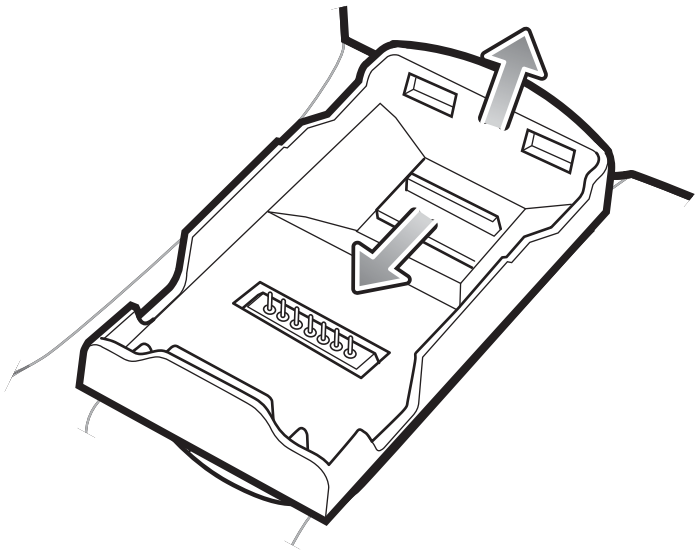
Procedure:

1 Remove power from the cradle or charger.

2 Remove the battery from Battery Adapter.

3 Slide the release latch toward the contact pins.

Figure 23: Release Latch



4 Rotate the Battery Adapter up.
5 Remove the Battery Adapter from the battery slot.
6 Reconnect power.

Single Slot Serial/USB Cradle

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

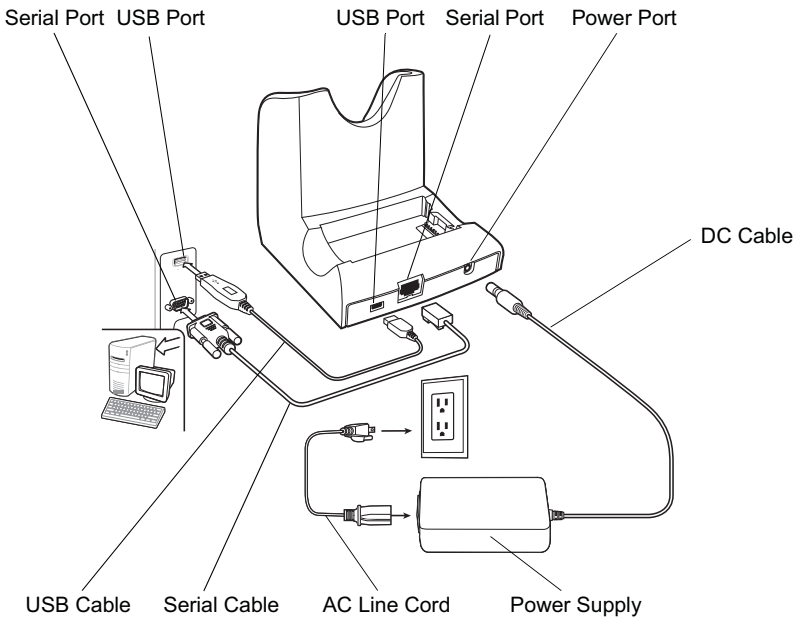
The Single Slot Serial/USB cradle:

- Provides 5.4VDC power for operating the mobile computer, charging the battery and charging a spare battery.
- Provides a serial port and a USB port for data communication between the mobile computer and a host computer or other serial devices (e.g., a printer).
- Synchronizes information between the mobile computer and a host computer. With customized or third party software, it can also synchronize the mobile computer with corporate databases.
- Provides serial connection through the serial pass-through port for communication with a serial device, such as a host computer.

- Provides USB connection through the USB pass-through port for communication with a USB device, such as a host computer.

Setup

Figure 24: Single Slot USB Cradle Power, Serial and USB Connections



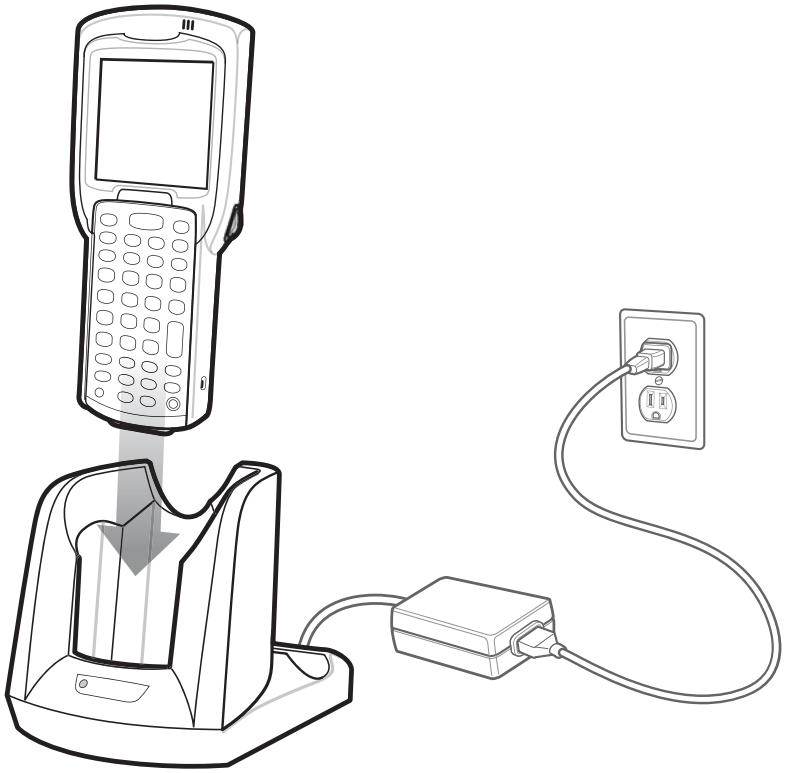
Charging the MC32N0 Battery

Procedure:

1 Ensure that the cradle is connected to power.

2 Slide the mobile computer into the slot in the cradle. The mobile computer amber Charge LED Indicator, indicates the mobile computer battery charging status.

Figure 25: MC32N0 Battery Charging



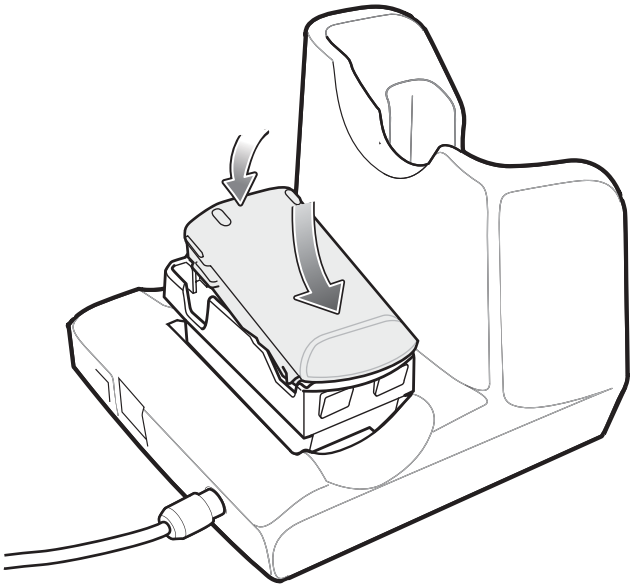
3 Gently press down on the device to ensure proper contact.
4 When charging is complete, remove the mobile computer from the cradle slot.

Charging an MC32N0 Spare Battery

Procedure:

1 Ensure that the cradle is connected to power.
2 Ensure that the Battery Adapter into the spare battery slot on the cradle. See *Battery Adapter on page 32*.
3 Insert the spare battery into the battery adapter, bottom first, and pivot the top of the battery down onto the contact pins.

Figure 26: MC32N0 Spare Battery Charging



4 Gently press down on the battery to ensure proper contact.
The Spare Battery Charging LED on the front of the cradle indicates the spare battery charging status.
5 When charging is complete, press the battery clip and lift the battery out of the slot.

Battery Charging in Single Slot Serial/USB Cradle

The Single Slot Serial/USB cradle charges the M32N0's main battery and a spare battery simultaneously.

The MC32N0's Charge LED indicates the status of the battery charging in the MC32N0. See *Table 1: LED Charge Indicators on page 23* for charging status indications.

The spare battery charging LED on the cradle indicates the status of the spare battery charging in the cradle. See below for charging status indications.

Table 3: Spare Battery LED Charging Indicators

Spare Battery LED (on cradle)	Indication
Slow Blinking Amber	Spare battery is charging.
Solid Amber	Charging complete.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Off	No spare battery in slot; spare battery not placed correctly; cradle is not powered.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC32N0.

To accomplish this, for small periods of time, the MC32N0 or cradle alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC32N0 or cradle indicates when charging is disabled due to abnormal temperatures via its LED.

Four Slot Charge Only Cradle

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

The Four Slot Charge Only cradle:

- Provides 5.4 VDC power for operating the mobile computer and charging the battery.
- Simultaneously charges up to four mobile computers.

Figure 27: Four Slot Charge Only Cradle

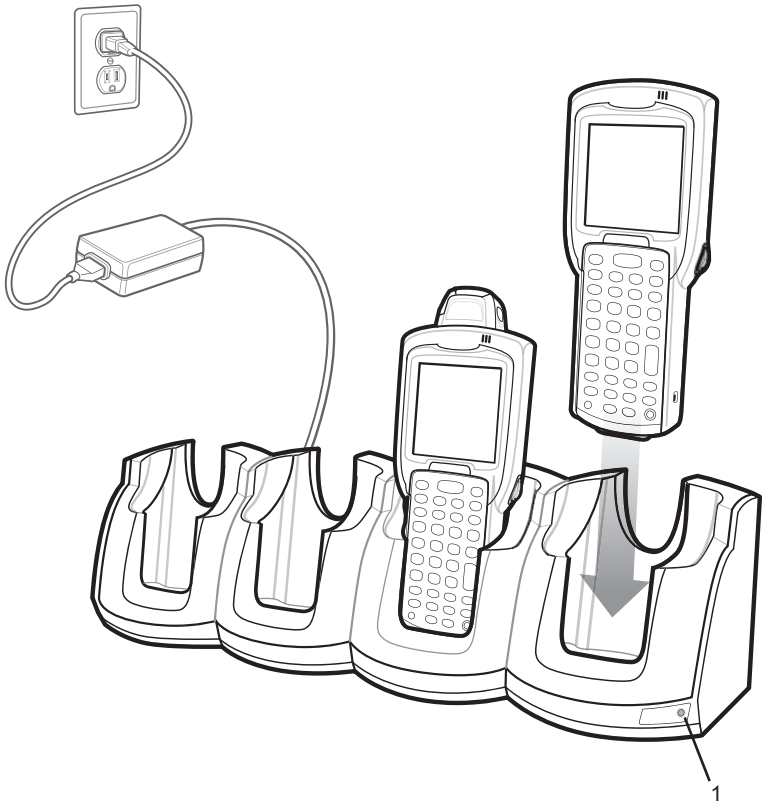


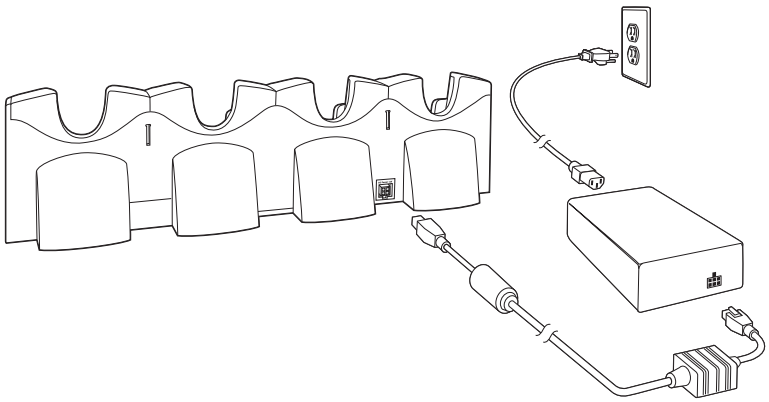
Table 4: Four Slot Charge Only Cradle LED

Item	Description
1	Power LED

Setup

Connect the Four Slot Charge Only cradle to a power source.

Figure 28: Four Slot Charge Only Cradle Setup



Charging the MC32N0 Battery

Procedure:

1. Ensure that the cradle is connected to power.
2. Slide the mobile computer into the slot in the cradle. The mobile computer amber Charge LED Indicator, indicates the mobile computer battery charging status.
3. Gently press down on the device to ensure proper contact.
4. When charging is complete, remove the mobile computer from the cradle slot.

Battery Charging in the Four Slot Charge Only Cradle

The MC32N0's Charge LED indicates the status of the battery charging in the MC32N0. See *Table 1: LED Charge Indicators on page 23* for charging status indications.

The Standard Battery charges in less than five hours and the Extended Battery charges in less than eight hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC32N0.

To accomplish this, for small periods of time, the MC32N0 or cradle alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC32N0 or cradle indicates when charging is disabled due to abnormal temperatures via its LED.

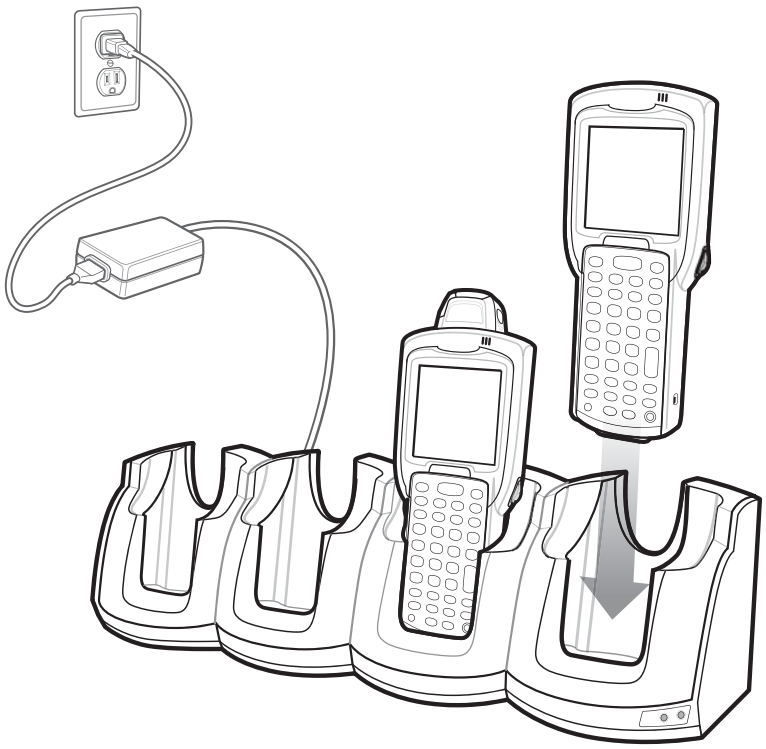
Four Slot Ethernet Cradle

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

The Four Slot Ethernet cradle:

- Provides 5.4 VDC power for operating the mobile computer.
- Connects the mobile computer (up to four) to an Ethernet network.

Figure 29: Four Slot Ethernet Cradle



LED Indicators

There are two green LEDs on the front of the cradle and two green LED on the Primary port on the back of the cradle. These green LEDs light and blink to indicate the data transfer rate. When the LEDs are not lit the transfer rate is 10 Mbps.

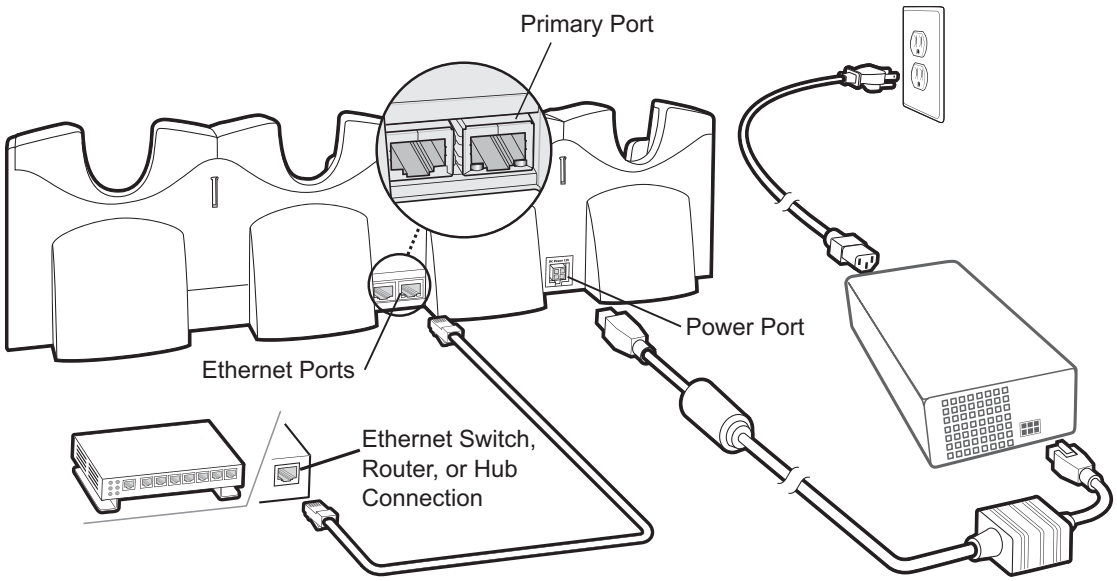
Table 5: CRD3X01-4001ER LED Indicators

Data Rate	Left 1000 LED	Right 100 LED
1 Gbps	On/Blink	Off
100 Mbps	Off	On/Blink
10 Mbps	Off	Off

CRD3X01-4001ER Setup

Connect the Four Slot Ethernet cradle to a power source and to an Ethernet switch, router, or hub, or a port on the host device.

Figure 30: CRD3X01-4001ER Four Slot Ethernet Cradle Connection



Daisychaining Ethernet Cradles

Daisychain up to four Four Slot Ethernet cradles to connect several cradles to an Ethernet network. Use either a straight or crossover cable. Daisy-chaining should not be attempted when the main Ethernet connection to the first cradle is 10 Mbps as throughput issues will almost certainly result.

To daisychain more than Four Slot Ethernet cradles:

Procedure:

1 Connect power to each Four Slot Ethernet cradle.

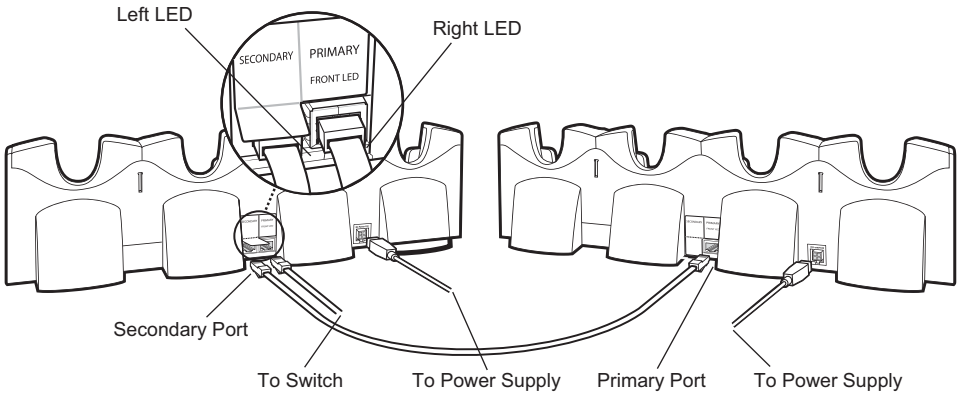
2 Connect an Ethernet cable to the Primary Port of the first cradle and to the Ethernet switch.

3 On the first Four Slot Ethernet cradle, lift or remove the label flap and connect a second Ethernet cable to the Secondary Port.

4 Connect the other end of the Ethernet cable to the Primary Port of the second Four Slot Ethernet cradle.

5 Connect additional cradles as described in *step 3* and *step 4*.

Figure 31: Daisychaining Four Slot Ethernet Cradles



Ethernet Settings on Android Devices

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The MC32N0 includes Ethernet cradle drivers. After inserting the MC32N0, configure the Ethernet connection:

Procedure:

1 Touch .

2 Touch .

3 Touch **Ethernet**.

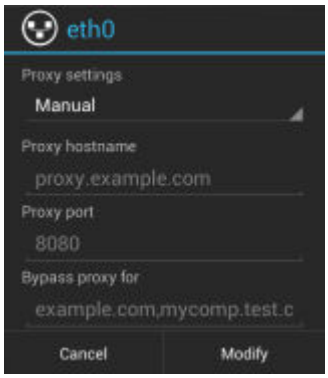
4 Slide the switch to the **ON** position.

5 Place the MC32N0 into the Ethernet cradle slot.

6 Touch and hold **Eth0** until the menu appears.

7 Touch **Modify Proxy**.

Figure 32: Ethernet Proxy Settings



8 Touch the **Proxy settings** drop-down list and select **Manual**.

9 In the **Proxy hostname** field, enter the proxy server address.

10 In the **Proxy port** field, enter the proxy server port number.

11 **Note:** When entering proxy addresses in the **Bypass proxy for** field, do not use spaces or carriage returns between addresses.

In the **Bypass proxy for** text box, enter addresses for web sites that do not require to go through the proxy server. Use the separator "|" between addresses.

12 Touch **Modify**.

13 Touch .

Configuring Ethernet Static IP Address

The MC32N0 includes Ethernet cradle drivers. After inserting the MC32N0, configure the Ethernet connection:

Procedure:

1 Touch .

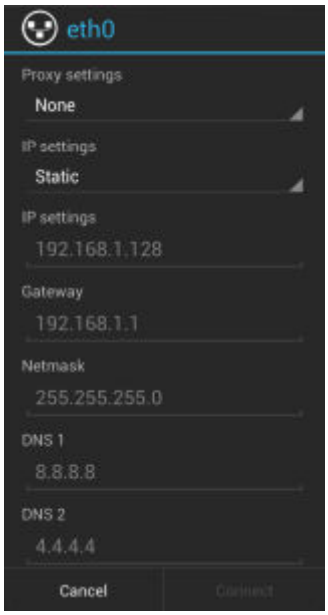
2 Touch .

3 Touch **Ethernet**.

4 Slide the switch to the **ON** position.

5 Place the MC32N0 into the Ethernet cradle slot.
6 Touch and hold **Eth0** until the menu appears.
7 Touch **Disconnect**.

Figure 33: Ethernet Proxy Settings



8 Touch and hold **Eth0** until the menu appears.
9 Touch the **IP setting** drop-down list and select **Static**.
10 In the **IP adress** field, enter the proxy server address.
11 If required, in the **Gateway** text box, enter a gateway address for the device.
12 If required, in the **Network prefix length** text box, enter a the prefix length.
13 If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
14 If required, in the **DNS 2** text box, enter a DNS address.
15 Touch **Connect**.
16 Touch .

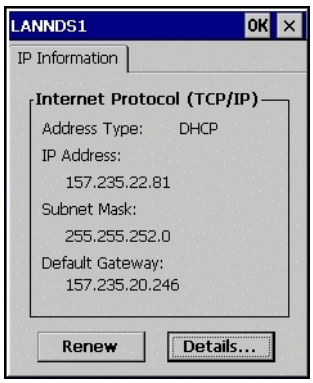
Ethernet Settings on WinCE Devices

The Ethernet cradle drivers are pre-installed on the MC32N0 and initiate automatically when the MC32N0 is placed in a properly connected Four Slot Ethernet cradle.

When the mobile computer is inserted into the Four Slot Ethernet cradle, the LAN icon indicates that the mobile computer is connected to a network.

Double-tap the LAN icon to open the LANNDS1 window. This window display the TCP/IP information for the mobile computer.

Figure 34: LANNDS1 Window



Charging the MC32N0 Battery

Procedure:

1. Ensure that the cradle is connected to power.
2. Slide the mobile computer into the slot in the cradle. The mobile computer amber Charge LED Indicator, indicates the mobile computer battery charging status.
3. Gently press down on the device to ensure proper contact.
4. When charging is complete, remove the mobile computer from the cradle slot.

Battery Charging in the Four Slot Ethernet Cradle

The MC32N0's Charge LED indicates the status of the battery charging in the MC32N0. See *Table 1: LED Charge Indicators on page 23* for charging status indications.

The Standard Battery charges in less than five hours and the Extended Life Battery charges in less than eight hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC32N0.

To accomplish this, for small periods of time, the MC32N0 or cradle alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC32N0 or cradle indicates when charging is disabled due to abnormal temperatures via its LED.

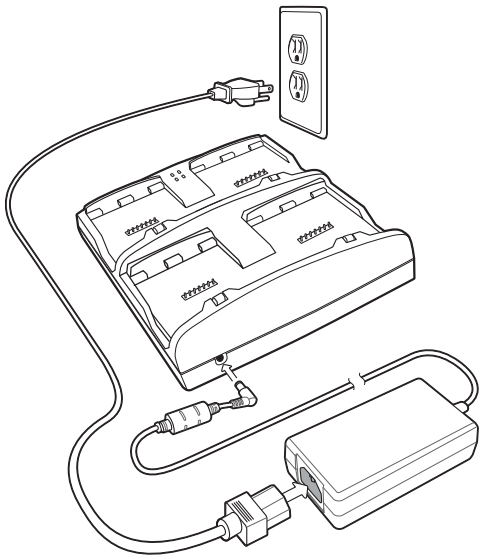
Four Slot Spare Battery Charger

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

The Four Slot Battery Charger charges up to four MC32N0 spare batteries.

Setup

Figure 35: Four Slot Battery Charger Power Setup



Charging Spare Batteries

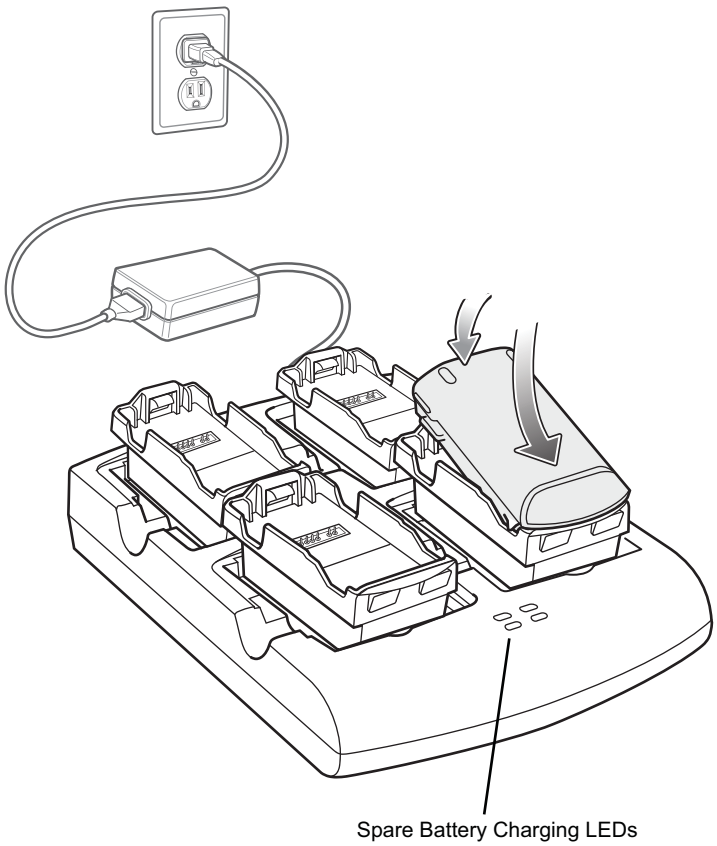
Prerequisites: Before installing the battery, install the Battery Adapter into the battery slot in the Four Slot Spare Battery Charger. See *Battery Adapter on page 32*.

Procedure:

1 Connect the charger to a power source.

2 Insert the battery into a battery adapter and gently press down on the battery to ensure proper contact.

Figure 36: Four Slot Battery Charger



Battery Charging

Spare Battery Charging

Each Battery Charging LED indicates the status of the battery charging in each slot. The table below describes the Battery Charging LED status.

The Standard battery charges in less than five hours and the Extended battery fully charges in less than eight hours.

Table 6: Battery LED Charging Indicators

LED	Indication
Off	No battery in slot. Battery is not charging. Battery Adapter is not inserted correctly in the slot. Battery is not inserted correctly in Battery Adapter. Charger is not powered.
Slow blinking amber	Battery is charging.
Solid amber	Charging complete.
Fast blinking amber	Charging error.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC32N0.

To accomplish this, for small periods of time, the changer alternately enables and disables battery charging to keep the battery at acceptable temperatures. The charger indicates when charging is disabled due to abnormal temperatures via its LED.

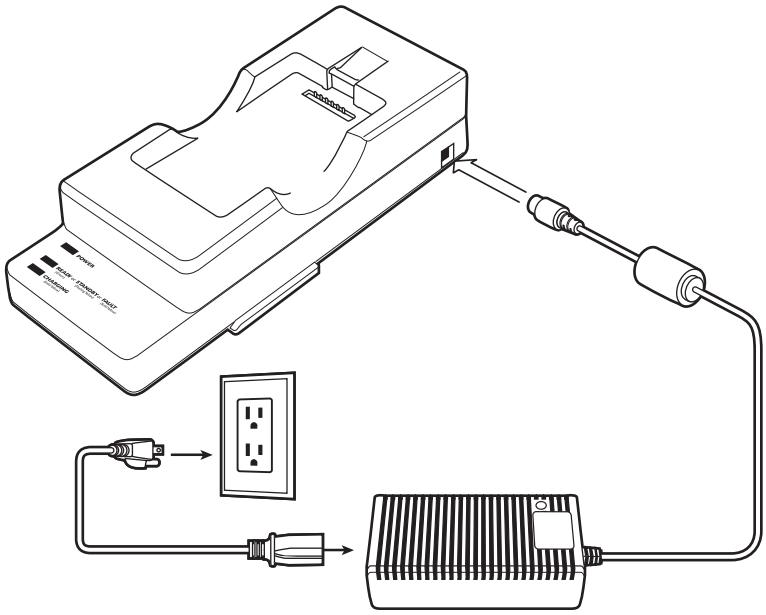
Universal Battery Charger Adapter

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 159*.

The Universal Battery Charger (UBC) Adapter can be used with a power supply as a standalone spare battery charger or it can be used with the four station UBC2000 to simultaneously charge up to four spare batteries. For additional information on the UBC 2000, see the *UBC 2000 Quick Reference Guide* p/n 70-33188-xx.

Setup

Figure 37: Universal Battery Charger Setup



Charging a Spare Battery in the UBC Adapter

Prerequisites:

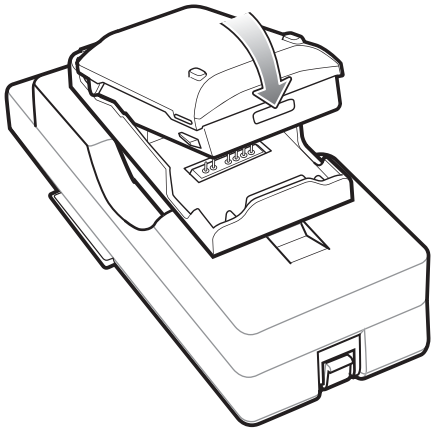
Before installing the battery, ensure that the Battery Adapter has been installed into the battery slot in the Universal Battery Charger Adapter. See *Battery Adapter on page 32*.

Ensure that the adapter is connected to power source.

Procedure:

1 Insert the battery into a battery adapter and gently press down on the battery to ensure proper contact.

Figure 38: Universal Battery Charger Adapter



2 Press down on the battery to ensure it is seated properly.

UBC Adapter Battery Charging

Spare Battery Charging

The UBC Adapter charging LEDs indicate the battery charging status. The Standard Battery usually charges in less than five hours and the Extended Life Battery usually charges in less than eight hours.

Figure 39: UBC Adapter LEDs

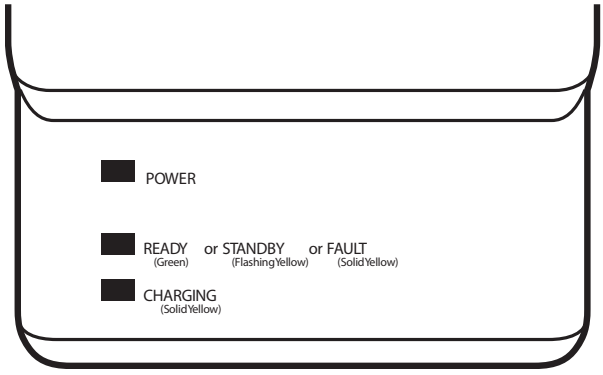


Table 7: UBC Adapter Charge LED Status Indications

LED	Indication	Description
POWER	Green	Power is connected to the UBC Adapter.
READY or	Green	Charging complete.
STAND-BY or	Flashing-Yellow	The battery was deeply discharged and is being trickle charged to bring the voltage up to the operating level. After operating level voltage is achieved, the battery charges normally.
FAULT	Yellow	Charging error, check placement of mobile computer/spare battery.
CHARG-ING	Yellow	Normal charge.

Wall Mount Bracket

Use the optional Wall Mount Bracket to mount a four slot cradle to a wall. To attach the Wall Mount Bracket:

Procedure:

1 Use the Wall Mount Bracket as a template and mark the locations of the four mounting screws.

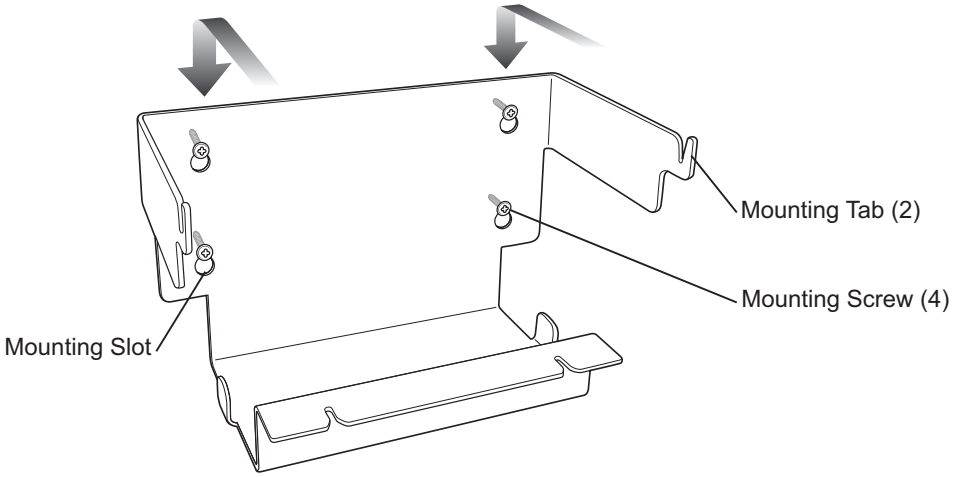
Note: Use fasteners appropriate for the type of wall and the Wall Mount Bracket mounting slots. The Wall Mount Bracket mounting slots are designed for a fastener with a #8 pan head. Fasteners must be able to hold a minimum of 4.9 Kg (10.8 lbs).

2 Mount the fasteners to the wall. The screw heads should protrude about a half of an inch from the wall.

3 Slip the Wall Mount Bracket over the screw heads and slide the bracket down over the screw heads.

4 Tighten the screws to secure the bracket to the wall.

Figure 40: Wall Mount Bracket



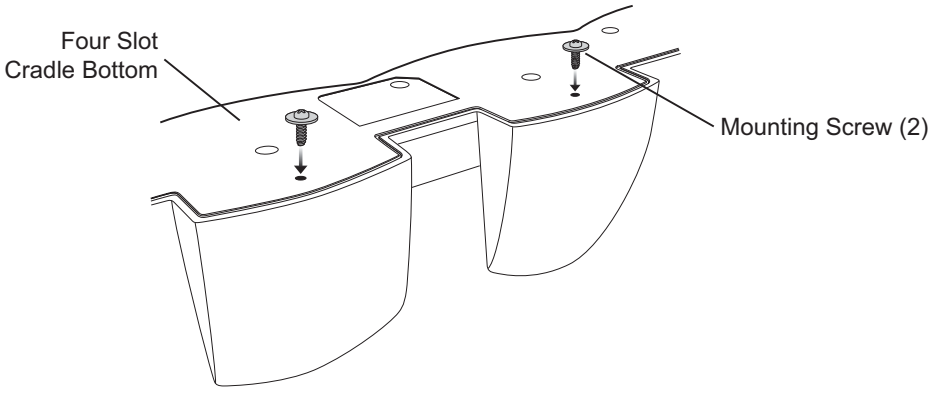
Mounting a Four Slot Cradle

To mount a four slot cradle:

Procedure:

1 Screw the supplied screws into the bottom of the four slot cradle. The screw heads should protrude about a quarter of an inch from the cradle.

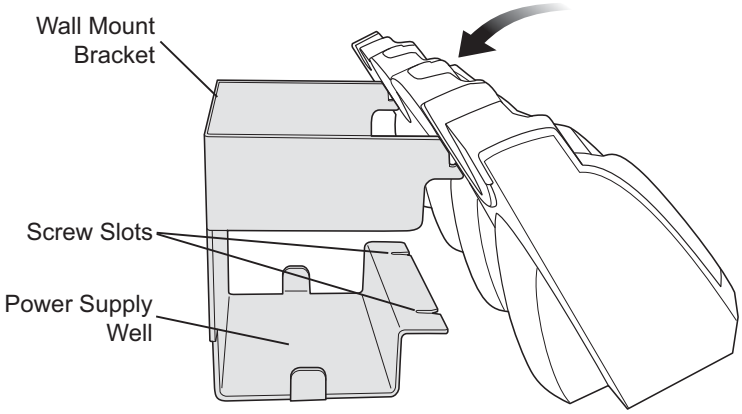
Figure 41: Cradle Mounting Screws



2 Align the Wall Mount Bracket mounting tabs with the mounting slots in the back of the four slot cradle. Slip the two mounting tabs into mounting slots.

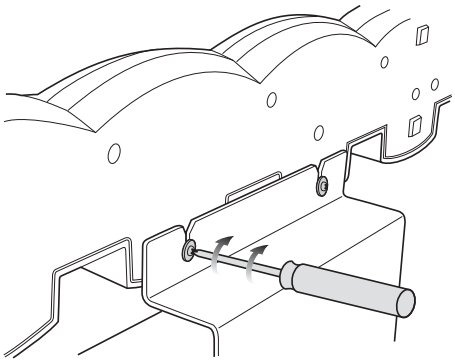
3 Swing the four slot cradle down onto the mounting bracket and align the mounting screws so that they fit into the screw slots.

Figure 42: Wall Mount Bracket



4 Tighten the mounting screws to secure the four slot cradle to the bracket.

Figure 43: Mounting Screws



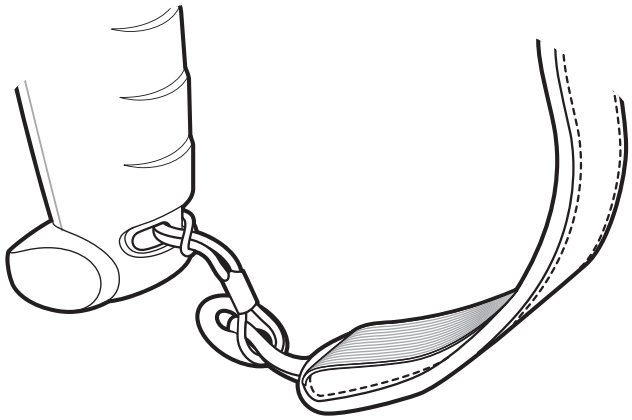
5 Connect power. The power supply should be located in the power supply well.

MC32N0–G Handstrap Replacement

Procedure:

1 Slip the button through the loop.

Figure 44: Remove Button from Loop



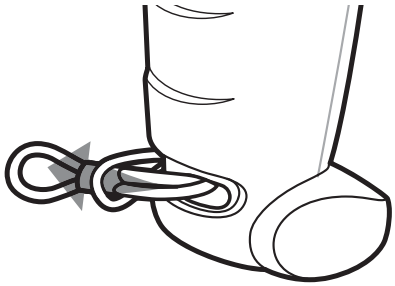
2 Remove loop section from handle.

3 Separate the loop and hook tape and pull the handstrap through the slot at the bottom of the device.

4 Insert one end of the new loop section into the mounting slot in the handle.

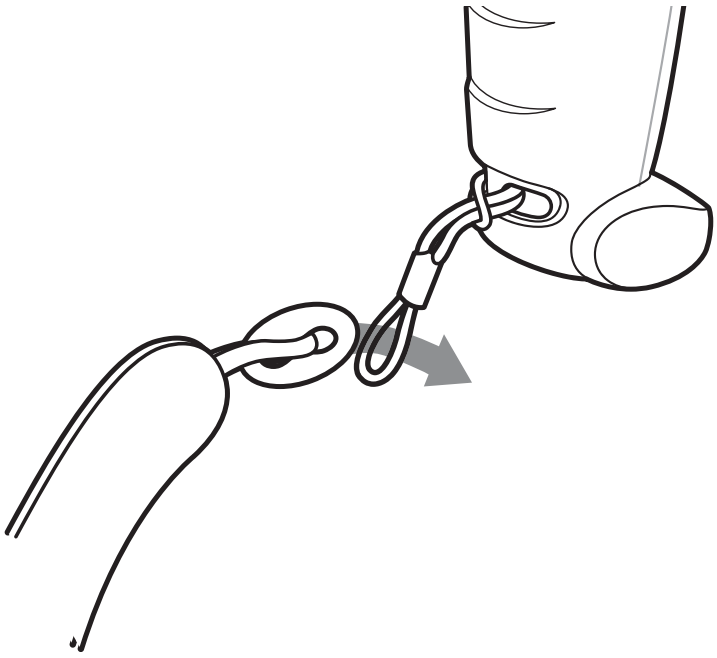
5 Thread the other end of the loop section through the loop and pull to tighten the loop.

Figure 45: Thread Loop



6 Slip the button into the loop section.

Figure 46: Slip Button Through Loop



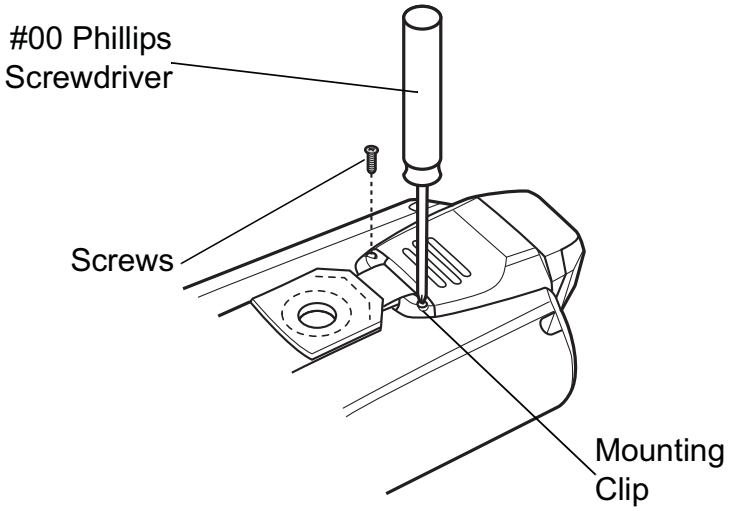
7 Thread the end of the handstrap into the slot at the bottom of the device.
8 Press the hook material against the loop material.

MC32N0–S/R Handstrap Replacement

Procedure:

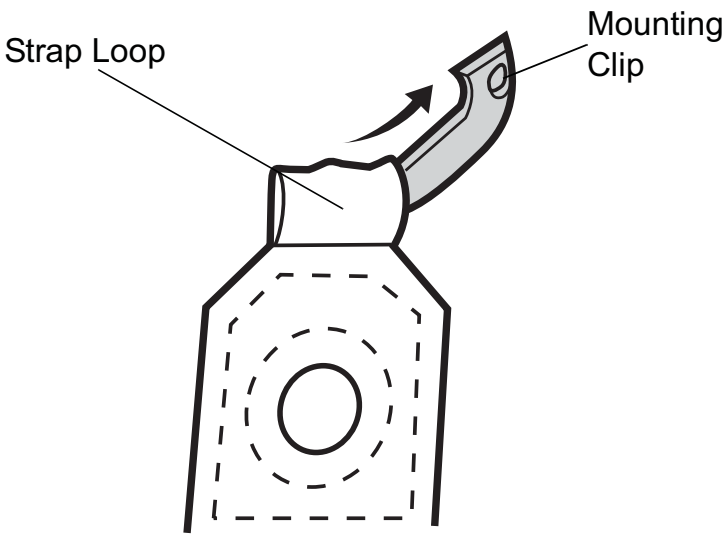
1 Use a #00 Phillips screwdriver to remove two screws.

Figure 47: Remove Mounting Clip



2 Lift the mounting clip.
3 Slide the mounting clip out of the strap loop.

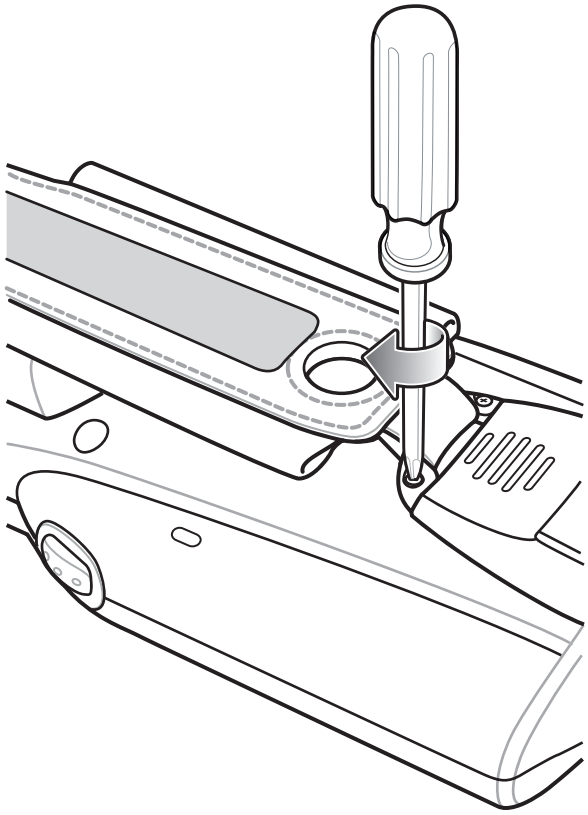
Figure 48: Remove Mounting Clip



4 Feed the mounting clip through the new strap loop.

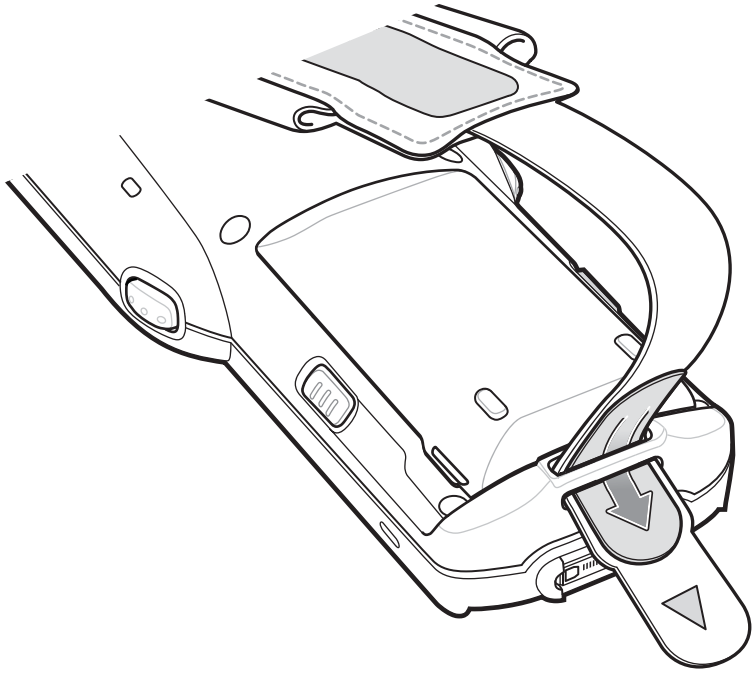
5 Secure the mounting clip to the housing using the two screws.

Figure 49: Secure Mounting Clip



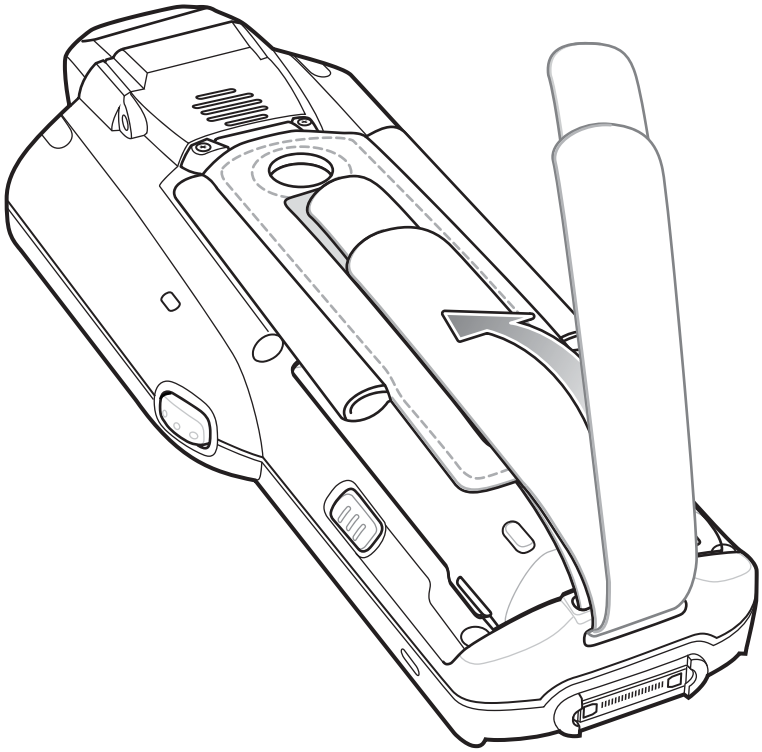
6 Feed the handstrap through the slot at the bottom of the device.

Figure 50: Feed Handstrap Through Slot



7 Attach the hook material to the loop material and press together.

Figure 51: Secure Handstrap



Chapter 3

USB Communication

Note: This chapter applies to Android devices only.

This chapter provides information for transferring files between the device and a host computer.

Connecting to a Host Computer via USB

Connect the MC32N0 to a host computer using the Single Slot Serial/USB cradle or USB Client Charge cable to transfer files between the MC32N0 and the host computer.

Caution:

When connecting the MC32N0 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Connecting to the MC32N0 as a Media Device

Note: Using Media Device, you can copy files to either the microUSB card or internal memory.

Procedure:

1. Connect the USB Client Charge cable to the MC32N0 and then to the host computer or place the MC32N0 into a Single Slot Serial/USB cradle that is connected to a host computer.
   Connected as a media device or **Connected as an installer** appears on the Status bar.
2. If **Connected as an installer** appears, pull down the Notification shade and touch **Connected as an installer** and then touch **Media device (MTP)**.
3. On the host computer, open a file explorer application.
4. Locate the **MC32N0** as a portable device.
5. Open the **SD card** or the **Internal storage** folder.
6. Copy or delete files as required.

Connecting to the MC32N0 as an Installer

Note: Using Installer, you can only copy files to the microUSB card.

Procedure:

1. Connect the USB Client Charge cable to the MC32N0 and then to the host computer or place the MC32N0 into a Single Slot Serial/USB cradle that is connected to a host computer.
   Connected as a media device or **Connected as an installer** appears on the Status bar.

2 If **Connected as media device** appears, pull down the Notification shade and touch **Connected as media device** and then touch **Media device (MTP)** to de-select.
3 Touch **Turn on USB Storage**.
4 On the host computer, open a file explorer application.
The MC32N0 storage appears as Removable Disk.
5 Locate the MC32N0 as a devices within Removable Storage.
6 Open the **Removable Disk**.
7 Copy or delete files as required.
8 On the MC32N0, touch **Turn off USB storage**

Disconnect from the Host Computer

Caution:

Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.

Procedure:

1 On the host computer, unmount the device.
2 Remove the USB Client Charge cable from the MC32N0 or remove the MC32N0 from the Single Slot Serial/USB cradle.

Chapter 4

DataWedge Configuration

Note: This chapter applies to DataWedge on Android devices.

DataWedge is an application that reads data, processes the data and sends the data to an application.

Basic Scanning

Scanning can be performed using the imager.

Using the Imager

To capture bar code data:

Procedure:

1 Ensure that an application is open on the MC32N0 and a text field is in focus (text cursor in text field).
2 Aim the exit window at a bar code.
3 Press and hold the a Scan button or Trigger. The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern. The

Figure 52: Data Capture MC32N0-G

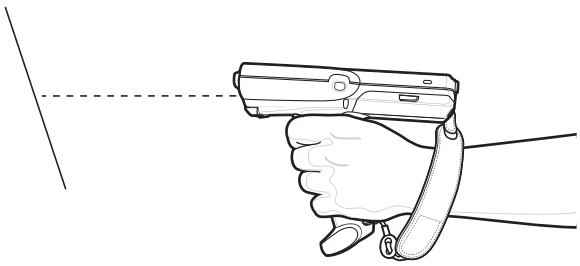
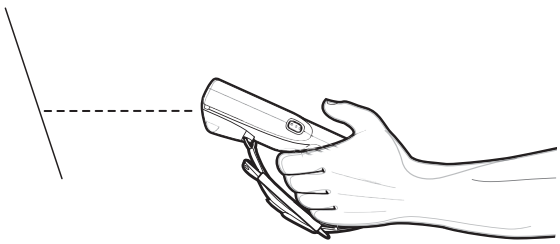


Figure 53: Data Capture – MC32N0–S



4 The Scan LEDs light green, a beep sounds, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

Using the Laser Scanner

To capture bar code data:

Procedure:

1 Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2 On the MC32N0–R, rotate the Turret for optimal scanning position.
3 Point the scan exit window at a bar code.
4 Press and hold the Scan button. The red scan line turns on to assist in aiming. Ensure that the scan line crosses every bar and space of the bar code.

Figure 54: Data Capture MC32N0–R

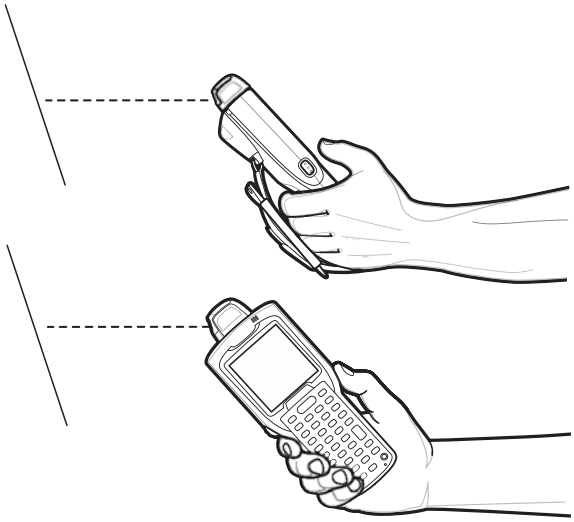
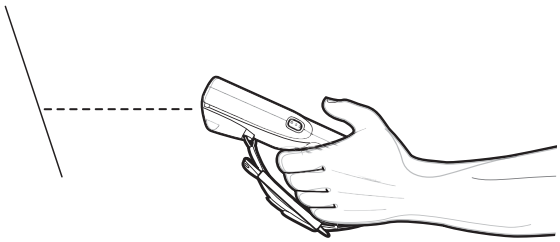


Figure 55: Data Capture MC32N0–S



The Scan LEDs light green and a beep sounds, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

Profiles

DataWedge is based on profiles and plug-ins. A profile contains information on how DataWedge should behave with different applications.

Profile information consists of:

- Associated application
- Input plug-in configurations
- Output plug-in configurations
- Process plug-in configurations.

Using profiles, each application can have a specific DataWedge configuration. For example, each user application can have a profile which outputs scanned data in the required format when that application comes to the foreground. DataWedge can be configured to process the same set of captured data differently based on the requirements of each application.

DataWedge includes the following visible and hidden pre-configured profiles which support specific built-in applications:

- Visible profiles:
  - **Profile0** - created automatically the first time DataWedge runs. Generic profile used when there are no user created profiles associated with an application.
  - **Launcher** - disables scanning when the Launcher is in foreground.
  - **DWDemo** - provides support for the DWDemo application.
- Hidden profiles (not shown to the device):
  - **RD Client** - provides support for MSP.
  - **MSP Agent** - provides support for MSP.
  - **MspUserAttribute** - provides support for MSP.
  - **Camera** - disables scanning when the default camera application is in foreground.
  - **RhoElements** - disables scanning when RhoElements is in foreground.

Profile0

Profile0 can be edited but cannot be associated with an application. That is, **DataWedge** allows manipulation of plug-in settings for **Profile0** but it does not allow assignment of a foreground application. This configuration allows **DataWedge** to send output data to any foreground application other than applications associated with user-defined profiles when **Profile0** is enabled.

Profile0 can be disabled to allow **DataWedge** to only send output data to those applications which are associated in user-defined profiles. For example, create a profile associating a specific application, disable **Profile0** and then scan. **DataWedge** only sends data to the application specified in the user-created profile. This adds additional security to **DataWedge** enabling the sending of data only to specified applications.

Plug-ins

A plug-in is a software module utilized in DataWedge to extend its functionality to encompass technologies such as bar code scanning. The plug-ins can be categorized into three types based on their operations:

- Input Plug-ins
- Output Plug-ins
- Process Plug-ins.

Input Plug-ins

An Input Plug-in supports an input device, such as a bar code scanner contained in, or attached to the device. **DataWedge** contains base plug-ins for these input devices.

- **Bar Code Scanner Input Plug-in** – The Bar Code Scanner Input Plug-in is responsible for reading data from the integrated bar code scanner and supports different types of bar code readers including laser, imager and internal camera. Raw data read from the bar code scanner can be processed or formatted using Process Plug-ins as

required. **DataWedge** has built-in feedback functionality for the bar code scanner to issue user alerts. The feedback settings can be configured according to user requirement.

Process Plug-ins

Process Plug-ins are used in **DataWedge** to manipulate the received data according to the requirement, before sending to the foreground application via the Output Plug-in.

- **Basic Data Formatting Process Plug-in** – The Basic Data Formatting Plug-in allows **DataWedge** to add a prefix and/or a suffix to the captured data before passing it to an Output Plug-in.
- **Advanced Data Formatting Process Plug-in** – The Advanced Data Formatting Plug-in allows **DataWedge** to apply rules (actions to be performed based on defined criteria) to the data received via an input plug-in before passing it to an Output Plug-in.

Output Plug-ins

Output Plug-ins are responsible for sending the data from Input Plug-ins to a foreground application on the device.

- **Keystroke Output Plug-in** – The Keystroke Output Plug-in collects and sends data received from the Input Plug-in to the foreground applications by emulating keystrokes.
- **Intent Output Plug-in** – The Intent Output Plug-in collects and sends data received from the Input Plug-ins to foreground applications using the Android Intent mechanism.
- **IP Output Plug-in** – The IP Output Plug-in collects and sends data received from the Input Plug-ins to a host computer via a network connection. Captured data can be sent over an IP network to a specified IP address and port using either TCP or UDP transport protocols.

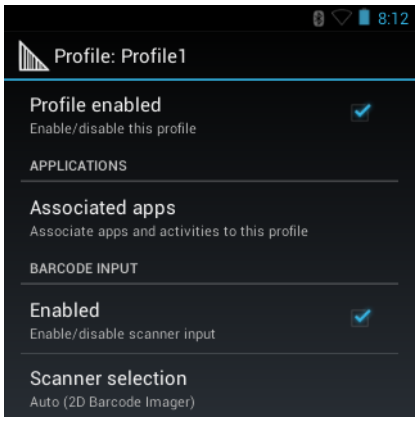
Profiles Screen

To launch DataWedge, touch > **DataWedge**. By default, three profiles appear:

- **Profile0**
- **Launcher**
- **DWDemo**.

Profile0 is the default profile and is used when no other profile can be applied.

Figure 56: DataWedge Profiles Screen



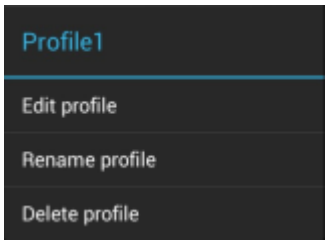
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

To configure a profile touch the profile name.

Profile Context Menu

Touch and hold a profile to open a context menu that allows additional actions to be performed on the selected profile.

Figure 57: Profile Context Menu

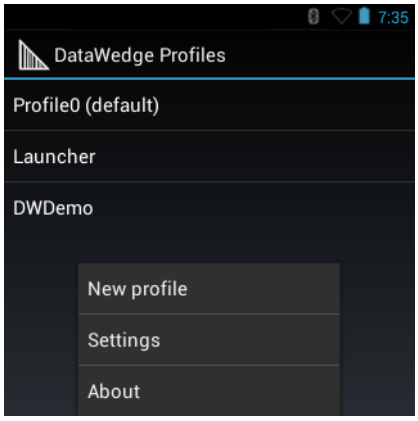


The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

Options Menu

Press to open the options menu.

Figure 58: DataWedge Options Menu



The menu provides options to create a new profiles, access to general DataWedge settings and DataWedge version information.

Disabling DataWedge

Procedure:

1. Touch .
2. Touch .
3. Press .
4. Touch **Settings**.
5. Touch **DataWedge enabled**.
   The blue check disappears from the checkbox indicating that DataWedge is disabled.

Creating a New Profile

Procedure:

1 Touch .

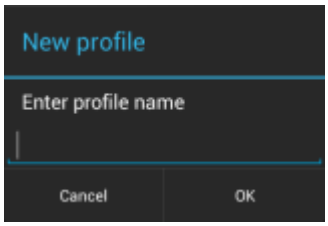
2 Touch .

3 Press .

4 Touch **New profile**.

5 In the **New profile** dialog box, enter a name for the new profile. It is recommended that profile names be unique and made up of only alpha-numeric characters (A-Z, a-z, 0-9).

Figure 59: New Profile Name Dialog Box

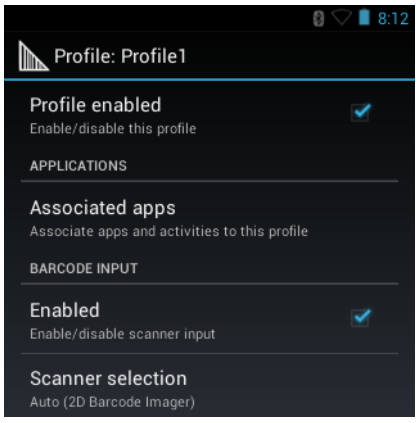


6 Touch **OK**.
The new profile name appears in the **DataWedge profile** screen.

Profile Configuration

To configure the Profile0 or a user-created profile, touch the profile name.

Figure 60: Profile Configuration Screen



The configuration screen lists the following sections:

- Profile enabled
- Applications
- Barcode Input
- Keystroke output
- Intent Output

- IP Output.

Bar Code Input

Use the **Bar Code Input** options to configure the Bar Code Scanner Input Plug-in for the profile.

Enabled

Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.

Scanner Selection

Configures which scanning device to use for bar code data capture when the profile is active.

- **Auto** - The software automatically selects the 2D Imager.
- **2D Imager** - Scanning is performed using the 2D Imager.

Decoders

Configures which bar code decoders are enabled or disabled. For best performance disable all unnecessary decoders.

Touch **Decoders**. The **Barcode input** screen appears. A check in the checkbox indicates that the decoder is enabled. By default the most commonly used decoders are enabled (shown below with an asterisk). The supported decoders are:

UPC-A*	UPC-E0*	EAN-13*
EAN-8*	Code 128*	Code 39*
Interleaved 2 of 5	GS1 DataBar*	GS1 DataBar Limited
GS1 DataBar Expanded	Datamatrix*	QR Code*
PDF417*	Composite AB	Composite C
MicroQR	Aztec*	Maxicode*
MicroPDF	USPostnet	USPlanet
UK Postal	Japanese Postal	Australian Postal
Canadian Postal	Dutch Postal	US4state FICS
Codabar*	MSI	Code 93
Trioptic 39	Discrete 2 of 5	Chinese 2 of 5
Korean 3 of 5	Code 11	TLC 39
Matrix 2 of 5	UPC-E1	

Press ⮌ to return to the previous screen.

Decoder Params

Use **Decode Params** to configure individual decoder parameters.

- **UPCA**
  - **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - enabled).
  - **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

There are three options for transmitting a UPCA preamble:

+ **Preamble None** - Transmit no preamble.
+ **Preamble Sys Char** - Transmit System Character only (default).
+ **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA). Select the appropriate option to match the host system.

- **UPCE0**
  - **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).
  - **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

    There are three options for transmitting a UPCE0 preamble:

    + **Preamble Sys Char** - Transmit System Character only.
    + **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).
    + **Preamble None** - Transmit no preamble (default).
  - **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).
- **Code128**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 67* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 67* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Enable Plain Code 128** - Flag to enable other 128 sub types (besides GS1-128 and ISBT-128).
  - **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
  - **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
  - **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:

    + **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
    + **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
    + **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
  - **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.

    + **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” bar codes.
    + **Security Level 1** - This setting eliminates most misdecodes (default).
    + **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
    + **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes.

Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.

- **Code39**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 67* for more information.
  - **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 67* for more information.
  - **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).
  - **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
  - **Full ASCII** - Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled),
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
  - **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character “A” to all Code 32 bar codes (default - disabled).
  - **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).
- **Interleaved 2 of 5**
  - **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 67* for more information.
  - **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 67* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **Check Digit**
    - **No Check Digit** - A check digit is not used. (default)
    - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
    - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
  - **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).
  - **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
  - **I2of5 Security Level** - Options: **I2of5 Security level 0**, **I2of5 Security Level 1**, **I2of5 Security Level 2** and **I2of5 Security Level 3** (default - I2of5 Security level 1).
- **Composite AB**
  - **UCC Link Mode**
    - **Link Flag ignored** - 1D component is transmitted regardless of whether a 2D component is detected.
    - **Always Linked** - 1D and the 2D components are transmitted. If 2D is not present, the 1D component is not transmitted.
    - **Auto Discriminate** - the digital scanner determines if there is a 2D portion, then transmits the 1D component, as well as the 2D portion if present. (default).
- **UK Postal**
  - **Report Check Digit** - Transmit UK Postal data with or without the check digit. A check in the checkbox indicates to send UK Postal data with check digit (default - disabled).
- **Codabar**

- **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 67* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 67* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).

• **MSI**

- **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 67* for more information.
- **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 67* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
  + **One Check Digit** - Verify one check digit (default).
  + **Two Check Digits** - Verify two check digits.
- **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
  + **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
  + **Mod-10-10** - Both check digits are MOD 10.
- **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).

• **Code93**

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 67* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 67* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

• **Discrete 2 of 5**

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 67* for more information.
- **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 67* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

• **Code 11**

- **Length1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 67* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 67* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code.
  + **No Check Digit** - Do not verify check digit.
  + **1 Check Digit** - Bar code contains one check digit (default).
  + **2 Check Digits** - Bar code contains two check digits.
- **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).

• **Matrix 2 of 5**

- **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 67* for more information.
- **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 67* for more information.

  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
  - **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).
- **UPCE1**
  - **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).
  - **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

    There are three options for transmitting a UPCE1 preamble:

    + **Preamble Sys Char** - Transmit System Character only.
    + **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).
    + **Preamble None** - Transmit no preamble (default).
  - **Convert UPCE1 To UPCA** - Enable this to convert UPCE1 decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable this to transmit UPCE1 decoded data as UPCE1 data, without conversion (default - disabled).

Decode Lengths

The allowable decode lengths are specified by options **Length1** and **Length2** as follows:

- Variable length: Decode symbols containing any number of characters.
  - Set both **Length1** and **Length2** to 0.
- Range: Decode a symbol with a specific length range (from *a* to *b*, including *a* and *b*).
  - Set **Length1** to *a* and set **Length2** to *b*.
- Two Discrete Lengths: Decode only symbols containing either of two selected lengths.
  - Set both **Length1** or **Length2** to the specific lengths. **Length1** must be greater than **Length2**.
- One Discrete Length: Decode only symbols containing a specific length.
  - Set both **Length1** and **Length2** to the specific length.

UPC EAN Params

Allows the configuration of the parameters that apply to more than one UPC or EAN decoder.

- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
  - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding “in-spec” UPC/EAN bar codes (default).
  - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
  - **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
  - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.

- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
  - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled.
- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.

Reader Params

Allows the configuration of parameters specific to the selected bar code reader.

- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -15000).
- **Linear Security Level** - Sets the number of times a bar code is read to confirm an accurate decode.
  - **Security Short or Codabar** - Two times read redundancy if short bar code or Codabar.
  - **Security All Twice** - Two times read redundancy for all bar codes (default).
  - **Security Long and Short** - Two times read redundancy for long bar codes, three times for short bar codes.
  - **Security All Thrice** - Three times read redundancy for all bar codes.
- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.

  - **Disable** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Centered** - Enables the Picklist mode so that only the bar code in the center of the image is decoded. This is most useful when used in conjunction with the static and dynamic reticle viewfinder modes. Note: This mode is only valid for decoder modules that supports a viewfinder. If one tries to set this for a unsupported decoder then the device would issue an error. (Camera scanner only).
  - **Reticle** - Enables the Picklist mode so that only the bar code that is directly under the cross-hair (reticle) is decoded. This is useful when used in conjunction with the static and dynamic reticle viewfinder modes. (Scan Module Only)
- **LCD Mode** - Enables or disables LCD mode. LCD mode enhances the ability of the imager to read bar codes from LCD displays such as cellphones (imager only).
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.

  Note: When using the LCD mode, a degradation in performance may be observed and the aiming crosshair may blink until the bar code is decoded.
- **Illumination mode** - Turns camera illumination on and off. This option is only available when camera is selected in the Barcode input Scanner selection option.
  - **On** - Illumination is on.
  - **Off** - Illumination is off (default).
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D bar codes.
  - **Disable** - Disables decoding of inverse 1D bar codes (default).
  - **Enable** - Enables decoding of only inverse 1D bar codes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D bar codes.
- **Viewfinder Mode** - Configures the Viewfinder modes supported for camera scanning.
  - **Viewfinder Enabled** - Enables only the viewfinder.
  - **Static Reticle** - Enables the viewfinder and a red reticle in the center of the screen which helps selecting the bar code (default).

Scan Params

Allows the configuration of Code ID and decode feedback options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned bar code. This is useful when the reader is decoding more than one code type. Select a code ID character to insert between the prefix and the decoded symbol.
  - **Code ID Type None** - No prefix (default).
  - **Code ID Type Aim** - A standards based three character prefix.
  - **Code ID Type Symbol** - A Symbol defined single character prefix.

  Note: Not all ringtones are fully supported as decode tones and those of longer length may be truncated when used as a decode tone. The recommendation is to test the selected tone for operation before deployment to a customer site.
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).

MSR Input

Use **MSR Input** options to configure the MSR Input Plug-in for the profile.

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.

Keystroke Output

Use to configure the Keystroke Output Plug-in for the profile.

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code data for use in native Android applications. This feature is helpful when populating or executing a form.
  - **None** - Action key character feature is disabled (default).
  - **Tab** - Tab character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 75* for more information.
- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Output

Allows configuration of the Intent Output Plug-in for the profile. The Intent Output Plug-in allows the captured data to be sent to an application in the form of an implicit Intent. Refer to the Android Developer web site for more information, *http://developer.android.com*.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).
- **Intent delivery** - Select the method by which the intent is delivered:
  - Send via StartActivity
  - Send via startService (default)
  - Broadcast intent

- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 75* for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Overview

The core components of an Android application (its activities, services, and broadcast receivers) are activated by intents. An intent is a bundle of information (an Intent object) describing a desired action - including the data to be acted upon, the category of component that should perform the action, and other pertinent instructions. Android locates an appropriate component to respond to the intent, launches a new instance of the component if one is needed, and passes it the Intent object.

Components advertise their capabilities, the kinds of intents they can respond to, through intent filters. Since the system must learn which intents a component can handle before it launches the component, intent filters are specified in the manifest as <intent-filter>elements. A component may have any number of filters, each one describing a different capability. For example, if the manifest contains the following:

```
<intent-filter . . . >
<action android:name=”android.intent.action.DEFAULT” />
<category android:name=”android.intent.category.MAIN” />
</intent-filter>
```

In the Intent output plug-in configuration, the **Intent action** would be:

`android.intent.category.DEFAULT`

and the Intent category would be:

`android.intent.category.MAIN`.

The **Intent delivery** option allows the method by which the intent is delivered to be specified. The delivery mechanisms are **Send via startActivity**, **Send via startService** or **Broadcast intent**.

The decode related data added to the Intent’s bundle can be retrieved using the `Intent.getStringExtra()` and `Intent.getSerializableExtra()` calls, using the following String tags:

- String LABEL_TYPE_TAG = “com.symbol.emdk.datawedge.label_type”;

  - String contains the label type of the bar code.
- String DATA_STRING_TAG = “com.symbol.emdk.datawedge.data_string”;
  - String contains the output data as a String. In the case of concatenated bar codes, the decode data is concatenated and sent out as a single string.
- String DECODE_DATA_TAG = “com.symbol.emdk.datawedge.decode_data”;
  - Decode data is returned as a list of byte arrays. In most cases there will be one byte array per decode. For bar code symbologies that support concatenation e.g. Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per bar code). Clients can get data in each byte array by passing an index.

Most scanning applications might want the user to be able to decode data and for that decode data to be sent to the ***current*** activity but not necessarily displayed. If this is the case, then the activity needs to be marked as ‘singleTop’ in its AndroidManifest.xml file. If your activity is not defined as singleTop, then on every decode, the system will create another copy of your Activity and send the decode data to this second copy.

Finally there will be a configuration option for each process plug-in so that the process plug-in can be configured specifically for the intent output, which in this case is the basic data formatting process plug-in.

IP Output

Note: IPWedge application is required on a host computer. Download the IPWedge application from the Support Central web site: *http://www.zebra.com/support*.

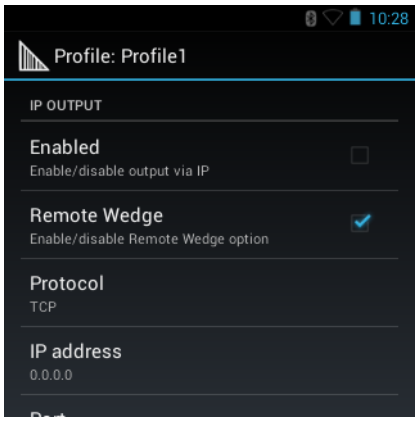
IP Output allows DataWedge to send captured data to a host computer via a network connection. Captured data can be sent over an IP network to a specified IP address and port using either TCP or UDP transport protocols.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.
- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 75* for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Usage

This section provides information on how to configure IP Output using the DataWedge configuration user interface. To use IP Output in a particular DataWedge profile (for example: **Profile0**), scroll downward on **IP Output**.

Figure 61: IP Output Screen



Using IP Output with IPWedge

IPWedge is a computer application that can be easily configured to retrieve data sent over network by DataWedge IP Output. Refer to the *IPWedge User Manual* on how to install and configure in a host computer. To enable IP Output to send captured data to a remote computer that is installed with IPWedge:

Procedure:

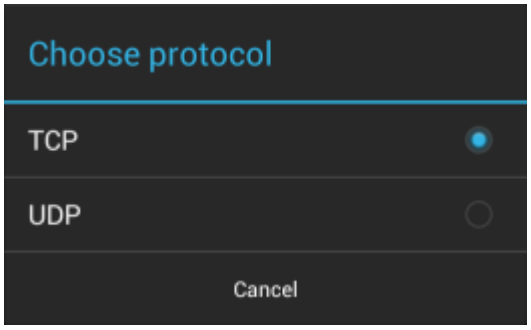
1 In **IP Output**, touch **Enabled**.
A check appears in the checkbox.

2 Ensure **Remote Wedge** option is enabled.

3 Touch **Protocol**.

4 In the **Choose protocol** dialog box, touch the same protocol selected for the **IPWedge** computer application. (TCP is the default).

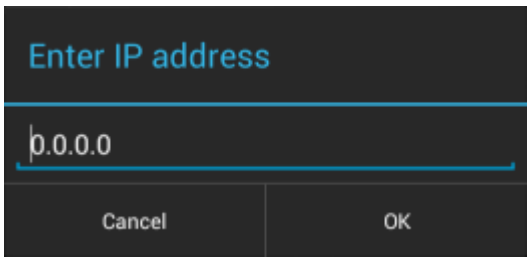
Figure 62: Protocol Selection



5 Touch **IP Address**.

6 In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

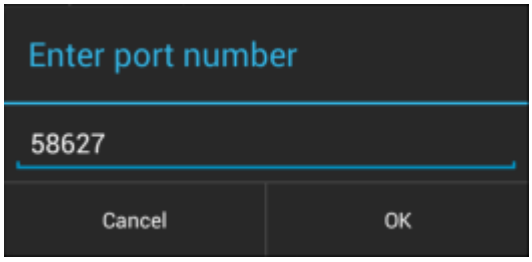
Figure 63: IP Address Entry



7 Touch **Port**.

8 In the **Enter port number** dialog box, enter same port number selected for **IPWedge** computer application.

Figure 64: Port Number Entry



9 Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

Using IP Output without IPWedge

IP Output Plug-in can be used to send captured data from **DataWedge** to a remote device or host computer without using **IPWedge**. At the data receiving end, the host computer or mobile device should have an application, that listens to TCP or UDP data coming from a configured port and IP address in the IP Output plug-in. To enable IP Output to send captured data to a remote computer:

Procedure:

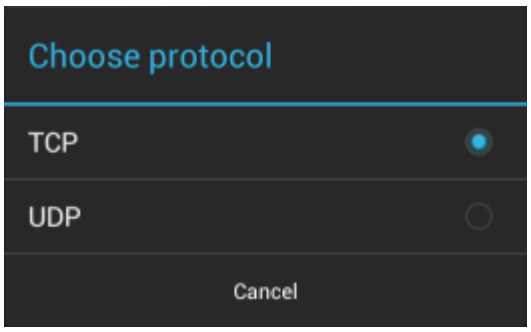
1 In **IP Output**, touch **Enabled**.
A check appears in the checkbox.

2 Ensure **Remote Wedge** option is disabled.

3 Touch **Protocol**.

4 In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

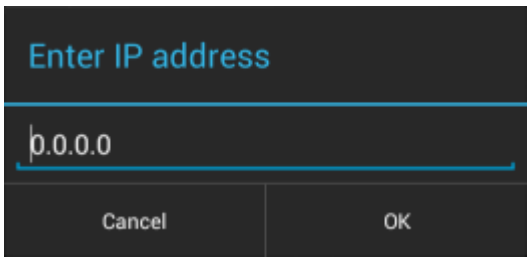
Figure 65: Protocol Selection



5 Touch **IP Address**.

6 In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.

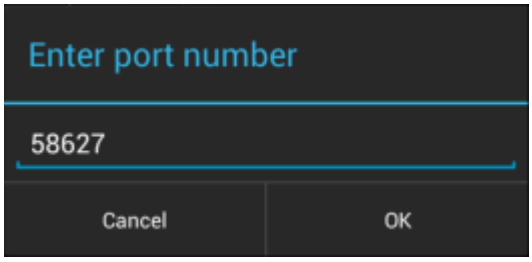
Figure 66: IP Address Entry



7 Touch **Port**.

8 In the **Enter port number** dialog box, enter the port number that the host computer application is listening on.

Figure 67: Port Number Entry



9 Configure **Advanced Data Formatting** and **Basic Data Formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

Generating Advanced Data Formatting Rules

The ADF plug-in applies rules (actions to be performed based on defined criteria) to the data received via an input plug-in before sending it to the output plug-in.

- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.
- Criteria - Criteria can be set according to Input plug-in, symbology, matching string within the data (at the specified position) and/or data length. Received data must match the defined criteria in order for the data to be processed.
- Actions - A set of procedures defined to format data. There are four types of actions which are for formatting cursor movement, data modification, data sending and delay specifications. An action can be defined to send the first number of characters to the Output plug-in, pad the output data with spaces or zeros, remove spaces in data, etc.

Configuring ADF Plug-in

Configuring the ADF plug-in consists of creating a rule, defining the criteria and defining the actions.

Procedure:

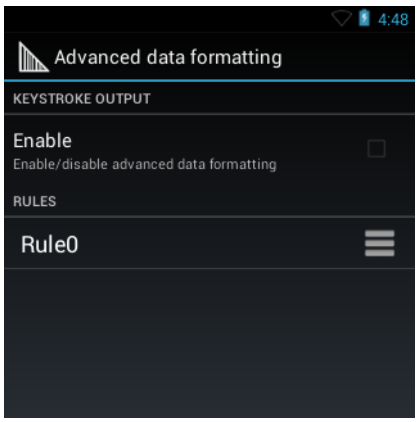
1 Touch  .

2 Touch  .

3 Touch a DataWedge profile.

4 In **Keystroke Output**, touch **Advanced data formatting**.

Figure 68: Advanced Data Formatting Screen



5 Touch the **Enable** checkbox to enable ADF.

Creating a Rule

Note: By default, **Rule0**, is the only rule in the **Rules** list.

Procedure:

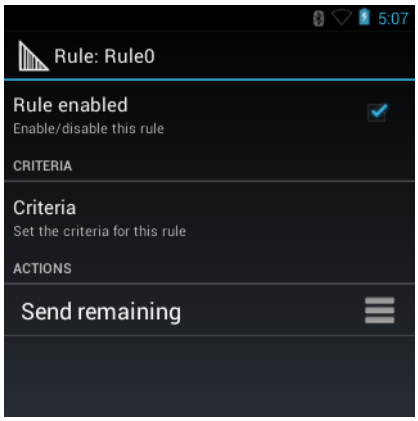
1 Press .
2 Touch **New rule**.
3 Touch the **Enter rule name** text box.
4 In the text box, enter a name for the new rule.
5 Touch **Done**.
6 Touch **OK**.

Defining a Rule

Procedure:

1 Touch the newly created rule in the **Rules** list.

Figure 69: Rule List Screen



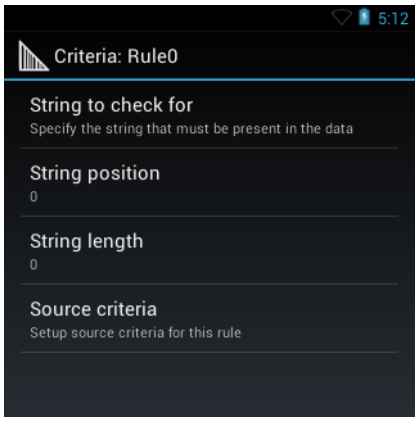
2 Touch the **Rule enabled** checkbox to enable the current rule.

Defining Criteria

Procedure:

1 Touch **Criteria**.

Figure 70: Criteria Screen



2 Touch **String to check for** option to specify the string that must be present in the data.

3 In the **Enter the string to check for** dialog box, enter the string

4 Touch **Done**.

5 Touch **OK**.

6 Touch **String position** option to specify the position of the string specified in the **String to check for** option. The ADF rule is only applied if the specific string in **String to check** for is found at the specified **String position** location (zero for the start of the string).

7 Touch the + or - to change the value.

8 Touch **OK**.

9 Touch **String length option** to specify a length for the received data. The ADF rule only applies to the bar code data with that specified length.

10 Touch the + or - to change the value.

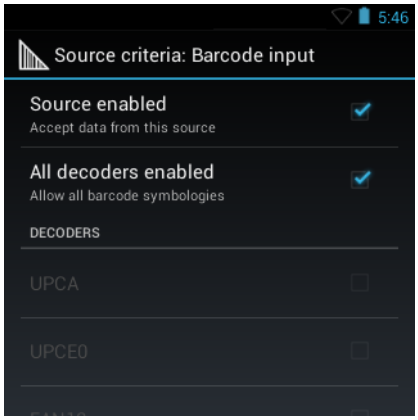
11 Touch **OK**.

12 Touch **Source criteria** option to associate an input device to an ADF rule. The ADF rule only applies to data received from associated input devices.

13 Touch **Barcode input**.

14 Touch the **Source enabled** checkbox to accept data from this source.

Figure 71: Barcode Input Screen



15 For **Barcode inputs**, touch the **All decoders enabled** checkbox to select all bar code symbologies. Deselect the **All decoders enabled** checkbox to individually select the symbologies.

16 Press ⮌ until the **Rule** screen appears.

17 If required, repeat steps to create another rule.

18 Press ⮌ until the **Rule** screen appears.

Defining an Action

Note: By default the **Send remaining** action is in the **Actions** list.

Procedure:

1 Press ▭.

2 Touch **New action**.

3 In the **New action** menu, select an action to add to the **Actions** list. See *Table 8: ADF Supported Actions on page 78* for a list of supported ADF actions.

4 Some Actions require additional information. Touch the Action to display additional information fields.

5 Repeat steps to create more actions.

6 Press ⮌.

7 Press ⮌.

Deleting a Rule

Procedure:

1 Touch and hold on a rule until the context menu appears.

2 Touch **Delete** to delete the rule from the **Rules** list.

Note: When there is no rule available for ADF plug-in or all rules are disabled, DataWedge passes decoded data to the output plug-in without processing the data.

Order Rules List

Note: When there are no rules defined, ADF passes the captured data through as is. In contrast, when rules are defined but all are disabled, ADF does not pass any captured data through.

Rules are processed in top-down order. The rules that are on top of the list are processed first. Use the icon next to the rule to move it to another position in the list.

Table 8: ADF Supported Actions

Type	Actions	Description
Cursor Movement	Skip ahead	Moves the cursor forward by a specified number of characters. Enter the number of characters to move the cursor ahead.
	Skip back	Moves the cursor back by a specified number of characters. Enter the number of characters to move the cursor back.
	Skip to start	Moves the cursor to the beginning of the data.
	Move to	Moves the cursor forward until the specified string is found. Enter the string in the data field.

Table continued…

Type	Actions	Description
	Move past a	Moves the cursor forward past the specified string. Enter the string in the data field.
Data Modification	Crunch spaces	Remove spaces between words to one and remove all spaces at the beginning and end of the data.
	Stop space crunch	Stops space crunching. This disables the last **Crunch spaces** action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last **Remove all spaces** action.
	Remove leading zeros	Remove all zeros at the beginning of data.
	Stop zero removal	Stop removing zeros at the beginning of data. This disables the previous **Remove leading zeros** action.
	Pad with zeros	Left pad data with zeros to meet the specified length. Enter the number zeros to pad.
	Stop pad zeros	Stop padding with zeros. This disables the previous **Pad with zeros** action.
	Pad with spaces	Left pad data with spaces to meet the specified length. Enter the number spaces to pad.
	Stop pad spaces	Stop padding with spaces. This disables the previous **Pad with spaces** action.
	Replace string	Replaces a specified string with a new string. Enter the string to replace and the string to replace it with.
	Stop all replace string	Stop all **Replace string** actions.
Data Sending	Send next	Sends the specified number of characters from the current cursor position. Enter the number of characters to send.
	Send remaining	Sends all data that remains from the current cursor position.
	Send up to	Sends all data up to a specified string. Enter the string.
	Send pause	Pauses the specified number of milliseconds before continuing the next action. Enter the amount of time in milliseconds.
	Send string	Sends a specified string. Enter the string to send.
	Send char	Sends a specified ASCII/ Unicode character. Enter a character value. The maximum Unicode character value can be entered is U-10FFFF (= 1114111 in decimal).

Deleting an Action

Procedure:

1 Touch and hold the action name.

2 Select **Delete action** from the context menu.

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

When a user scans a bar code with the following criteria:

- Code 39 bar code.
- length of 12 characters.
- contains 129 at the start position.

Modify the data as follows:

- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

To create an ADF rule for the above example:

Procedure:

1 Touch  .
2 Touch **DataWedge**.
3 Touch **Profile0**.
4 Under **Keystroke Output**, touch **Advanced data formatting**.
5 Touch **Enable**.
6 Touch **Rule0**.
7 Touch **Criteria**.
8 Touch **String to check for**.
9 In the **Enter the string to check for** text box, enter `129` and then touch **OK**.
10 Touch **String position**.
11 Change the value to `0`.
12 Touch **OK**.
13 Touch **String length**.
14 Change value to `12`.
15 Touch **OK**.
16 Touch **Source criteria**.
17 Touch **Barcode input**.
18 Touch **All decoders enabled** to disable all decoders.
19 Touch **Code 39**.
20 Press  three times.
21 Touch and hold on the **Send remaining rule** until a menu appears.
22 Touch **Delete action**.
23 Press  .
24 Touch **New action**.
25 Select **Pad with zeros**.
26 Touch the **Pad with zeros** rule.
27 Touch **How many**.
28 Change value to `8` and then touch **OK**.
29 Press  three times.
30 Press .
31 Touch **New action**.
32 Select **Send up to**.
33 Touch **Send up to** rule.

34 Touch **String**.

35 In the **Enter a string** text box, enter `X`.

36 Touch **OK**.

37 Press ⮌ three times.

38 Press ▭.

39 Touch **New action**.

40 Select **Send char**.

41 Touch **Send char** rule.

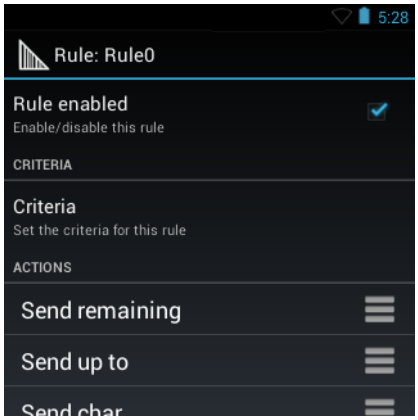
42 Touch **Character code**.

43 In the **Enter character code** text box, enter `32`.

44 Touch **OK**.

45 Press ⮌.

Figure 72: ADF Sample Screen



46 Ensure that an application is open on the device and a text field is in focus (text cursor in text field).

47 Aim the exit window at the bar code.

Figure 73: Sample Bar Code

48 Press and hold the scan button.

The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern. The LED light red to indicate that data capture is in process.

49 The LED lights green and a beep sounds, by default, to indicate the bar code was decoded successfully. The formatted data 000129X<space>appears in the text field.

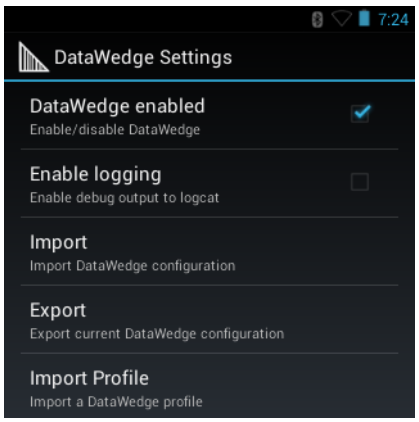
Scanning a Code 39 bar code of 1299X15598 does not transmit data (rule is ignored) because the bar code data did not meet the length criteria.

Figure 74: Formatted Data

DataWedge Settings

The DataWedge Settings screen provides access to general, non-profile related options. Press > **Settings**.

Figure 75: DataWedge Settings Window



- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option.
- **Enable logging** - Enables or disables debug output file to logcat. To enable logging check this option.
- **Import** - allows import of a DataWedge configuration file. The imported configuration replaces the current configuration.
- **Export** - allows export of the current DataWedge configuration to the microSD card.
- **Import Profile** - allows import of a DataWedge profile file.
- **Export Profile** - allows export of a DataWedge profile.
- **Restore** - return the current configuration back to factory defaults.

Importing a Configuration File

Procedure:

1 Copy the configuration file to the root of the microSD card.

2 Touch .

3 Touch .

4 Press  .
5 Touch **Settings**.
6 Touch **Import**.
7 Touch **SD Card**.
8 Touch **Import**. The configuration file (`datawedge.db`) is imported and replaces the current configuration.

Exporting a Configuration File

Procedure:

1 Touch  .
2 Touch  .
3 Press  .
4 Touch **Settings**.
5 Touch **Export**.
6 Touch **SD Card**.
7 Touch **Export**. The configuration file (`datawedge.db`) is saved to the root of the microSD card.

Importing a Profile File

Note: Do not change the filename of the of the profile file. If the filename is changed, the file will not be imported.

Procedure:

1 Copy the profile file to the root of the microSD card.
2 Touch  .
3 Touch  .
4 Press  .
5 Touch **Settings**.
6 Touch **Import Profile**.
7 Touch the profile file to import.
8 Touch **Import**. The profile file (`dwprofile_x.db`, where x = the name of the profile) is imported and appears in the profile list.

Exporting a Profile

Procedure:

1 Touch  .
2 Touch  .
3 Press  .
4 Touch **Settings**.
5 Touch **Export Profile**.
6 Touch the profile to export.

7 Touch **Export**.

8 Touch **Export**. The profile file (`dwprofile_x.db`, where x = name of the profile) is saved to the root of the microSD card.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

Procedure:

1 Touch  .

2 Touch  .

3 Press  .

4 Touch **Settings**.

5 Touch **Restore**.

6 Touch **Yes**.

Configuration and Profile File Management

The configuration or profile settings for DataWedge can be saved to a file for distribution to other devices.

After making configuration or profile changes, export the new configuration or profile to the root of the microSD card. The configuration file created is automatically named `datawedge.db`. The profile file created is automatically named `dwprofile_x.db`, where `x` is the profile name. The files can then the copied to the microSD card of other devices and imported into DataWedge on those devices. Importing a configuration or profile replaces the existing settings.

Enterprise Folder

Internal storage contains the Enterprise folder (`/enterprise`). The Enterprise folder is persistent and maintains data after an Enterprise reset. After an Enterprise Reset, DataWedge checks folder `/enterprise/device/settings/datawedge/enterprisereset/` for a configuration file, `datawedge.db` or a profile file, `dwprofile_x.db`. If the file is found, it imports the file to replace any existing configuration or profile.

Note: A Factory Reset deletes all files in the Enterprise folder.

Auto Import

DataWedge supports remote deployment of a configuration to a device, using tools such as MSP. DataWedge monitors the `/enterprise/device/settings/datawedge/autoimport` folder for the DataWedge configuration file (`datawedge.db`) or a profile file (`dwprofile_x.db`). When DataWedge launches it checks the folder. If a configuration or profile file is found, it imports the file to replace any existing configuration or profile. Once the file has been imported it is deleted from the folder.

While DataWedge is running it receives a notification from the system that a file has been placed into the `/enterprise/device/settings/datawedge/autoimport` folder. When this occurs, DataWedge imports this new configuration or profile, replacing the existing one and delete the file. DataWedge begins using the imported configuration immediately.

Note:

A Factory Reset deletes all files in the Enterprise folder.

It is strongly recommended that the user exits DataWedge before remotely deploying any configuration or profile. It is required that the file permissions are set to 666.

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application

To override the trigger key in an application, create a profile for the application that disables the Barcode input. In the application, use standard APIs, such as onKeyDown() to listen for the KEYCODE_BUTTON_L1 and KEYCODE_BUTTON_R1 presses.

Capture Data and Taking a Photo in the Same Application

To be able to capture bar code data and take a photo in the same application:

- Create a Datawedge profile pertaining to the picture taking Activity in your application that disables scanning and use standard Android SDK APIs to control the Camera.
- The default Datawedge profile takes care of the scanning in the application. You might want to create another DataWedge profile that caters to any specific scanning needs, associated to your Application's Activity pertaining to scanning.

Disable DataWedge on MC32N0 and Mass Deploy

To disable DataWedge and deploy onto multiple MC32N0 devices:

Procedure:

1. Touch  .
2. Touch  .
3. Press  .
4. Touch **Settings**.
5. Unselect the **DataWedge enabled** check box.
6. Export the DataWedge configuration. See *Exporting a Configuration File on page 83* for instructions. See *Configuration and Profile File Management on page 84* for instructions for using the auto import feature.

Soft Scan Feature

DataWedge allows a native Android application to programmatically start, stop, or toggle the scan trigger state. The application can issue an Android Broadcast Intent, to control the scanner, without requiring the scan button to be pressed. The active DataWedge profile is required to control all the parameters during a scan operation.

The structure of the broadcast intent that resolves to the soft scan is:

action: “com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”

extras: This is a String name/value pair that contains trigger state details.

name: “com.symbol.emdk.datawedge.api.EXTRA_PARAMETER”

value: “START_SCANNING” or “STOP_SCANNING” or “TOGGLE_SCANNING”

Sample

```
Intent sendIntent = new Intent();
sendIntent.setAction(“com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”);
sendIntent.putExtra(“com.symbol.emdk.datawedge.api.EXTRA_PARAMETER”, “TOGGLE_SCANNING”);
sendBroadcast(sendIntent);
```

Chapter 5

Administrator Utilities

Note: This chapter applies to Android devices only.

We provide a suite of utilities that allow an administrator to manage the following features:

- Multi-user Login - The Multi-user Login feature allows an administrator to set up the device to be used by multiple users. The users have access to specific applications and features depending upon the user settings.
- Application Lock - The Application Lock feature allows an administrator to restrict application access for specific applications by user or groups of users. The permitted applications are managed using groups of user accounts from Multi-user Login feature.
- Secure Storage - Secure Storage Administrator application allows installation and deletion of encrypted keys and creation, mounting, un-mounting and deletion of the encrypted file systems.

The following applications help the administrator configure these features.

- On-device applications - reside on the device.
  - MultiUser Administrator
  - AppLock Administrator
  - Secure Storage Administrator.
- Host computer application - reside on a host computer.
  - Enterprise Administrator.

Required Software

These tools are available on the Support Central web site at *Support Central*. Download the required files from the Support Central web site and follow the installation instruction provided.

On-device Application Installation

See *Application Installation on page 119* for instruction on installing applications onto the device.

Multi-user/AppLock Configuration

To use the Multi-user Login and Application Lock features, the administrator must create user and group account information using the Enterprise Administrator application.

Note: The administrator can also create the account information manually. See *Manual File Configuration on page 97* for more information.

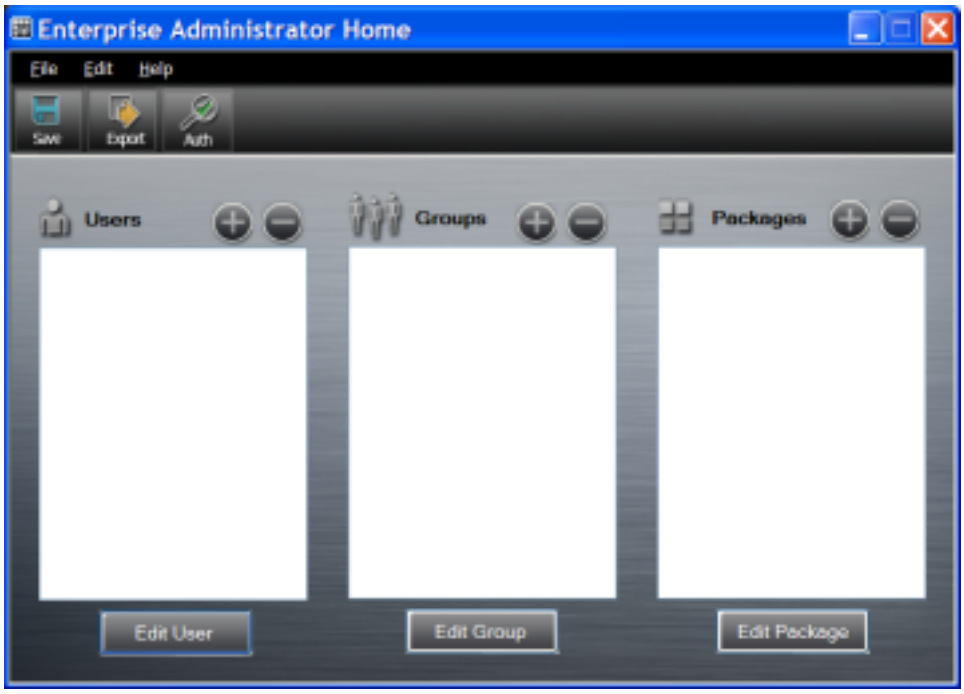
Enterprise Administrator Application

Note: .Net Compact Framework 4 or later is required to run the Enterprise Administrator. To download, go to *www.microsoft.com*.

Use the Enterprise Administrator application to setup user and group accounts and create the required (Password, Group and White List) files for using the Multi-user and Application Lock features.

On the host computer launch the **Enterprise Administrator** application.

Figure 76: Enterprise Administrator Window



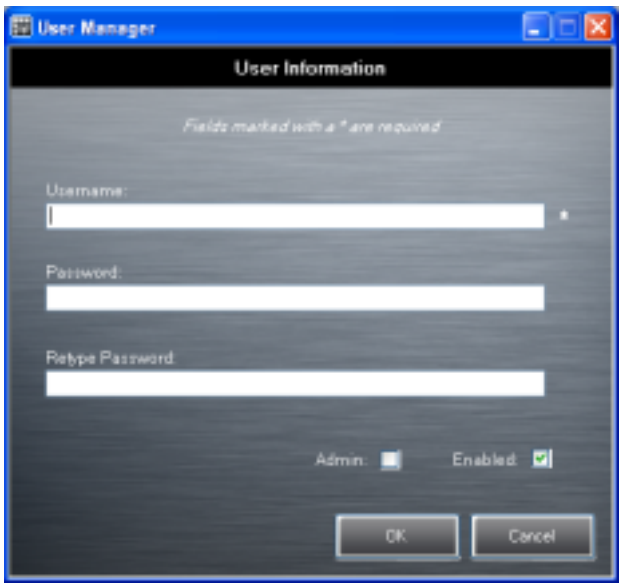
Creating Users

Each person that uses the device has to have a user name and password. To create a user:

Procedure:

1 Click + above the **Users** list box.

Figure 77: User Manager Window



2 In the **Username** text box, enter a user name. The text is case sensitive and required.
3 In the **Password** text box, enter a password for the user. The text is case sensitive and required.
4 In the **Retype Password** text box, re-enter the user password.
5 Select the **Admin** checkbox to set the user to have administrator rights.
6 Select the **Enabled** checkbox to enable the user.
7 Click **OK**.
8 Repeat steps 1 through 7 for each additional user.

Adding Packages

Note: All system applications that are on the default image are available to all users.

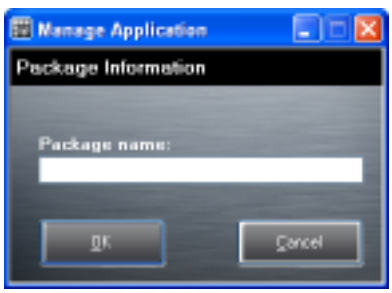
Create a list of installed applications (packages) on the device that are available for use by all the users.

Procedure:

1 Click + next to **Packages**.

Note: To get a list of all the applications (packages) on the device see *Determining Applications Installed on the Device on page 100*.

Figure 78: Package Information Window



2 In the **Package name** text box, enter the name of an application.
3 Click **OK**.

4 Repeat steps 1 through 3 for each additional package.

Creating Groups

Create groups of users that have access to specific applications.

Procedure:

1 Click + above the **Groups** list. The **Group Manager** window appears with a list of users and packages.

Figure 79: Group Manager Window

2 In the **Group name** text box, enter a name for the group. This field is required.

3 Select a user in the **Available Users** list box and then click the **Add** button to add the user to the **Users in Group** list box or click the **Add All** button to add all the users in the **Available Users** list box to the **Users in Group** list box.

4 Select a package in the **Available Packages** list box and then click the **Add** button to add the package to the **Packages in Group** list box or click the **Add All** button to add all the packages in the **Available Packages** list box to the **Packages in Group** list box.

5 Click **OK**.

6 Click **Save**.

Creating Remote Authentication

Use the Remote Authentication feature to set a remote server for authentication.

Procedure:

1 Click the **Auth** button. The **Authentication** window appears.

Figure 80: Authentication Window

2 Select the **Remote** radio button.
3 In the **Server IP** text box, enter the address of the remote server.
4 In the **Port** text box, enter the port number of the remote server.
5 Select the **use SSL Encryption** check box if SSL encryption is required.
6 Click **OK**.

Save Data

At any time, the administrator can save the current data. The application creates two files in the <user>_APP_DATA folder: *database* and *passwd*.

Exporting File

In order to use the features on the device, export the required files and then copy them to the device. The following files are created by the Enterprise Administrator application:

- Password File - Filename: `passwd`. Lists the user names, encrypted passwords, administrator and enable flags.
- Group File - Filename: `groups`. Lists each group and users associated to each group.
- White List Files - Filename: the filenames are the names of the group created in the Group file. Lists the user installed applications that the group is allowed to access.
- Remote Server - Filename: `server`. Lists the remote server IP address and port number.

Procedure:

1 Click **Export**.
2 In the **Browse For Folder** window, select a folder and then click **OK**.
3 Click **OK**.
4 Click **File → Export → Server Information**.
The server file is saved in the `<user>\_APP_DATA` folder.
5 Copy all the files to the root of the microSD card. See *USB Communication on page 55* for information on copying files to the device.

Importing User List

Procedure:

1 Click **File → Import → User List**.

2 Navigate to the location when the *passwd* file is stored.
3 Select the `passwd` file.
4 Click **Open**.
The user information is populated into the **Users** list.

Importing Group List

Procedure:

1 Click **File → Import → Group List**.
2 Navigate to the location when the `group` file is stored.
3 Select the `group` file.
4 Click **Open**.
The group and package information is populated into the **Groups** and **Packages** list.

Importing Package List

To import a package list (see *Package List File on page 98* for instructions for creating a Package List file):

Procedure:

1 Click **File → Import → Package List**.
2 Navigate to the location when the package file is stored.
3 Select the package text file.
4 Click **Open**.
The package information is populated into the **Packages** list.

Editing a User

Procedure:

1 Select a user in the **Users** list.
2 Click **Edit User**.
3 Make changes and then click **OK**.

Deleting a User

Procedure:

1 Select a user in the **Users** list.
2 Click **-**. The user name is removed from the list.

Editing a Group

Procedure:

1 Select a user in the **Groups** list.
2 Click **Edit Group**.
3 Make changes and then click **OK**.

Deleting a Group

Procedure:

1 Select a group in the **Groups** list.

2 Click -.
3 Click **Yes**. The group name is removed from the list.

Editing a Package

Procedure:

1 Select a package in the **Packages** list.
2 Click **Edit Package**.
3 Make changes and then click **OK**.

Deleting a Package

Procedure:

1 Select a package in the **Packages** list.
2 Click -. The package name is removed from the list.

MultiUser Administrator

Use the MultiUser Administrator application to allow an administrator to enable, disable and configure the Multiuser Login feature.

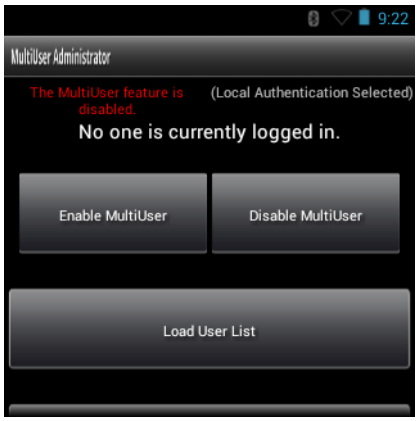
Importing a Password

When the MultiUser Administrator is used for the first time, the password file must be imported.

Procedure:

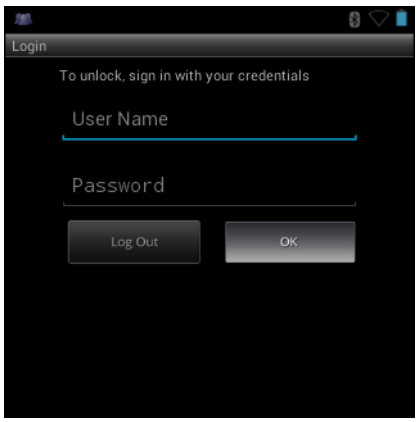
1 Touch .
2 Touch .

Figure 81: MultiUser Administrator Screen



3 Touch **Load User List**. The application reads the data from the `passwd` file and configures the Multi-user Login feature.
4 Touch **Enable Multiuser** to enable the feature.

Figure 82: MultiUser Login Screen



5 In the **Login** text box, enter the username.
6 In the **Password** text box, enter the password.
7 Touch **OK**.

Disabling the Multi-user Feature

Note: To disable the Multi-user Login feature, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Procedure:

1 Touch .
2 Touch .
3 Touch **Disable MultiUser**.
The Multi-user feature is disabled immediately.

Enabling Remote Authentication

Caution: When Remote Authentication is enable, the device searches for the remote server during the login procedure. If the remote server is not available or the address is incorrect, the user would not be able to login and an Enterprise reset is required to access the device.

Procedure:

1 Touch .
2 Touch .
3 Touch **Load Server Info**. The application reads the data from the *server* file and configures the Multi-user Login feature.
4 Press .
5 Touch **Enable Remote Authentication**.
The device accesses the remote server and then Login screen appears.

Disabling Remote Authentication

Caution: When Remote Authentication is enable, the device searches for the remote server during the login procedure. If the remote server is not available or the address is incorrect, the user would not be able to login and an Enterprise reset is required to access the device.

Procedure:

1 Touch .

2 Touch .

3 Press .

4 Touch **Disable Remote Authentication**.
The remote authentication feature is disabled immediately. The device suspends. When resumed, the login screen appears.

Enabling Data Separation

Note: To enable Data Separation, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Data Separation feature allows each user of the device to have separate isolated data area for installed application. To enable data separation:

Procedure:

1 Touch .

2 Touch .

3 Press .

4 Touch **Enable Data Separation**. The current user is logged out to prepare the data space for each user as they log in.

Disabling Data Separation

Note: To disable Data Separation, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Procedure:

1 Touch .

2 Touch .

3 Press .

4 Touch **Disable Data Separation**. The current user is logged out to restore the system to common data space for all users.

Delete User Data

Note: To delete user data, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Procedure:

1 Touch .
2 Touch .
3 Press .
4 Touch **Delete Individual User Data**. A dialog box displays with all of the users that currently have data associated with their log in.
5 Select each user to delete or **Select All** to delete all user data.
6 Touch **Delete** to delete the data.

Capturing a Log File

Procedure:

1 Touch .
2 Touch .

Note: To capture a log file, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

3 Touch **Export Log** to copy the log file to the On-device Storage. The log file can be captured when the multi-user feature is in either the enabled or disabled mode.
4 The log file and a backup log file are named `multiuser.log` and `multiuser.log.bak`, respectively.

AppLock Administrator

The Application Lock feature allows the system administrator to restrict application access for specific applications by user or groups of users. The permitted applications are managed using groups of user accounts from Multi-user feature.

The permitted application names are built into an application White List that is used to know which applications are managed by the system.

The Application Lock feature does not prevent execution of native code or plug-ins and it does not prevent applications from accessing public classes within non-permitted applications. The AppLock Administrator application takes advantage of the Application Lock feature allowing an administrator to enable, disable and install White Lists and Groups files.

Note: To use the AppLock Administrator application, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Enabling Application Lock

Procedure:

1 Touch .

2 Touch  .

3 Touch **Enable Application Lock**.

Disabling Application Lock

Procedure:

1 Touch  .

2 Touch  .

3 Touch **Disable Application Lock**.

Manual File Configuration

Groups File

A Groups file is a text file that provides a list of groups and assigns users to each group.

The text file contains one line for each group. Each line is formatted as follows:

`<groupname>:<user1>,<user2>,...<usern>`

where:

`<groupname>` = the name for a group. This is also the name of the White List file for this group. This field uses any alphanumeric character.

`<user1>` through `<userN>` = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 93* for more information.

Note:

If the same user is assigned to multiple groups, then that user's White List will be a logical union of the White Lists for all of the groups that user is assigned.

A line starting with the # character is considered a comment and is ignored.

Examples:

- `AdminGroup:alpha`
  - The Group name is AdminGroup and assigns user alpha to the group.
- `ManagersGroup:beta,gamma`
  - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

A White List file is a text file that provides a list of allowed packages from that group. The text file contains one line for each allowed package for that user group. Each line is format as follows:

`<package1name>`

.

.

.

`<packageNname>`

where:

<package1Name> = the package name allowed for this group. Wild cards are allowed for this field.

Example:

Refer to the example of the Groups file above. A White List file of the name AdminGroup could have the following lines:

```
com.companyname.application
com.symbol.*
```

where:

`com.companyname.application` = the specific application with the package name

`com.companyname.application` will be permitted for this group.

`com.symbol.*` = any application that has a package name that starts with

`com.symbol` will be permitted for this group.

Note:

The wildcard ".*" is allowed and indicates that this group is permitted to run any package.

A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

To assure that administrative users have access to all device functionality, the White List for the administrative users group should use the wildcard.

At a minimum, the White List for the administrative users group should contain *com.symbol.fusion* to allow administrative users the ability to configure Wi-Fi advanced settings.

Package List File

A Package List file is a text file that lists package names that can be imported into the Packages list. The file makes it easier to enter package name into the application. The text file contains one line for each package name.

Example:

```
com.zebra.example1
com.zebra.example2
com.zebra.example3
com.zebra.example4
```

Groups File

A Groups file is a text file that provides a list of groups and assigns users to each group.

The text file contains one line for each group. Each line is formatted as follows:

```
<groupname>:<user1>,<user2>,...<usern>
```

where:

<groupname> = the name for a group. This is also the name of the White List file for this group. This field uses any alphanumeric character.

<user1> through <userN> = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 93* for more information.

Note:

If the same user is assigned to multiple groups, then that user's White List will be a logical union of the White Lists for all of the groups that user is assigned.

A line starting with the # character is considered a comment and is ignored.

Examples:

- `AdminGroup:alpha`
  - The Group name is AdminGroup and assigns user alpha to the group.
- `ManagersGroup:beta,gamma`
  - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

A White List file is a text file that provides a list of allowed packages from that group. The text file contains one line for each allowed package for that user group. Each line is format as follows:

`<package1name>`

.

.

.

`<packageNname>`

where:

`<package1Name>` = the package name allowed for this group. Wild cards are allowed for this field.

Example:

Refer to the example of the Groups file above. A White List file of the name AdminGroup could have the following lines:

`com.companyname.application`

`com.symbol.*`

where:

`com.companyname.application` = the specific application with the package name

`com.companyname.application` will be permitted for this group.

`com.symbol.*` = any application that has a package name that starts with

`com.symbol` will be permitted for this group.

Note:

The wildcard ".*" is allowed and indicates that this group is permitted to run any package.

A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

To assure that administrative users have access to all device functionality, the White List for the administrative users group should use the wildcard.

At a minimum, the White List for the administrative users group should contain *com.symbol.fusion* to allow administrative users the ability to configure Wi-Fi advanced settings.

Determining Applications Installed on the Device

To determine the names of applications installed on the device for use with the Enterprise Administrator application:

Procedure:

1 Connect the device to the host computer.

Note: See *Development Tools on page 118* for information on installing the USB driver for use with adb.

2 On the host computer, open a command prompt (or a terminal in Ubuntu) and run the following:

`adb devices`. This returns the device id.

```
adb shell
$pm list packages -f > sdcard/pkglist.txt
$exit
```

3 A pkglist.txt file is created in the root of the microSD card. The file lists all the .apk files installed with their package names.

Package List File

A Package List file is a text file that lists package names that can be imported into the Packages list. The file makes it easier to enter package name into the application. The text file contains one line for each package name.

Example:

```
com.symbol.example1
com.symbol.example2
com.symbol.example3
com.symbol.example4
```

Secure Storage

Secure Storage Administrator application allows:

- installation and deletion of encrypted keys
- creation, mounting, un-mounting and deletion of the encrypted file systems.

Installing a Key

Procedure:

1 Touch  .

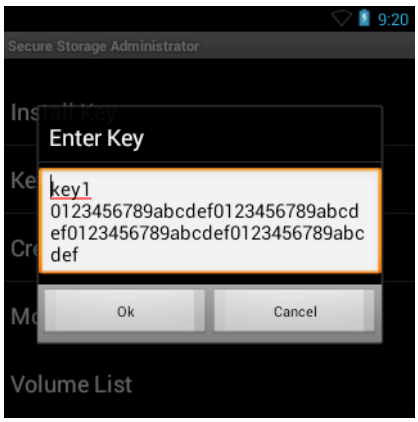
2 Touch  .

3 Touch **Install Key**.

4 Touch **Manual**.

5 Touch **OK**.

Figure 83: Enter Key Dialog Box



6 In the **Enter key** text box, enter the key name followed by the key value obtained in step 1, using the following format:

<Key Name> <Key value in Hex String>

Example: key2 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

The key value must be a 64 hexadecimal character string.

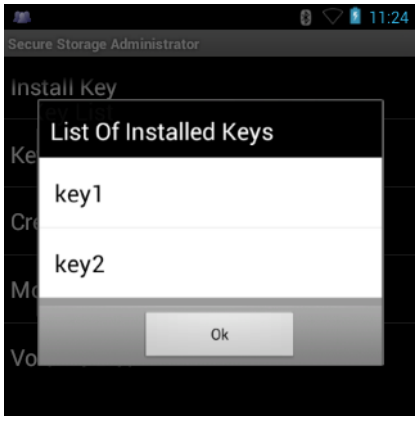
7 Touch **OK**. The key is imported into the device. The message **successfully installed the key** appears on the screen.

Viewing Key List

Procedure:

1 Touch **Key List**.

Figure 84: List of Keys



2 Touch **OK**.

Deleting a Key

Procedure:

1 Touch **Revoke Key**.

2 Touch the key to deleted.

3 Touch **OK**.

Note: If a key is deleted then all the volumes created using that key are un-mounted. The same key is required to re-mount the volume.

Volumes

Creates an encrypted file system (volume) on the device. The user must have Administrative privileges to create a volume.

Creating Volume Using EFS File

Procedure:

1 Create an efs file. See *Creating an EFS File on page 103* for instruction on creating the efs file.
2 Copy the `keyfile` and `efsfile` files to root of the microSD card. See *USB Communication on page 55*.
3 Touch **Create Volume**.
4 Touch **Import**.
5 Touch **OK**. The message **Successfully Created the Volume** appears briefly.

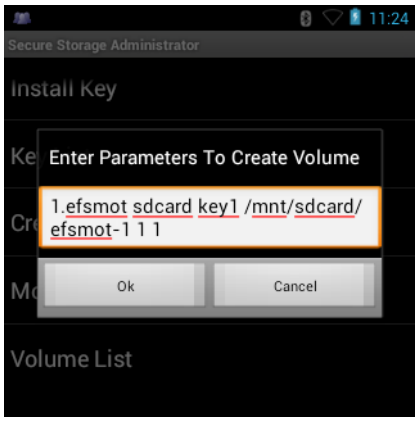
Creating a Volume Manually

Procedure:

1 Touch **Create Volume**.
2 Touch **Manual**.
3 Touch **OK**.
4 In the **Enter Parameters To Create Volume** text box, enter the parameters in the follow format:
<Volume Name> <Volume Storage Type> Key Name> <Mount Path> <Auto Mount> <Volume size>
where:

- <Volume Name> = name of the volume.
- <Volume Storage Type> = storage location. Options: internal or sdcrad.
- <Key Name> = name of the key to use when creating the volume.
- <Mount Path> = path where the volume will be located.
- <Auto Mount> = Options: 1 = yes, 0 = no.
- <Volume size> = size of the volume in Megabytes.

Figure 85: Enter Parameter To Create Volume Dialog Box



5 Touch **OK**. The message **Successfully Created the Volume** appears briefly. If the size of the volume is very large, a progress bar displays.

Mounting a Volume

Procedure:

1 Touch **Mount Volume**.
2 Touch **sdcard** or **internal**.
3 Touch **OK**.
4 Select a volume.
5 Touch **OK**.

Listing Volumes

Procedure:

1 Touch **Volume List**.
2 Touch **sdcard** to list volumes on the microSD card or **internal** to list volumes on internal storage.
3 Touch **OK**. The **List of EFS Volumes** dialog box appears with all the volumes of the selected storage location.
4 Touch **OK**.

Unmounting a Volume

Procedure:

1 Touch **Unmount Volume**.
2 Touch **sdcard** to list the mounted volumes on the microSD card or **internal** to list the mounted volumes on internal storage.
3 Touch **OK**.
4 Select the volume to un-mount.
5 Touch **OK**.

Deleting a Volume

Procedure:

1 If the encrypted volume is mounted, unmount it.
2 Touch **Delete Volume**.
3 Touch **sdcard** to list the unmounted volumes on the microSD card or **internal** to list the unmounted volumes on internal storage.
4 Select the volume to delete.
5 Touch **OK**.

Encrypting an SD Card

Caution: All data will be erased from the microSD card when this is performed.

Procedure:

1 Touch **Encrypt SD card**. A warning message appears.
2 Touch **Yes**. The Key List dialog box appears.
3 Select a key from the list and then touch **Ok**.

The encryption process begins and when completed, displays a successfully completed message.

Creating an EFS File

When creating an encrypted volume, the parameter information can be imported from a file instead of entering manually.

Procedure:

1 On a host computer, create a text file.

2 In the text file enter the following:

<Volume Name> <Volume Storage Type> <Key Name> <Mount Path> <Auto Mount> <Volume size>

where:

<Volume Name> = name of the volume

<Volume Storage Type> = storage location. Options: internal or sdcard.

<Key Name> = name of the key to use when creating the volume.

<Mount Path> = path where the volume will be located.

<Auto Mount> = Options: 1 = yes, 0 = no.

<Volume size> = size of the volume in Megabytes.

Example:

MyVolume sdcard key1 /mnt/sdcard/efsfolder 1 1

3 Save the text file as `efsfile`.

Off-line Extraction Tool

The Secure Storage feature allows for the usage of an encrypted file system. The off-line extraction tool allows encrypted file systems to be used on an Ubuntu version number 10.04LTS desktop. The off-line extraction tool is a shell script used to create, mount and unmount an encrypted file system used with the Secure Storage feature.

Connect the device to the host computer.

Usage

On a Ubuntu desktop, at a terminal prompt, type: `offline_extraction.sh`.

The following Main Menu appears:

```
[ Offline-extraction tool ]
1) Create an image
2) Mount an existing EFS image
3) Unmount final mount location, device mapper and loop device
4) Quit
Please, choose one from the list and press ENTER:
```

Usage

On a Ubuntu desktop, at a terminal prompt, type: `offline_extraction.sh`.

The following Main Menu appears:

```
[ Offline-extraction tool ]
1) Create an image
2) Mount an existing EFS image
3) Unmount final mount location, device mapper and loop device
4) Quit
Please, choose one from the list and press ENTER:
```

Creating an Image

Procedure:

1 From the Main Menu, select item **1**. The following appears:

```
Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>
Please enter encryption key (64-bytes hex value):
Please enter the EFS image size (in MB): <volume size in MB>
Please enter EFS image filesystem type (e.g. ext4, vfat...): ext4
DONE - OK
```

2. The utility first prompts for the name of the volume to create. Any ASCII string that meets standard Linux file naming rules is valid. Enter the image name and then press **Enter**.
3. The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
4. The utility then prompts for the image size. Enter the size of the volume in MB. A number must be entered without the units. It is understood that MB. A value of 2000, is 2 GB. Note that 4 GB is the largest volume that is supported on the device.
5. The utility lastly prompts for the filesystem type. Enter ext4 and then press **Enter**.

   The utility then creates the volume in the current working directory.

   The utility then finishes the creation process and then prompts to whether the volume should be mounted.

   ```
   Press [1] if you want to mount or press [2] if you want to exit
   ```
6. Press **1** will prompt for the mount point. For example, /mnt is prompted. Press **Enter** to mount the encrypted volume at the selected point. After mounting, an option to return to the Main Menu or Exit is provided.

   Press **2** to exit the utility without mounting.
7. If the volume is mounted on the desktop, then that volume can be provisioned with files for deployment.
8. Unmounted volumes can then be copied to the device and subsequently mounted using the Secure Storage Administrator by providing the encryption key used.

Mounting an Image

Procedure:

1. From the Main Menu, select item **2**. The following appears:

   ```
   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>
   Please enter encryption key (64-bytes hex value):
   Please enter mount path (e.g. /mnt): <existing mount point>
   DONE - OK
   ```
2. Enter the name of the volume and then press **Enter**.
3. The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
4. Enter the mount point where to connect the volume into the file system and then press **Enter**. The example of /mnt is provided.

Unmounting an Image

Procedure:

1. From the Main Menu, select item **3**. The following appears:

   ```
   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>
   DONE - OK
   ```
2. Enter the name of the volume to unmount.
3. Press **Enter**.

Chapter 6

Settings for Android Devices

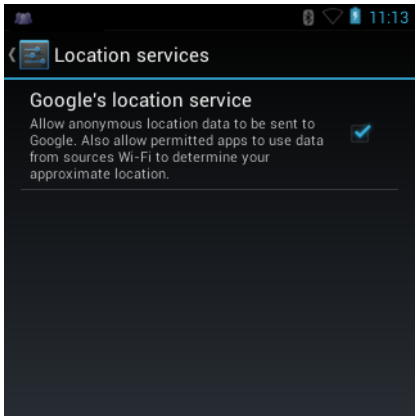
Note: This chapter applies to Android devices only.

This chapter describes settings available for configuring the device.

Location Settings

Use the **Location services** settings to set preferences for using and sharing location information. Touch > > **Location services**.

Figure 86: Location Access Screen



- **Google's location service** - Check to allow anonymous location data to be sent to Google and to allow permitted applications to use data from sources such as Wi-Fi to determine approximate location.

Screen Unlock Settings

Use the **Security settings** to set preferences for locking the screen. Touch > **Security**.

Note: Options vary depending upon the application's policy, for example, email.

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.
  - **None** - Disable screen unlock security.

- **Slide** - Slide the lock icon to unlock the screen.
- **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 108* for more information.
- **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 109* for more information.

Lock the screen to protect access to data on the device. Some email accounts require locking the screen. The Locking feature functions differently in Single-user versus Multiple-user mode.

Single User Mode

When locked, a slide, PIN or password is required to unlock the device. Press the Power button to lock the screen. The device also locks after a pre-defined time-out.

Press and release the Power button to wake the device. The Lock screen displays.

Slide up to unlock the screen.

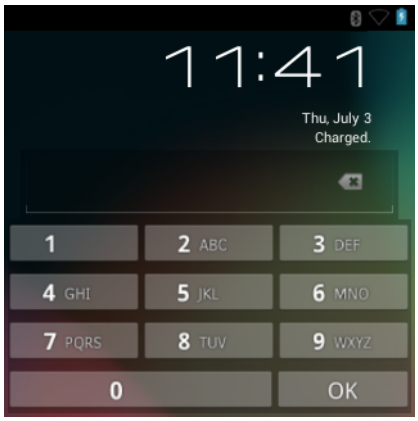
If the PIN or Password screen unlock feature is enabled, enter the PIN or password after unlocking the screen.

Set Screen Unlock Using PIN

Procedure:

1. Touch .
2. Touch .
3. Touch **Security**.
4. Touch **Screen lock**.
5. Touch **PIN**.
6. Touch in the text field.
7. Enter a PIN (between 4 and 16 characters) then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. Press . The next time the device goes into suspend mode a PIN is required upon waking.

Figure 87: PIN Screen



Set Screen Unlock Using Password

Procedure:

1 Touch .

2 Touch .

3 Touch **Security**.

4 Touch **Screen lock**.

5 Touch **Password**.

6 Touch in the text field.

7 Enter a password (between 4 and 16 characters) then touch **Next**.

8 Re-enter the password and then touch **Next**.

9 Touch . The next time the device goes into suspend mode a PIN is required upon waking.

Figure 88: Password Screen

Multiple User Mode

For Multi-user Mode configuration, see *Administrator Utilities on page 87*.

Passwords

To set the device to briefly show password characters as the user types, set this option. Touch > **Security**. Touch **Make passwords visible**. A check in the checkbox indicates that the option is enabled.

Button Remapping

The MC32N0's buttons can be programmed to perform different functions or shortcuts to installed applications.

- Trigger 1- Scan button
- Trigger 2 - Trigger button on MC32N0-G or Side Scan buttons on MC32N0-R and MC32N0-S.

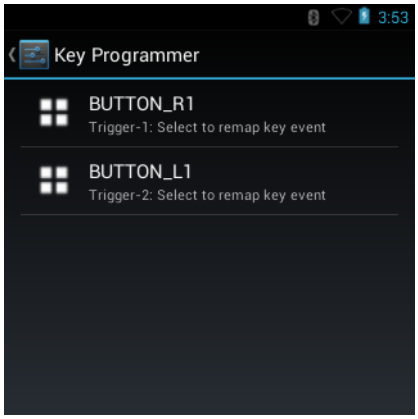
Remapping a Button

Procedure:

1 Touch  .

2 Touch **Key Programmer**.

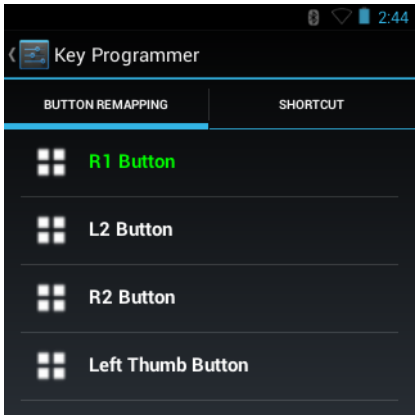
Figure 89: Key Programmer Screen



3 Select the button to remap.

4 Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.

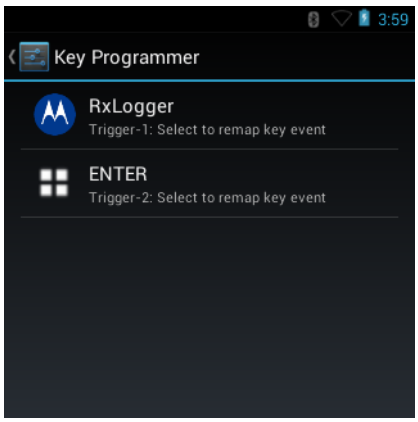
Figure 90: Button/Shortcut Selection



5 Touch a function or application shortcut to map to the button.

Note: If you select an application shortcut, the application icon appears next to the button on the **Key Programmer** screen.

Figure 91: Remapped Button



6 Press .

Exporting a Configuration File

The Button Remapping configuration can be exported to an xml file and imported into other MC32N0 devices.

Procedure:

1 Touch .

2 Touch **Key Programmer**.

3 Press .

4 Touch **Export**.
The configuration file (`key-config.xml`) is saved in the folder: `/enterprise/usr/`.

5 Copy the xml file from the folder to a host computer. See *USB Communication on page 55* for more information.

Importing a Configuration File

Procedure:

1 Copy the configuration file (`key-config.xml`) from a host computer to the root of the microSD card. See *USB Communication on page 55* for more information.

2 On the MC32N0, use **File Browser** to move the file from the root of the microSD card to the `/enterprise/usr` folder.

3 Touch .

4 Touch **Key Programmer**.

5 TouchPress .

6 Touch **Import**.

Creating a Remap File

The administrator can create an xml configuration file and import it into any MC32N0 device. Use any text editor to create the xml file with the filename: `key-config.xml`.

```
<?xml version="1.0" encoding="UTF-8"?>
<Button_Remap>
     <trigger_1 mode="Remap Button">
          <REMAP_CODE>BUTTON_L1</REMAP_CODE>
          <EXTRA_SHORTCUT>MPA3_TRIGGER_1</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
     </trigger_1>
     <trigger_2 mode="Remap Button">
          <REMAP_CODE>BUTTON_R1</REMAP_CODE>
          <EXTRA_SHORTCUT>MPA3_TRIGGER_2</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
     </trigger_2>
     <trigger_3 mode="Remap Button">
          <REMAP_CODE>VOLUME_UP</REMAP_CODE>
          <EXTRA_SHORTCUT>MPA3_TRIGGER_3</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
     </trigger_3>
     <trigger_4 mode="Remap Button">
          <REMAP_CODE>VOLUME_DOWN</REMAP_CODE>
     <EXTRA_SHORTCUT>MPA3_TRIGGER_4</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
     </trigger_4>
     <trigger_5 mode="Shortcut">
          <REMAP_CODE>BUTTON_R2</REMAP_CODE>
          <EXTRA_SHORTCUT>MPA3_TRIGGER_5</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
          </EXTRA_PACKAGE_NAME>
     </trigger_5>
     <search_key mode="Remap Button">
          <REMAP_CODE>NONE</REMAP_CODE>
          <EXTRA_SHORTCUT>SEARCH_KEY</EXTRA_SHORTCUT>
          <EXTRA_TITLE/>
          <EXTRA_PACKAGE_NAME/>
     </search_key>
     <headset mode="Remap Button">
          <REMAP_CODE>NONE</REMAP_CODE>
     </headset>
</Button_Remap>
```

Replace the options for each trigger. See *Keypad Remap Strings on page 179* for a list of available button functions.

Enterprise Reset

To ensure that the configuration persists after an Enterprise Reset:

1. Export the settings before an Enterprise Reset and then import the settings after an Enterprise Reset or

2. Push the configuration file using a MSP or a third-party MDM to the `/enterprise/device/settings/keypad/` folder before the Enterprise Reset. After the Enterprise Reset the key configuration will be automatically applied from this file.

Two ways to persist the settings:

1. Export the settings before Enterprise Reset, and Import the same after Enterprise Reset.

2. Copy the `key-config.xml` file to folder `/enterprise/device/settings/keypad/` before the Enterprise Reset. After the Enterprise Reset the key configuration will be automatically applied from this file.

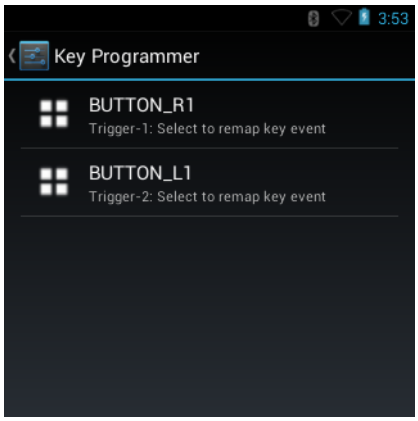
Enable Key Wakeup

Procedure:

1 Touch  .

2 Touch **Key Programmer**.

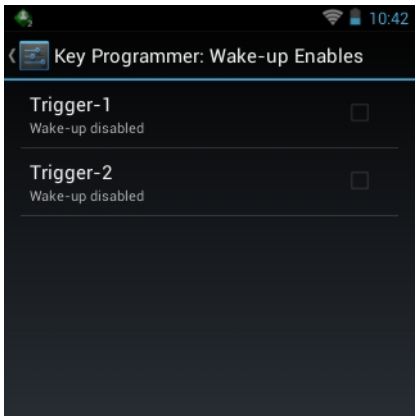
Figure 92: Key Programmer Screen



3 Touch  .

4 Touch **Wake-up enables**.

Figure 93: Wake-up Enables



5 Touch the checkbox next to the key to enable wake up.

On the MC32N0–G, **Trigger-1** is the scan key and **Trigger-2** is the Triger.

On the MC32N0–R/S, **Trigger-1** is the scan key and **Trigger-2** is the right and left scan butons.

6 Press  .

Accounts

Use the **Accounts** to add, remove, and manage accounts. Use these settings to control how applications send, receive, and sync data on their own schedules, and whether applications can synchronize user data automatically.

Applications may also have their own settings to control how they synchronize data; see the documentation for those applications for details.

Language Usage

Use the **Language & input** settings to change the language that display for the text and including words added to its dictionary.

Changing the Language Setting

Procedure:

1 Touch **Language**.
2 In the **Language** screen, select a language from the list of available languages.

The operating system text changes to the selected language.

Adding Words to the Dictionary

Procedure:

1 In the **Language & input** screen, touch **Personal dictionary**.
2 Touch + to add a new word or phrase to the dictionary.
3 In the **Phrase** text box, enter the word or phrase.
4 In the **Shortcut** text box, enter a shortcut for the word or phrase.
5 In the **Language** drop-down list, select the language that this word or phase is stored.
6 Touch **Add to dictionary** in the top left corner of the screen to add the new word.

Keyboard Settings

Use the **Language & input** settings for configuring the on-screen keyboards. The device contains the following keyboard settings:

- Android Keyboard
- Chinese keyboard

About Device

Use **About device** settings to view information about the MC32N0. Touch  > **About device**.

- **Status** - Touch to display the following:
  - **Battery status** - Indicates if the battery is charging (on AC power) or discharging (on battery power).
  - **Battery level** - Indicates the battery charge level.

  - **IP address** - Displays the IP address of the device.
  - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
  - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
  - **Serial number** - Displays the serial number of the device.
  - **Up time** - Displays the time that the MC32N0 has been running since being turned on.
- **Battery information** - Displays information about the battery.
- **Hardware config** - Lists part number for various hardware on the MC32N0.
- **Legal information** - Opens a screen to view legal information about the software included on the MC32N0.
- **Model number** - Displays the devices model number.
- **EA Version** - Displays the EA firmware version.
- **SSPAM** - Displays SSPAM firmware version.
- **Serial number** - Displays the device serial number.
- **Build Tag** - Displays the build name.
- **Android version** - Displays the operating system version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

Chapter 7

Application Deployment for Android Devices

This chapter describes features in Android including new security features, how to package applications, and procedures for deploying applications onto the device.

Security

The device implements a set of security policies that determine whether an application is allowed to run and, if allowed, with what level of trust. To develop an application, you must know the security configuration of the device, and how to sign an application with the appropriate certificate to allow the application to run (and to run with the needed level of trust).

Secure Certificates

If the VPN or Wi-Fi networks rely on secure certificates, obtain the certificates and store them in the device's secure credential storage, before configuring access to the VPN or Wi-Fi networks.

If downloading the certificates from a web site, set a password for the credential storage. The device supports X.509 certificates saved in PKCS#12 key store files with a .p12 extension (if key store has a .pfx or other extension, change to .p12).

The device also installs any accompanying private key or certificate authority certificates contained in the key store.

Installing a Secure Certificate

Procedure:

1. Touch  .
2. Touch **Security**.
3. Navigate to the location of the certificate file.
4. Touch the filename of the certificate to install. Only the names of certificates not already installed display.
5. If prompted, enter the certificate's password and touch **OK**.
6. Enter a name for the certificate and touch **OK**. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

Configuring Credential Storage Settings

Procedure:

1. Touch  .
2. Touch **Security**.

- **Trusted credentials** - Touch to display the trusted system and user credentials.
- **Clear credentials** - Deletes all secure certificates and related credentials.

Development Tools

Android development tools are available at *http://developer.android.com*.

To start developing applications for the device, download the development SDK and the Eclipse IDE. Development can take place on a Microsoft® Windows®, Mac® OS X®, or Linux® operating system.

Applications are written in the Java language, but compiled and executed in the Dalvik VM (a non-Java virtual machine). Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

The development SDK is distributed as a ZIP file that unpacks to a directory on the host computer hard drive. The SDK includes:

- android.jar
  - Java archive file containing all of the development SDK classes necessary to build an application.
- documention.html and docs directory
  - The SDK documentation is provided locally and on the Web. It's largely in the form of JavaDocs, making it easy to navigate the many packages in the SDK. The documentation also includes a high-level Development Guide and links to the broader community.
- Samples directory
  - The samples subdirectory contains full source code for a variety of applications, including ApiDemo, which exercises many APIs. The sample application is a great place to explore when starting application development.
- Tools directory
  - Contains all of the command-line tools to build applications. The most commonly employed and useful tool is the adb utility.
- usb_driver
  - Directory containing the necessary drivers to connect the development environment to an enabled device. These files are only required for developers using the Windows platform.

Open the **Developer options** screen to set development related settings.

On the Home screen, touch  >  > { } **Developer options**. Slide the switch to the **ON** position to enable developer options.

ADB USB Setup

To use the ADB, install the USB driver. This assumes that the development SDK has been installed on the host computer. Go to *http://developer.android.com/sdk/index.html* for details on setting up the development SDK.

ADB driver for Windows and Linux are available on the Zebra web site. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

Application Installation

After an application is developed, install the application onto the device using one of the following methods:

- USB connection, see *Installing Applications Using the USB Connection on page 119*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 119*.
- microSD Card, see *Installing Applications Using a microSD Card on page 120*
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

Installing Applications Using the USB Connection

Caution:

When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 55*.

2 On the host computer, copy the application `.apk` file from the host computer to the device.

3 Disconnect the device from the host computer. See *USB Communication on page 55*.

4 On the device, touch .

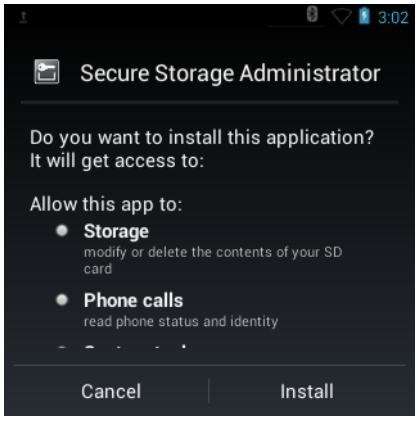
5 Touch to view files on a microSD card or Internal Storage.

6 Locate the application `.apk` file.

7 Touch the application file to begin the installation process.

8 To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.

Figure 94: Accept Installation Screen



9 Touch **Open** to open the application or **Close** to exit the installation process. The application appears in the App list.

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

Caution:

When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Prerequisites: Ensure that the ADB drivers are installed on the host computer. See *ADB USB Setup on page 118*.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 55*.

2 Touch  .

3 Touch { } **Developer options**.

4 Slide the switch to the **ON** position.

5 Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

6 Touch **OK**.

7 On the host computer, open a command prompt window and use the adb command:

`adb install <application>`

where: <application> = the path and filename of the apk file.

8 Disconnect the device from the host computer. See *USB Communication on page 55*.

Installing Applications Using a microSD Card

Caution:

When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 55*.

2 Copy the application `.apk` file from the host computer to the microSD card.

3 Remove the microSD card from the host computer.

4 Press and hold the Power button until the menu appears.

5 Touch **Power off**.

6 If hand strap is attached, slide the hand strap clip up toward the top of the device and then lift.

7 Press the two battery latches in.

8 Lift the battery from the device.

9 Lift the access door.

10 Insert the microSD card.

11 Replace the access door.

12 Insert the battery, bottom first, into the battery compartment in the back of the device.

13 Press the battery down until the battery release latch snaps into place.

14 Replace the hand strap, if required.

15 Press and hold the Power button to turn on the device.

16 Touch  .

17 **Note:**

In **File Browser**, the microSD card path is `/sdcard` or `/storage/sdcard1`.

Touch  to view files on the microSD card.

18 Locate the application `.apk` file.

19 Touch the application file to begin the installation process.

20 To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.

21 Touch **Open** to open the application or **Close** to exit the installation process. The application appears in the App list.

Uninstalling an Application

Procedure:

1 Touch  .

2 Touch  **Apps**.

3 Swipe left or right until the **Downloaded** screen displays.

Figure 95: Downloaded Screen

4 Touch the application to uninstall.

5 Touch **Uninstall**.

6 Touch **OK** to confirm.

Updating the MC32N0 System

System Update packages can contain either partial or complete updates for the operating system. Zebra distributes the System Update packages on the Zebra web site.

Procedure:

1 Download the system update package:

a Go to the Zebra Support web site, at http://www.zebra.com/support.

b Download the appropriate System Update package to a host computer.

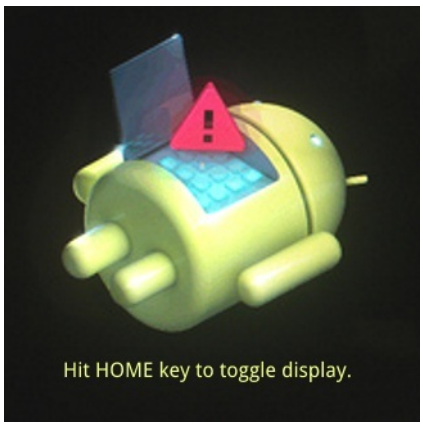
2 Copy the `MC32N0JxxRUyyzzzzz.zip` file to the root directory of the microSD card. See *USB Communication on page 55* for more information.

3 Press and hold the Power button until the menu appears.

4 Touch **Reset**.

5 On the MC32N0-G, press and hold the Trigger button or on the MC32N0–R/S, press and hold the right Scan button..

Figure 96: Recovery Screen



6 Press .

Figure 97: System Recovery Screen

7 Use the navigation keys to navigate to the **apply update from /sdcard** option.

8 Press the Enter button.

9 Use the navigation keys to navigate to the `MC32N0JxxRUyyzzzzz.zip` file .

10 Press the Enter key. The System Update installs and then the MC32N0 resets.

Storage

The device contains four types of file storage:

- Random Access Memory (RAM)
- External storage (microSD card)
- Internal storage
- Enterprise folder.

Random Access Memory

Executing programs use RAM to store data. Data stored in RAM is lost upon a reset.

The operating system manages how applications use RAM. It only allows applications and component processes and services to use RAM when required. It may cache recently used processes in RAM, so they restart more quickly when opened again, but it will erase the cache if it needs the RAM for new activities.

To view the amount of free and used memory, touch > **Apps**. Swipe the screen until the **Running** screen appears.

Figure 98: Running Screen

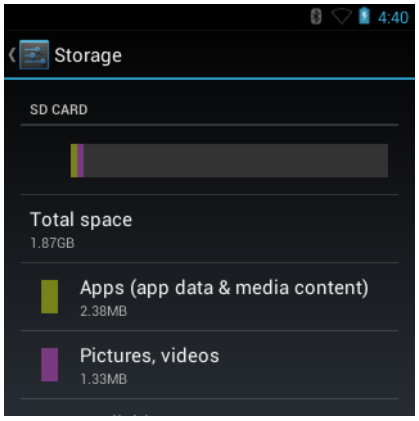
The bar at the bottom of the screen displays the amount of used and free RAM.

External Storage

The MC32N0 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the MC32N0 is connected to a host computer. Some applications are designed to be stored on the microSD card rather than in internal memory.

To view the used and available space on the microSD card, touch > > **Storage**.

Figure 99: Storage Settings



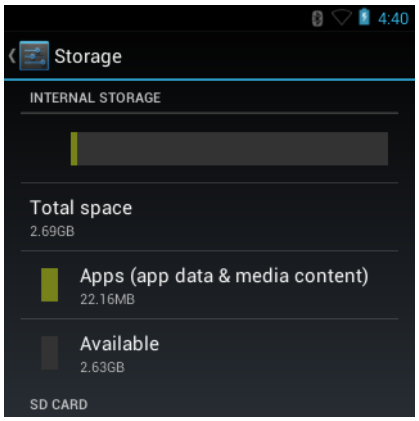
- **Total space** - Displays the total amount of space on the installed microSD card.
- **Apps** - Displays the available space used for applications and media content on the installed microSD card.
- **Pictures, videos** - Displays the available space used for pictures and videos on the installed microSD card.
- **Available** - Displays the available space on the installed microSD card.
- **Unmount SD card** - Unmounts the installed microSD card from the MC32N0 so that it can be safely removed. This setting is dimmed if there is no microSD card installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase external SD card** - Permanently erases everything on the installed microSD card.

Internal Storage

The MC32N0 has internal storage. The internal storage content can be viewed and files copied to and from when the MC32N0 is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

To view the used and available space on the internal storage, touch > > **Storage**.

Figure 100: Internal Storage Screen



- **Internal Storage**
  - **Total space** - Displays the total amount of space on internal storage (approximately 1.0 GB).
    - **Apps** - Displays the available space used for applications and media content on internal storage.
    - **Available** - Displays the available space on internal storage.

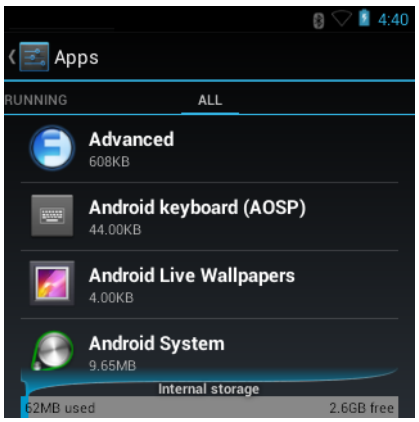
Enterprise Folder

The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 MB (formatted). Applications can persist data after an Enterprise Reset by saving data to the enterprise/user folder. The folder is ext4 formatted and is only accessible from a host computer using ADB or from an MDM.

Application Management

Applications use two kinds of memory: storage memory and RAM. Applications use storage memory for themselves and any files, settings, and other data they use. They also use RAM when they are running.

Figure 101: Manage Applications Screen



The **Manage Applications** screen has four tabs, with lists of applications and their components in each. At the bottom of each tab is a graph of the memory used by the items in the list and amount of free memory.

Touch an application, process, or service in a list to open a screen with details about it and, depending on the item, to change its settings, stop it or uninstall it

- Slide the screen to the **Downloaded** tab to view the applications downloaded to the device.
- Slide the screen to the **All** tab to view all the applications installed on the device, including factory installed applications and downloaded applications.
- Slide the screen to the **On SD card** tab to view the applications installed on the microSD card. A check mark indicates that the application is installed on the microSD card. Unchecked items are installed in internal storage and can be moved to the microSD card.
- Touch the **Running** tab to view the applications and their processes and services that are running or cached

When on the **Downloaded**, **All**, or **On SD card** tab, press > **Sort by size** to switch the order of the list.

Viewing Application Details

Applications have different kinds of information and controls, but commonly include:

- Touch **Force stop** to stop an application.
- Touch **Uninstall** to remove the application and all of its data and settings from the device. See *Uninstalling an Application on page 121* for information about uninstalling applications.
- Touch **Clear data** to delete an application's settings and associated data.
- Touch **Move to USB storage** or **Move to SD card** to change where some applications are stored.
- Cache If the application stores data in a temporary area, lists how much information is stored, and includes a button for clearing it.
- **Launch by default** clears If you have configured an application to launch certain file types by default, you can clear that setting here.
- **Permissions** lists the areas on the device that the application has access to.

Procedure:

1. Press > **Manage apps**.
2. Touch an application, process, or service.

   The **App Info** screen lists the application name and version number, and details about the application. Depending on the application and where it came from, it may also include buttons for managing the application's data, forcing the application to stop, and uninstalling the application. It also lists details about the kinds of information about your phone and data that the application has access to.

Stopping an Application

To monitor how much RAM running applications and cached processes are using and if necessary, stop them.

Procedure:

1 Press > **Manage apps**.

2 Swipe the screen to display the **Running** tab.

3 Touch **Show cached processes** or **Show running services** to switch back and forth. The **Running** tab lists the applications, processes, and services that are currently running or that have cached processes and how much RAM they are using.

Figure 102: Running Applications

4 The graph at the bottom of the screen displays the total RAM in use and the amount free. Touch an application, process, or service.

5 **Note:** Stopping an application or operating system processes and services disables one or more dependant functions on the device. The device may need to be reset to restore full functionality.

Touch **Stop**.

Changing Application Location

Some applications are designed to be stored on a microSD card, rather than in internal storage. Others are designed so you can change where they are stored. You may find it helpful to move large applications off of your internal storage, to make more room for other applications that don't offer the option. Many large applications are designed this way for exactly this reason.

Procedure:

1 Press > **Manage apps**.

2 Swipe the screen to display the **On SD card** tab.

The tab lists the applications that must be or can be stored on the microSD card. Each application lists the amount of storage it uses on internal storage (even when not stored there, all applications use at least a small amount of internal storage).

Applications that are stored on the microSD card are checked.

The graph at the bottom shows the amount of memory used and free of the microSD card: the total includes files and other data, not just the applications in the list.

3 Touch an application in the list.

The Storage section of the application's details screen shows details about the memory used by the application. If the application can be moved, the Move button is active.

4 Touch **Move to SD card** to move the bulk of the application from the device's internal storage to the microSD card.

5 Touch **Move to device** to move the application back to the device's internal storage.

Managing Downloads

Files and applications downloaded using the Browser or Email are stored on the microSD card in the Download directory. Use the **Downloads** application to view, open, or delete downloaded items.

Procedure:

1 Touch  .

2 Touch  .

3 Touch an item to open it.

4 Touch headings for earlier downloads to view them.

5 Check items to delete; then touch  . The item is deleted from storage.

6 Touch **Sort by size** or **Sort by time** to switch back and forth.

When an application is opened, the other applications being used do not stop. The operating system and applications work together to ensure that applications not being used do not consume resources unnecessarily, stopping and starting them as needed. For this reason, there's no need to stop applications unless it is not functioning properly.

Chapter 8

Synchronization

Note: Applies to WinCE devices only.

Synchronization lets the user manage information between an MC32N0 and a host computer so that changes made either on the MC32N0 or on the host computer appear in both places. Download and install synchronization software to the host computer (either Microsoft ActiveSync for Windows XP or Windows Mobile Device Center (WMDC) for Windows Vista and Windows 7) in order to use the sync feature. Visit www.microsoft.com on the host computer for details.

The synchronization software:

- Allows working with MC32N0-compatible host applications on the host computer. The sync software replicates data from the MC32N0 so the host application can view, enter, and modify data on the host computer.
- Synchronizes files between the MC32N0 and host computer, converting the files to the correct format.
- Backs up the data stored on the MC32N0. Synchronization is a one-step procedure that ensures the data is always safe and up-to-date.
- Copies (rather than synchronizes) files between the MC32N0 and host computer.
- Controls when synchronization occurs by selecting a synchronization mode, e.g., set to synchronize continually while the MC32N0 is connected to the host computer, or set to only synchronize on command.
- Selects the types of information to synchronize and control how much data is synchronized.

Installing the Sync Software

To download and install either Microsoft ActiveSync (for Windows XP) or WMDC (for Windows Vista and Windows 7), visit www.microsoft.com and follow the instructions provided.

Mobile Computer Setup

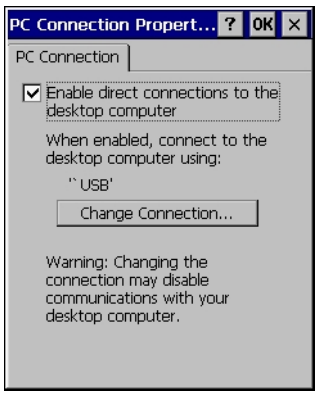
Note: Microsoft recommends installing synchronization software on the host computer before connecting the mobile computer.

The MC32N0 can be set up to communicate with a USB connection. The MC32N0 communication settings must be set to match the communication settings used with ActiveSync or WMDC.

Procedure:

1 On the MC32N0 touch **Start** > **Settings** > **Control Panel** > **PC Connection** icon. The **PC Connection Properties** window appears.

Figure 103: PC Connection Properties Window



2 Touch the **Change Connection** button.

3 Select the connection type from the drop-down list.

4 Touch **OK** to exit the **Change Connection** window and touch **OK** to exit the **PC Connection Properties** window.

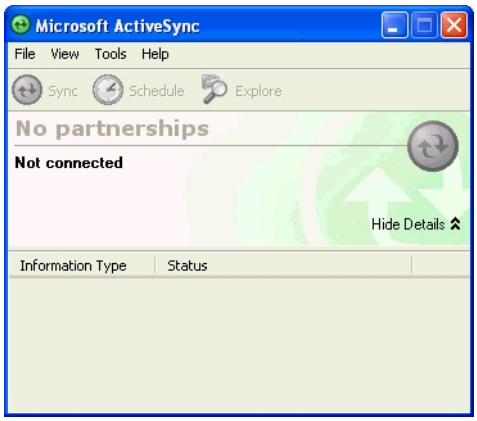
5 Proceed with installing ActiveSync or WMDC on the host computer and setting up a partnership.

Setting Up a Connection Using ActiveSync

Procedure:

1 Select **Start** > **Programs** > **Microsoft ActiveSync** on the host computer. The **ActiveSync Window** displays.

Figure 104: ActiveSync Window



2 **Note:** Assign each MC32N0 a unique device name. Do not try to synchronize more than one MC32N0 to the same name.

In the ActiveSync window, select **File** > **Connection Settings**. The **Connection Settings** window appears.

Figure 105: Connection Settings Window

3 Select **Allow USB connections** check box.

4 Select the **Show status icon** in **Taskbar** check box.

5 Select **OK** to save any changes made.

Setting Up a Connection Using WMDC

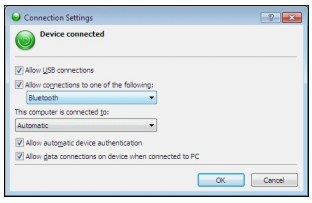
Procedure:

1 Select **Start** > **All Programs** > **Windows Mobile Device Center** on the host computer. The **Windows Mobile Device Center** displays.

Figure 106: Windows Mobile Device Center Window

2 In the WMDC window, under **Mobile Device Settings**, click **Connection settings**.

Figure 107: Connection Settings Window



3 Select **Allow USB connections** and adjust any additional settings as needed.

4 Select **OK** to save any changes made.

Setting up a Partnership

Procedure:

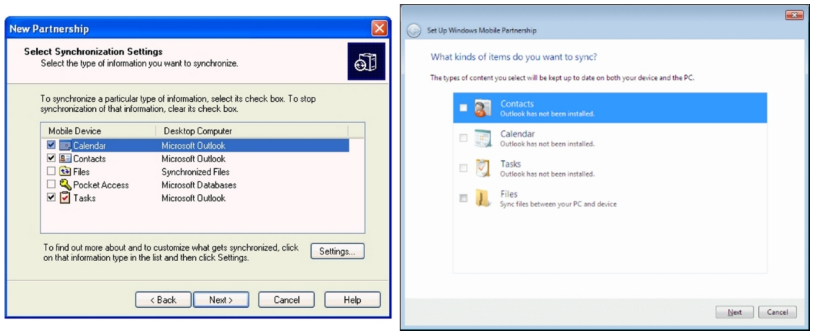
1 If the **Get Connected** window does not appear on the host computer, select **Start** > **All Programs** > **Microsoft ActiveSync**.

Figure 108: New Partnership Window

2 Select if you want to create synchronize with the host computer or to connect as a guest.

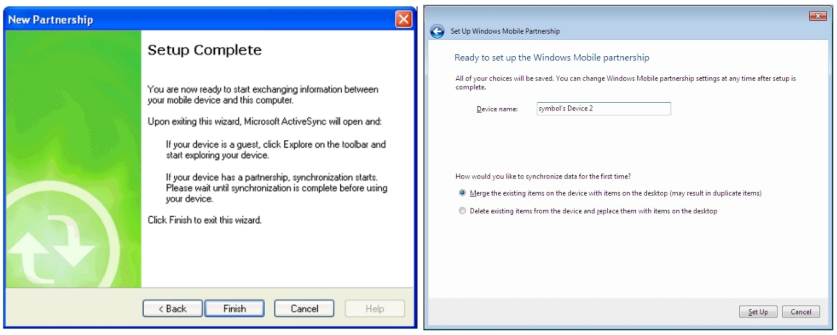
3 Click **Next**.

Figure 109: Select Synchronization Setting Window



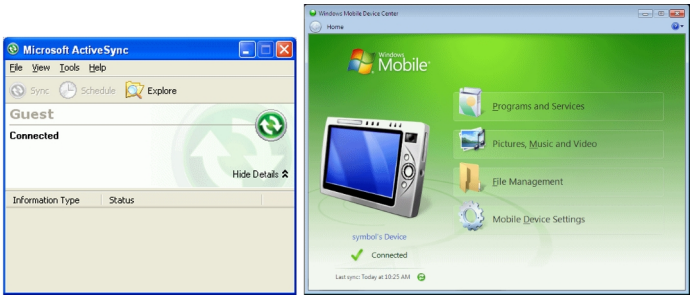
4 Select the appropriate settings and click **Next**.

Figure 110: Setup Complete Window



5 Click **Finish** or **Setup**.

Figure 111: Connected Window



During the first synchronization, information stored on the MC32N0 is copied to the host computer. When the copy is complete and all data is synchronized, the MC32N0 can be disconnect from the host computer.

Note: The first synchronization operation must be performed with a local direct connection. To retain partnerships after a cold boot, capture partnership registry information in a .reg file and save it in the Flash File System, detailed information is provided in the EMDK Windows CE Help File for the MC32N0.

For more information about using ActiveSync or WMDC, start the application on the host computer, then see Help.

Chapter 9

Settings for WinCE Devices

This chapter describes settings available for configuring the device.

Interactive Sensor Technology Configuration

This chapter provides information for configuring the Interactive Sensor Technology (IST) settings. IST settings can be accessed:

Tap **Start** > **Settings** > **System** > **IST Settings** icon.

Display Tab

Use the **Display** tab configure display interaction settings.

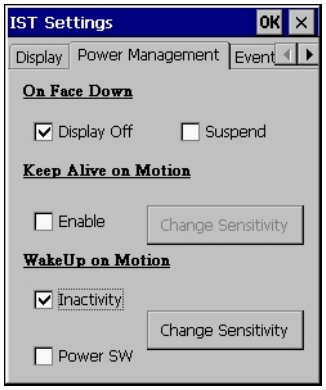
Figure 112: Display Tab

The Auto Orientation parameter controls the display rotation according to the MC32N0 orientation. Select the **Auto Orientation** checkbox to enable this feature. Auto orientation is disabled by default.

Power Management Tab

Use the **Power Management** tab to configure power management settings.

Figure 113: Power Management Tab



On Face Down

The **On Face Down** section provides configurable options to control what happens when the MC32N0 is placed with the display face down.

Select the **Display Off** checkbox to turn off the backlight when the MC32N0 is placed face-down. The backlight automatically powers on when the MC32N0 is tuned face-up.

Select the **Suspend** checkbox to suspend the MC32N0 when it placed face-down. To wake the MC32N0 use the controls listed in the **Wake Up on Motion** section below.

Keep Alive On Motion

Select the **Enabled** checkbox to prevent the MC32N0 from going into suspend mode while it is in motion. The motion sensitivity is configurable. To set the sensitivity, tap the **Change Sensitivity…** button.

Note: Select the Enabled checkbox to prevent the MC32N0 from going into suspend mode while it is in motion. The motion sensitivity is configurable. To set the sensitivity, tap the Change Sensitivity… button.

Wake Up on Motion

The **Wake Up on Motion** section provides configurable options for waking the MC32N0 from suspend mode by shaking the MC32N0.

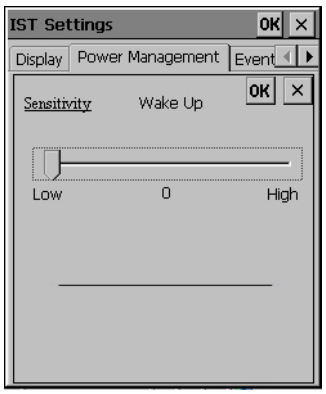
Select **Inactivity** checkbox to allow IST to wake the MC32N0 when it was suspended due to inactivity.

Use the **Change Sensitivity…** button to configure the sensitivity settings.

Setting Sensitivity

Use the slider to set the sensitivity. A low setting indicates that a harder shake (faster movement) is required for the IST to initiate a wake up action. The sensitivity can be set from “0” to “10” and when the sensitivity is set to lower values a simple shake/motion can be detected by IST. A high setting allows IST to issue a wake up action when an easier movement to the MC32N0 is detected. Shake the MC32N0 to test the set sensitivity. An audio sound is heard and a message is displayed on screen when the shaking level reaches the set sensitivity level.

Figure 114: Set IST Sensitivity Window



Events Tab

Use the **Event** tab to display the event details. This feature in IST mainly focuses on abuse by dropping the device.

Figure 115: Events Tab

Use the Audible Notification panel to enable playing of a wave file when the MC32N0 is dropped. Select a desired .wav file from the Sounds: drop-down list.

Sensors Tab

Use the **Sensors** tab to display the list of sensors available in IST :

- Orientation
- Motion
- Accelerometer
- Tilt Angle.

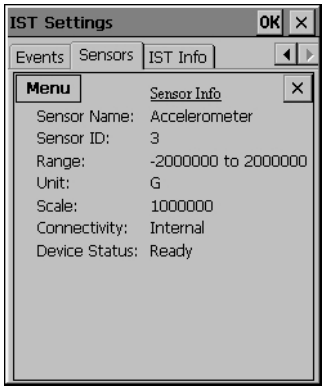
Figure 116: Sensors Tab

Tap on each sensor to view the **Sensor Info**.

Sensor Info

The **Sensor Info** list displays the name, ID, range, unit, scale, connectivity and status of the sensor.

Figure 117: Sensor Info Window



Tap **Menu** to select **VisualizeView** or **GraphView** for the sensor.

Figure 118: VisualizeView Window

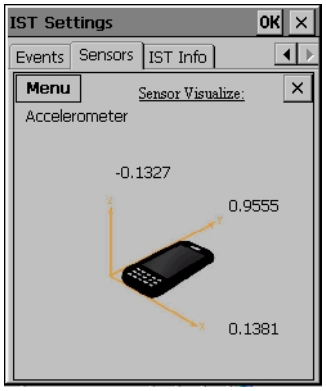
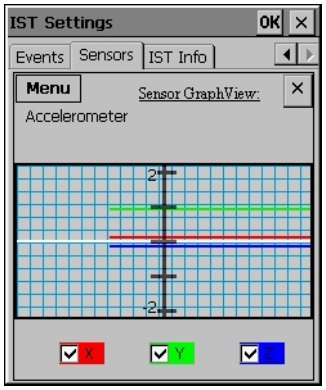


Figure 119: GraphView Window



IST Info

Use the **IST Info** tab to view IST software information.

Figure 120: IST Info Tab

Table 9: IST Info Tab Information

Item	Description
CPL Ver	Displays the version information of IST control panel.
API Ver	Displays the version information of IST application programming interface.
Service Ver	Displays the version information of IST service.
Driver Ver	Displays the version information of IST driver.
HAL Ver	Displays the version information of IST hardware abstraction layer.
Firmware Ver	Displays the version information of IST device firmware.

Wakeup Conditions

The wakeup conditions define what actions wake up the mobile computer after it has gone into suspend mode. The mobile computer can go into suspend mode by either pressing the Power button or automatically by Control Panel time-out settings. These settings are configurable and the factory default settings are shown in the table below.

To access the Wakeup settings touch **Start** > **Settings** > **Control Panel** > **Power** icon > **Wakeup** tab.

Figure 121: Power Settings – Wakeup Tab

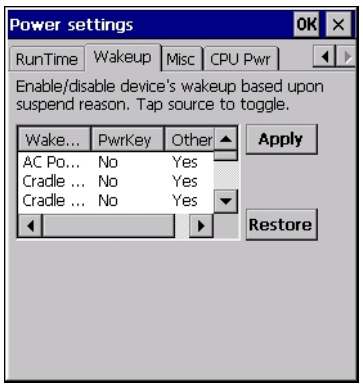


Table 10: Wakeup Default Settings

Condition for Wakeup	Power Button	Automatic Time-out
AC power is applied.	No	Yes
Mobile computer is inserted into a cradle.	No	Yes
Mobile computer is removed from a cradle.	No	Yes
Mobile computer is connected to a USB device.	No	Yes
Mobile computer is disconnected from a USB device.	No	Yes
A key is pressed.	No	Yes
The scan triggered is pressed.	No	Yes
The screen is touched.	No	No
Wireless LAN activity is detected.	No	No
USB Host	No	No
On Motion	Yes	Yes
Bluetooth	Yes	Yes

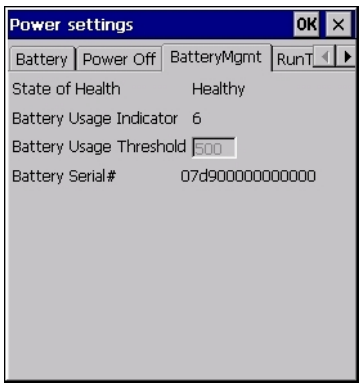
Battery Usage Threshold Setting

By default the Battery Usage Threshold value is set to a pre-defined value (400 by default). To change the threshold value, a registry key must be created to allow changing this value.

A battery becomes unhealthy when the Battery Usage Indication reach a predefined threshold (end of usable life).

Note: The point at which a battery becomes unhealthy may vary depending upon the environment and charging conditions.

Figure 122: Power BatteryMgmt Tab



Registry Setting

Create the following registry key:

```
[HKEY_LOCAL_MACHINE\ControlPanel\Power]
```

```
"EnableCycleCntThresholdEdit"=DWORD:0
```

where:

- dword:0 = Enable threshold change

Warm boot the device to have the registry setting take effect.

Changing Threshold Value

1 Tap **Start** > **Settings** > **Power** > **BatteryMgmt** tab.

Figure 123: BatteryMgmt Tab with Threshold Change Checkbox

2 In the **Battery Usage Threshold** text box, enter a new value.
3 Select the **Check to change the Battery Age Threshold to read only field** checkbox.
4 Tap **Apply**.
5 Tap **ok**. The new value is set and then the registry key is deleted.

Bluetooth Configuration Setting

The MC32N0 supports both the Microsoft Bluetooth stack and the StoneStreet One Bluetooth stack. Only one Bluetooth stack can be used at a time. By default, the Microsoft Bluetooth stack is enabled. A registry key on the MC32N0 can be modified to disable the Microsoft stack and enable the StoneStreet One stack.

Registry Setting

Using a registry editor, navigate to the following:

```
[HKEY_LOCAL_MACHINE\Software\SymbolBluetooth]
```

Edit the following key:

```
"SSStack"=dword:1
```

where:

- 0 = enable Microsoft stack and disable StoneStreet One stack (default)
- 1 = enable StoneStreet One stack and disable Microsoft stack

After setting the registry key, warm boot the MC32N0.

Sample Applications and StartUpCtl Configuration

The MC32N0 with Windows CE 7.0 contains a set of sample applications that can be installed on the device. As part of the installation, an application called StartUpCtl is also installed.

On the desktop, double-tap the **Install Samples** icon.

The Sample Applications and StartUpCtl application installs on the device and the Sample Applications window appears.

After a warm or cold boot, the **Sample Applications** window appears automatically.

StartUpCtl Application Configuration

StartUpCtl application can be used to automatically launch any application whenever a warm or cold boot is performed.

Refer to the StartUpCtl instruction available with the StartUpCtl software download available on the Support Central web site: http//www.zebra.com/support.

Removing Sample Applications and StartUpCtl Application

To remove the installed applications (before a cold boot is performed):

1. Tap **Start** > **Setting** > **Control Panel** > **Remove Programs** icon.
2. Select **Motorola Samples.C** from the list.
3. Tap the **Remove** button.
4. Tap the **Yes** button.
5. Select **Motorola startUpCtl** from the list.
6. Tap the **Remove** button.
7. Tap the **Yes** button.
8. Tap **OK**.

To remove the installed applications (after a cold boot is performed):

1. Tap **Start** > **Programs** > **Windows Explorer**.
2. Open the `Application` folder.
3. Delete the `Sample.C` folder and its contents.
4. Delete the `StartUpCtl` folder and its contents.
5. Delete the `Samples.C` file.
6. Open the `StartUp` folder.
7. Delete the `StartUpCtl` file.

After a cold boot the **Install Samples** icon appears on the desktop.

Chapter 10

Application Deployment for Windows CE

This chapter describes new features in Windows CE 6.0 including how to package applications, and procedures for deploying applications onto the MC32N0.

Application Design Considerations

To ensure application compatibility of a 320 x 320 display in Windows Mobile, some applications will need to be recompiled with the Microsoft WM6 SDK.

Software Installation on Development PC

To develop applications to run on the mobile computer, use one or both of the following:

- Microsoft Windows XP (32-bit) or Microsoft Windows Vista (32-bit) or Microsoft Windows 7 (32-bit and 64-bit).
- One of the following device sync components:
  - Microsoft ActiveSync 4.5 or higher for Windows XP
  - Microsoft® Mobile Device Center pre-installed with Windows Vista
  - Microsoft® Windows Mobile Device Center 6.1 or higher for Windows 7.
- Install one or more of the following:
  - Microsoft® Visual Studio 2005 with Service Pack 1
  - Microsoft® Visual Studio 2008 with Service Pack 1
- Enterprise Mobility Developer Kit (EMDK) for C
  - The EMDK for C is a development tool used to create native C and C++ applications for all Zebra devices. It includes documentation, header files (.H), and library files (.LIB) for native code application development that targets Zebra value-add APIs.
- Platform Software Developer Kit (Platform SDK) for MC32N0
  - The Platform SDK for MC32N0 is used in conjunction with the EMDK for C to create Windows CE applications for the wearable terminal. The Platform SDK installs a new Windows CE device type and its associated libraries onto the development PC.

Platform SDK

To download and install the appropriate Platform SDK:

1. Download the appropriate Platform SDK from the Support Central web site, http://www.zebra.com/support.
   a. Select MC32N0. The MC32N0 Product page displays.
   b. On the MC32N0 Product page, select the appropriate Platform SDK for MC32N0 from the Software Downloads section. The Platform SDK page displays.
   c. Save the .exe file to the development computer.
2. Run the file and follow the screen prompts to install.

EMDK for C

To download and install the EMDK for C:

1. Download the EMDK from the Support Central web site, http://www.zebra.com/support.
   a. Select MC32N0. The MC32N0 Product page displays.
   b. On the MC32N0 Product page, select the appropriate Enterprise Mobility Developer Kit for C from the Software Downloads section. The Enterprise Mobility Developer Kit for C page displays.
   c. Select the latest version, and save the .exe file to the development computer.
2. Locate the .exe file on the development computer, double-click the executable file and follow the install screen prompts.
3. Once installed, access the components of the EMDK for C from the Enterprise Mobility Developer Kit for C program group of the Windows Start menu.
4. The sample applications provide examples of how to interface with the Zebra API functions. To build a sample application, open the Samples folder from the Windows Start menu. Open the folder for the desired sample and then open the project file. The project file has an extension of VCP. Microsoft Visual C++ v4.0 automatically launches. Select WinCE as the Active WCE Configuration. Select Win32 (WCE ARMV4) Debug as the active configuration.

Installing Other Development Software

Developing applications for the MC32N0 may require installing other development software, such as application development environments, on the development PC. Follow the installation instructions provided with the software.

Software Updates

Download updates to the EMDK for C from the Support Central web site at: http://www.zebra.com/support. Check this site periodically for important updates and new software versions.

Windows CE Flash Storage

In addition to the RAM-based storage standard on Windows CE, the MC32N0 is also equipped with a non-volatile Flash-based storage area which can store data (partitions) that can not be corrupted by a cold boot. This Flash area is divided into two categories: Flash File System (FFS) Partitions and Non-FFS Partitions.

FFS Partitions

The MC32N0 includes two FFS partitions. These partitions appear to the MC32N0 as a hard drive that the OS file system can write files to and read files from. Data is retained even if power is removed.

The two FFS partitions appear as two separate folders in the Windows CE file system and are as follows:

- Platform: The Platform FFS partition contains Zebra-supplied programs and Dynamic Link Libraries (DLLs). This FFS is configured to include DLLs that control system operation. Since these drivers are required for basic MC32N0 operation, only experienced users should modify the content of this partition.
- Application: The Application FFS partition is used to store application programs needed to operate the MC32N0.

Working with FFS Partitions

Because the FFS partitions appear as folders under the Windows CE file system, they can be written to and read like any other folder. For example, an application program can write data to a file located in the Application folder just as it would to the Windows folder. However, the file in the Application folder is in non-volatile storage and is not lost on a cold boot (e.g., when power is removed for a long period of time).

Standard tools such as ActiveSync can be used to copy files to and from the FFS partitions. They appear as the “Application” and “Platform” folders to the ActiveSync explorer. This is useful when installing applications on the MC32N0. Applications stored in the Application folder are retained even when the MC32N0 is cold booted, just as the Sample Applications program is retained in memory.

There are two device drivers included in the Windows CE image to assist developers in configuring the MC32N0 following a cold boot: RegMerge and CopyFiles.

RegMerge.dll

RegMerge.dll is a built-in driver that allows registry edits to be made to the Windows CE registry. Regmerge.dll runs very early in the boot process and looks for registry files (.reg files) in certain Flash File System folders during a cold boot. It then merges the registry changes into the system registry located in RAM.

Since the registry is re-created on every cold boot from the default ROM image, the RegMerge driver is necessary to make registry modifications persistent over cold boots.

RegMerge is configured to look in the root of two specific folders for .reg files in the following order:

- \Platform
- \Application

Regmerge continues to look for .reg files in these folders until all folders are checked. This allows folders later in the list to override folders earlier in the list. This way, it is possible to override Registry changes made by the Platforms partitions folders. Take care when using Regmerge to make registry changes.

Note: Regmerge only merges the .reg files on cold boots. The merge process is skipped during a warm boot.

Making modifications to registry values for drivers loaded before RegMerge is not recommended. However, these values may require modification during software development. Since these early loading drivers read these keys before RegMerge gets a chance to change them, the MC32N0 must be cold booted. The warm boot does not re-initialize the registry and the early loading driver reads the new registry values.

Do not use Regmerge to modify built-in driver registry values, or merge the same registry value to two files in the same folder, as the results are undefined.

CopyFiles

Windows CE expects certain files to be in the Windows folder, residing in volatile storage. Windows CE maintains the System Registry in volatile storage. CopyFiles copies files from one folder to another on a cold boot. Files can be copied from a non-volatile partition (Application or Platform) to the Windows or other volatile partition during a cold boot. During a cold boot CopyFiles looks for files with a .CPY extension in the root of the Platform and Application FFS partitions (Platform first and then Application). These files are text files containing the source and destination for the desired files to be copied separated by “>”.

Files are copied to the Windows folder from the Flash File System using copy files (*.cpy) in the following order:

- \Platform
- \Application

Example:

```
\Application\ScanSamp2.exe>\Windows\ScanSamp2.exe
```

This line directs CopyFiles to copy the ScanSamp2.exe application from the \Application folder to the \Windows folder.

Non-FFS Partitions

Non-FFS partitions include additional software and data pre-loaded on the MC32N0 that can be upgraded. Unlike FFS Partitions, these partitions are not visible when the operating system is running. They also contain system information. Non-FFS partitions include the following:

- Windows CE: The complete Windows CE operating system is stored on Flash devices. If necessary, the entire OS image may be downloaded to the MC32N0 using files provided by Zebra. Any upgrades must be obtained from Zebra. This partition is mandatory for the MC32N0.
- Splash Screen: a bitmap smaller than 16 Kb (and limited to 16 bits per pixel) is displayed as the MC32N0 cold boots. To download a customized screen to display, see *Creating a Splash Screen on page 157*.
- Bootloader: This program interfaces with the host computer and allows downloading via USB cable any or all of the partitions listed above, as well as updated versions of Bootloader. Use caution downloading updated Bootloader versions; incorrect downloading of a Bootloader causes permanent damage to the MC32N0. Bootloader is mandatory for the MC32N0.
- Partition Table: Identifies where each partition is loaded in the MC32N0.

Downloading Partitions to the MC32N0

USBDownload is used to specify a hex destination file for each partition and download each file to the MC32N0. This download requires a program loader stored on the MC32N0. The MC32N0 comes with a program loading utility, Bootloader, stored in the MC32N0's write-protected flash.

Bootloader

Bootloader allows the user to upgrade the MC32N0 with software updates and/or feature enhancements.

Partition Update vs. File Update

There are two types of updates supported by the MC32N0: partitions and files. The file system used by the MC32N0 is the same as the file system used on a desktop computer. A file is a unit of data that can be accessed using a file name and a location in the file system. When a file is replaced, only the contents of the previous file are erased. The operating system must be running for a file to be updated, so the Bootloader cannot perform individual file updates as it is a stand-alone program that does not require the operating system to be running.

A typical partition is a group of files, combined into a single “partition” that represents a specific area of storage. Examples of partitions are the flash file systems such as Platform or Application. (Using the desktop computer comparison, these partitions are roughly equivalent to a C: or D: hard disk drive.) In addition to the “hard disk” partitions, some partitions are used for single items such as the operating system, monitor, or splash screen. (Again using a desktop computer comparison, these partitions are roughly the equivalent of the BIOS or special hidden system files.) When a partition is updated, all data that was previously in its storage region is erased - i.e. it is not a merge but rather a replacement operation. Typically, the operating system is not running when partitions are update, so Bootloader can perform partition updates.

All partition images suitable for use by Bootloader are in hex file format for transfer by USBDownloader from the development computer to the MC32N0.

Upgrade Requirements

Upgrade requirements:

- The hex files to be downloaded (on development computer)
- A connection from the host computer and the MC32N0
- USBDownload (on development computer) to download the files.

Once these requirements are satisfied, the MC32N0 can be upgraded by invoking Bootloader and navigating the menus. See *Bootloader on page 5-5* for procedures on downloading a hex file to the MC32N0.

Deployment

This section provides information about installing software and files on the MC22N0.

Software deployment can be performed by:

- Copying files from a host computer
- Updating images.

Copying Files from a Host Computer

Copy files to the MC32N0 using ActiveSync or by placing the MC32N0 into mass storage mode.

ActiveSync

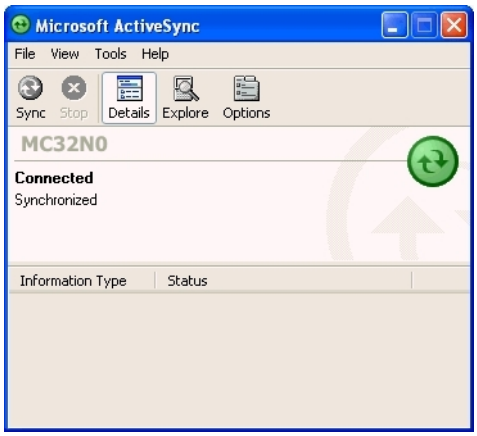
Procedure:

1 Ensure that ActiveSync or Windows Mobile Device Center is installed on the host computer and that a partnership was created.

2 Connect the MC32N0 to the host computer using a Single Slot Serial/USB cradle or an appropriate cable.

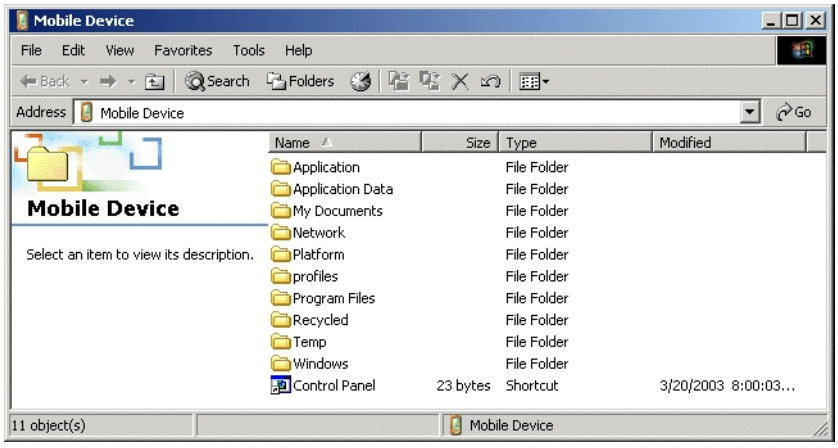
3 On the host computer, select **Start** > **Programs** > **ActiveSync**.

Figure 124: ActiveSync Connected Window



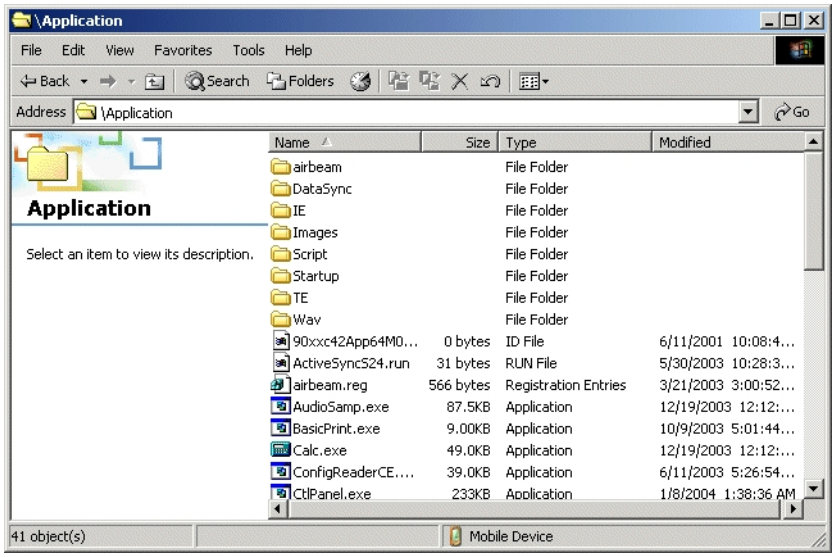
4 Select **Explore**.

Figure 125: ActiveSync Explorer



5 Double-click the folder to expand the folder contents.

Figure 126: Application Folder Contents



6 Use Explorer to locate the host computer directory that contains the file to download. Tap that directory in the left pane to display its contents in the right pane.

7 Drag the desired file(s) from the host computer to the desired mobile device folder.

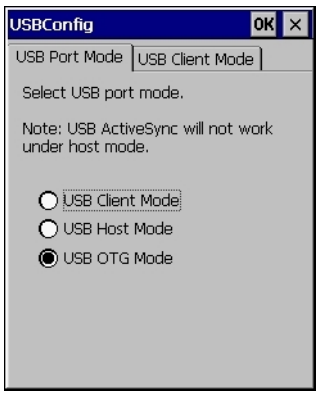
Mass Storage

To install an application or copy files to the MC32N0 using a USB connection:

Procedure:

1 On the MC32N0, select **Start** > **Settings** > **Control Panel** > **USBConfig**.

Figure 127: USBConfig Window



2 On the **USB Port Mode** tab, select **USB Client Mode**.

3 On the **USB Client Mode** tab, select **Mass Storage**.

4 In the drop-down list, select **Platform** or **Application**.

5 Select **OK**.

6 Connect the MC32N0 to a host computer using either a Single-slot Serial/USB cradle or a USB Client Charge cable.

7 On the host computer, open **Windows Explorer**. The MC32N0 appears as a hard disk drive in **Windows Explorer**.

8 On the host computer, open another **Windows Explorer** window and locate the files to copy to the MC32N0.

9 Drag the files from the new window to the MC32N0 folder window.

10 When complete, disconnect the MC32N0 from the host computer.

Updating Images

The MC32N0 contains tools that update all operating system components. All updates are distributed as packages and/or hex images. Update packages can contain either partial or complete updates for the operating system. Zebra distributes the update packages on the Support Central Web Site, http://www.zebra.com/support. Update an operating system component using one of the following:

- OS Update
- BootLoader.
- Mobility device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

OS Update Loader

Operating system component can be downloaded to the MC32N0 using the MC32N0 temp directory or an SD card.

Using MC32N0 Temp Folder

Procedure:

1 Go to the Support Central web site, http:/www.zebra.com/support.
2 Download the appropriate update package.
3 Connect the MC32N0 to a host computer using the Single Slot Serial/USB Cradle or USB Communication Cable.
4 On the host computer, use ActiveSync to copy the update package to the `temp` folder on the MC32N0.
5 On the MC32N0, use **Windows Explorer** and navigate to the `temp` folder.
6 Open the `OSUpdate` folder.
7 Double tap on the file: `32N0c70Ben_TEMP.lnk`.
8 When the OS Update application finds the appropriate file, it loads the package onto the MC32N0. A progress bar displays until the update completes.
9 When complete, the MC32N0 re-boots and the calibration screen appears.

Using an SD Card

Procedure:

1 Go to the Support Central web site, http://www.zebra.com/support.
2 Download the appropriate update package.
3 Copy the update package to the root directory of an SD card (using a host computer).
4 Install the SD card.
5 Connect the MC32N0 to AC power.
6 Use **Windows Explorer** to navigate to the SD card folder.
7 Open the `OSUpdate` folder.
8 Double tap on the file: `32N0c70Ben_SD.lnk`
9 When the OS Update application finds the appropriate file, it loads the package onto the MC32N0. A progress bar displays until the update completes.
10 When complete, the MC32N0 re-boots and the calibration screen appears.

Bootloader

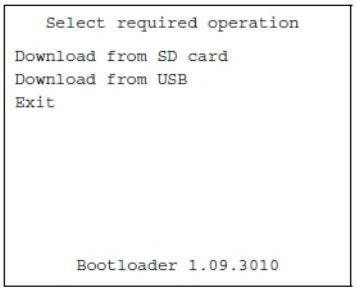
Use Bootloader to download hex files to the MC32N0 from an SD card or from a host computer via USB.

Loading Files From an SD Card

Procedure:

1 Copy the files to the root directory of an SD card.
2 Insert the SD card into the MC32N0.
3 Install the battery.
4 Simultaneously press the Power button and the 1 and 9 keys.
5 Immediately, as soon as the device starts to boot, press and hold the left scan button or trigger.
6 Continue to hold the scan button or trigger while releasing the 1, 9 and Power keys until the Bootloader screen appears.
7 When the Bootloader screen appears, release the scan button or trigger.

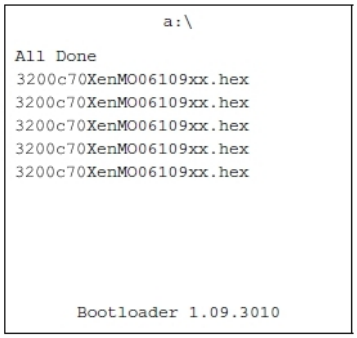
Figure 128: Bootloader Menu



Caution: To ensure a successful download, do not remove power from the mobile computer while in Bootloader.

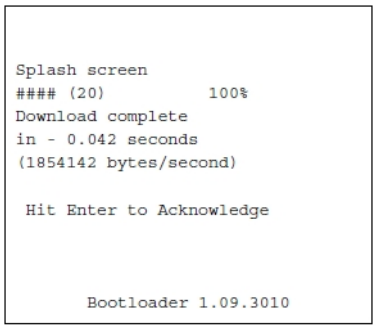
8 Use the up and down scroll buttons to select **Download from SD card**, then press **ENT**.
9 The Bootloader displays the hex files available on the SD card.

Figure 129: Hex File List



10 Use the up and down scroll buttons to select a hex file, then press **ENT**.
11 The hex file is downloaded to the device.

Figure 130: Download Complete Screen



12 On completion, press **ENT** to return to the Bootloader menu to select the next file to download.

13 To exit Bootloader, select Exit from the Bootloader main screen and press **ENT**.

Loading Files via USB

Use Bootloader to download customized flash file system partitions to the mobile computer and load hex files to the flash memory of the MC32N0.

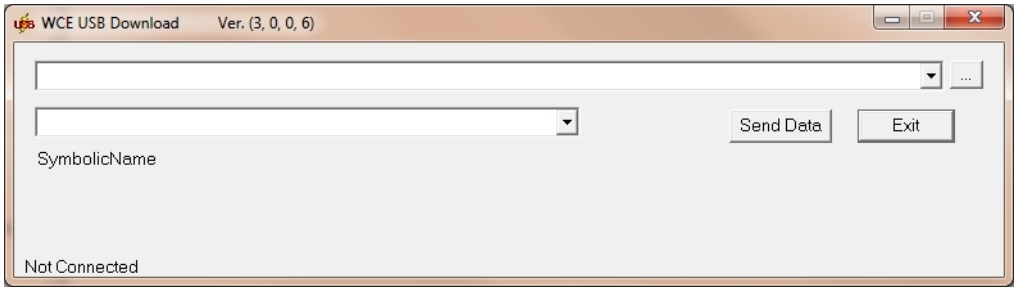
Procedure:

1 Download the **USBDownload** application from the Support Central web site. Follow the installation instructions with the application.

2 Connect the MC32N0 to a host computer using the Single Slot Serial/USB Cradle or USB Charge Cable.

3 On the host computer, launch the **USBDownload** application.

Figure 131: USB Download Window



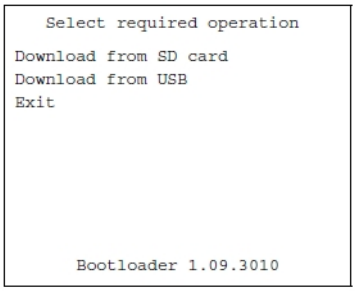
4 Simultaneously press the Power button and the 1 and 9 keys.

5 Immediately, as soon as the device starts to boot, press and hold the left scan button or trigger.

6 Continue to hold the scan button or trigger while releasing the 1, 9 and Power keys until the Bootloader screen appears.

7 When the **Bootloader** screen appears, release the scan button or trigger.

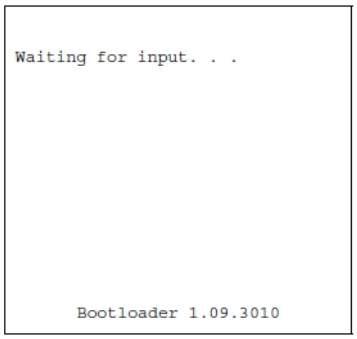
Figure 132: Bootloader Menu



Caution: To ensure a successful download, do not remove power from the mobile computer while in Bootloader.

8 Use the up and down scroll buttons to select **Download from USB**, then press **ENT**. The Bootloader displays the following:

Figure 133: Waiting for Input



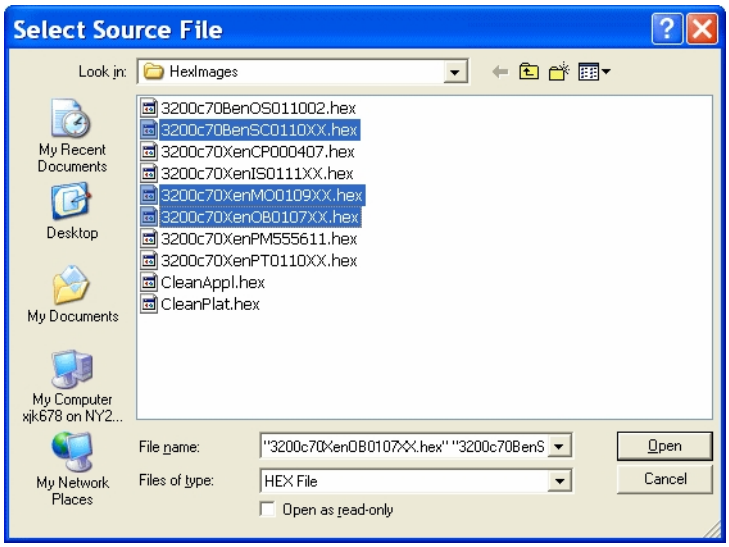
9 On the host computer, locate the hex files to download.

Note:

One hex file or multiple hex files can be selected. To select multiple files, press the Ctrl key while selecting files.

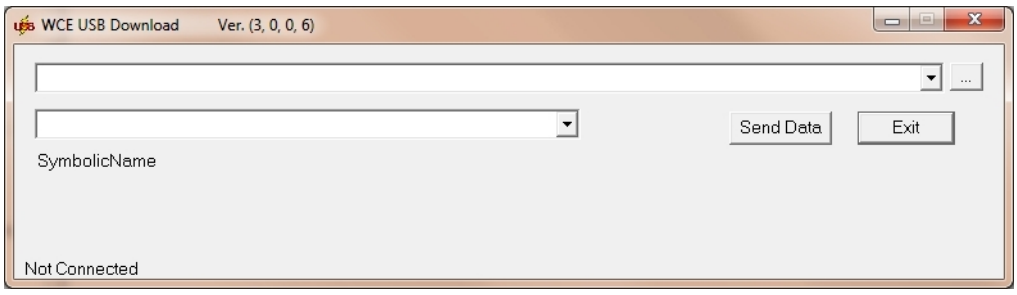
If selecting multiple files to download, USBDownload reads the header of the file and identifies the file type. If the Partition table file is among the files selected, then USBDownload downloads that file first. Similarly, USBDownload downloads the CPLD file last.

Figure 134: Select Source File Window



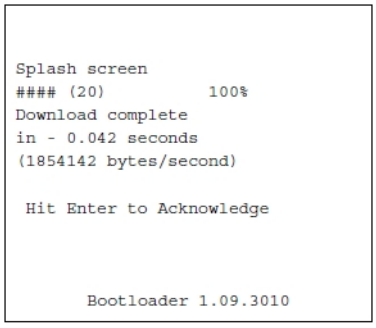
10 Select the hex files and the click **Open**.

Figure 135: USB Download Window



11 Click the **SEND DATA** button. The hex file(s) is downloaded to the device.

Figure 136: Download Complete Screen



12 On completion, press **ENT** to return to the Bootloader main screen to select the next file to download.

13 To exit Bootloader, select **Exit** from the Bootloader main screen and press **ENT**.

Bootloader Error Detection

While receiving data, Bootloader performs many checks on the data to ensure that the data is received correctly. If an error is detected, Bootloader immediately aborts the download, and reports the error on an error screen.

This error message screen displays until a key is pressed. Once the screen is acknowledged, Bootloader returns to the main menu to wait for a new selection.

To find the probable cause of the error, use the error number and/or the error text displayed on the screen to look up the error in the table below.

Table 11: Bootloader Errors

Error Text	Error Number	Probable Cause
Unknown error	-1	A general error occurred. Retry the download. If the failure persists, it is most likely due to a hardware failure; the mobile computer requires servicing.
Cancelled by user	-2	The user cancelled the download.
Can't open the source	-7	An error occurred opening the source device (either USB or SDMMC). Check source device connectivity and retry.
Can't open the destination	-8	An error occurred opening the destination device (either NAND, RAM, Power Micro, IST, Keyboard Controller or CPLD). Retry the download. If the failure persists, it is most likely due to a hardware failure; the mobile computer requires servicing.

Table continued...

Error Text	Error Number	Probable Cause
Can't read from the source device	-9	The source device (either USB or SDMMC) could not be read from. Check source device connectivity and retry.
Can't write to the destination device	-10	The destination device (either NAND, RAM, Power Micro, IST, Keyboard Controller or CPLD) could not be written to. Retry the download. If the failure persists, it is most likely due to a hardware failure; the mobile computer requires servicing.
Transmission checksum error	-11	An error occurred during transmission from the source device (either USB or SDMMC) and the checksum check failed. Check source device connectivity and retry.
Readback checksum error	-12	A checksum, generated from reading back data that was written to the destination device, was incorrect. An error during transmission or a write error to the destination device could cause this.
There is no more heap space available	-14	There is no more heap space available for the download procedure. Restart Bootloader and retry the download. If the failure persists, contact service with details of what is being downloaded.
Invalid data in verify file	-19	The file contains invalid data. Check that the file is suitable for downloading on this terminal.
Insufficient memory for buffering data	-20	There is no more heap space available for the download procedure. Restart Bootloader and retry the download. If the failure persists, contact service with details of what is being downloaded.
Insufficient data available to complete record	-21	A HEX file download was attempted but the HEX file is invalid. Ensure the file is in proper HEX file format.
Invalid Symbol HEX file	-23	A HEX file download was attempted but the HEX file is invalid. Ensure the file is in proper HEX file format.
Unrecognized or unsupported HEX record	-24	The HEX file being downloaded contains an invalid or unrecognized HEX record. Ensure the file is in proper HEX file format.
Invalid data in HEX file	-25	The HEX file being downloaded contains invalid data. Ensure the file is in proper HEX file format with valid HEX data.
Exceeded max size	-26	The download file is too large to fit into the space allocated for it. Either make the file smaller or increase the space allocated for it by altering the partition table.
Partition is not valid on this device	-27	The downloaded file specifies a partition entry that does not exist on the device. Only download files that are valid for this device, or change the partition table so that the new file is valid on the device.
Wrong destination code	-28	A specific partition was chosen from the Bootloader main menu but the file selected for download was for another partition. Ensure that the partition selected from the Bootloader main menu matches the file selected for download.
Non-contiguous record found	-30	A HEX file download was attempted but the HEX file is invalid. Ensure the file is in proper HEX file format.
Timed Out - No data	-31	Bootloader was waiting for data from the source device but timed out before receiving any. Check the source device connectivity and retry.

Table continued...

Error Text	Error Number	Probable Cause
Invalid file format	-33	The file format is invalid. Only HEX files are supported by Bootloader.
Partition Table not Valid	-34	The size of flash memory is different than that described in the partition table. Retry the download with the correct partition table file.
Invalid data in file	-35	The .bin or .sig file being downloaded contains invalid data. Ensure the file is in proper file format.
File cannot be loaded to this unit	-38	The file contains valid data that indicates it cannot be loaded onto the device.
File validation failed	-40	The file has either been signed incorrectly, or contains data that indicates that it cannot be loaded onto the terminal.

Creating a Splash Screen

A custom splash screen can be created and loaded onto the MC32N0. To create a custom splash screen:

Procedure:

1 Create a .bmp file using a graphic program with the following specifications:

- Size: 320 (W) x 320 (H).
- Colors: 256.

2 Modify the bitmap file and save.

Loading a Splash Screen

To load the splash screen:

Procedure:

1 Convert the bmp file into a hex file using the **OSUpdate Package Builder**.

2 Copy the hex file to the MC32N0 using BootLoader.

Chapter 11

Maintenance and Troubleshooting

This chapter includes instructions on cleaning and storing the device, and provides troubleshooting solutions for potential problems during operation.

Maintaining the MC32N0

For trouble-free service, observe the following tips when using the MC32N0:

- Do not scratch the screen of the MC32N0. When working with the MC32N0, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the MC32N0 screen.
- The touch-sensitive screen of the MC32N0 is glass. Do not to drop the MC32N0 or subject it to strong impact.
- Protect the MC32N0 from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store or use the MC32N0 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the MC32N0. If the surface of the MC32N0 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.
- A screen protector is applied to the MC32N0. Zebra recommends using this to minimize wear and tear. Screen protectors enhance the usability and durability of touch screen displays. Benefits include:
  - Protection from scratches and gouges
  - Durable writing and touch surface with tactile feel
  - Abrasion and chemical resistance
  - Glare reduction
  - Keeping the device’s screen looking new
  - Quick and easy installation.

Battery Safety Guidelines

Warning: Failure to follow these guidelines may result in fire, explosion, or other hazard.

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Follow battery usage, storage, and charging guidelines found in this guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between +32 ºF and +104 ºF (0 ºC and +40 ºC)

- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact Zebra Customer Support Center.
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- Seek medical advice immediately if a battery has been swallowed.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, contact Zebra Customer Support to arrange for inspection.

Cleaning Instructions

Caution:

Always wear eye protection.

Read warning label on compressed air and alcohol product before using.

If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.

Warning: Avoid exposing this product to contact with hot oil or other flammable liquids. If such exposure occurs, unplug the device and clean the product immediately in accordance with these guidelines.

Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite[1](see Important note below), hydrogen peroxide or mild dish soap.

Important:

Use pre-moistened wipes and do not allow liquid to pool.

[1] When using sodium hypochlorite (bleach) based products always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.
Due to the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidization (corrosion) when exposed to this chemical in the liquid form (including wipes). Avoid allowing any bleach based product to come in contact with the metal electrical contacts on the device, the battery, or the cradle. In the event that these types of disinfectants come in contact with metal on the device, prompt removal with alcohol-dampened cloth or cotton swab after the cleaning step is critical.

Harmful Ingredients

The following chemicals are known to damage the plastics on the device and should not come in contact with the device: ammonia solutions, compounds of amines or ammonia; acetone; ketones; ethers; aromatic and chlorinated hydrocarbons; acqueous or alcoholic alkaline solutions; ethanolamine; toluene; trichloroethylene; benzene; carbolic acid and TB-lysoform.

Cleaning Instructions

Do not apply liquid directly to the device. Dampen a soft cloth or use pre-moistened wipes. Do not wrap the device in the cloth or wipe, but gently wipe the unit. Be careful not to let liquid pool around the display window or other places. Allow the unit to air dry before use.

Special Cleaning Notes

Many vinyl gloves contain phthalate additives, which are often not recommended for medical use and are known to be harmful to the housing of the device. The device should not be handled while wearing vinyl gloves containing phthalates, or before hands are washed to remove contaminant residue after gloves are removed. If products containing any of the harmful ingredients listed above are used prior to handling the device, such as hand sanitizer that contain ethanolamine, hands must be completely dry before handling the device to prevent damage to the plastics.

Cleaning Materials Required

- Alcohol wipes
- Lens tissue
- Cotton-tipped applicators
- Isopropyl alcohol
- Can of compressed air with a tube.

Cleaning Frequency

The cleaning frequency is up to the customer's discretion due to the varied environments in which the mobile devices are used. They may be cleaned as frequently as required, but it is advisable to clean the camera window periodically when used in dirty environments to ensure optimum performance.

Cleaning the MC32N0

Housing

Using the alcohol wipes, wipe the housing including buttons.

Display

The display can be wiped down with the alcohol wipes, but care should be taken not to allow any pooling of liquid around the edges of the display. Immediately dry the display with a soft, non-abrasive cloth to prevent streaking.

Exit Window

Wipe the exit window periodically with a lens tissue or other material suitable for cleaning optical material such as eyeglasses.

Housing

Using the alcohol wipes, wipe the housing including keys and in-between keys.

Display

The display can be wiped down with the alcohol wipes, but care should be taken not to allow any pooling of liquid around the edges of the display. Immediately dry the display with a soft, non-abrasive cloth to prevent streaking.

Camera Window

Wipe the camera window periodically with a lens tissue or other material suitable for cleaning optical material such as eyeglasses.

Connector Cleaning

To clean the connectors:

Procedure:

1. Remove the main battery from mobile computer.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator back-and-forth across the connector. Do not leave any cotton residue on the connector.

4 Repeat at least three times.
5 Use the cotton-tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
6 Use a dry cotton-tipped applicator and repeat steps 4 through 6.

Caution: Do not point nozzle at yourself and others, ensure the nozzle or tube is away from your face.

7 Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.
8 Inspect the area for any grease or dirt, repeat if required.

Cleaning Cradle Connectors

To clean the connectors on a cradle:

Procedure:

1 Remove the DC power cable from the cradle.
2 Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3 Rub the cotton portion of the cotton-tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not leave any cotton residue on the connector.
4 All sides of the connector should also be rubbed with the cotton-tipped applicator.

Caution: Do not point nozzle at yourself and others, ensure the nozzle or tube is pointed away from your face.

5 Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.
6 Remove any lint left by the cotton-tipped applicator.
7 If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.
8 Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

   If the temperature is low and humidity is high, longer drying time is required. Warm temperature and dry humidity requires less drying time.

Troubleshooting

The following tables provides typical problems that might arise and the solution for correcting the problem.

Troubleshooting the MC32N0

Table 12: Troubleshooting the MC32N0

Problem	Cause	Solution
Mobile computer does not turn on.	Main battery not charged.	Charge or replace the main battery.
	Main battery not installed properly.	Ensure the battery is installed properly.
	MC32N0 not responding.	On Android devices, perform a soft reset. If the mobile computer still does not turn on, perform a hard reset. On WinCe devices, perform a warm boot. If the mobile computer still does not turn on, perform a cold boot. For more information see *Getting Started on page 19*.

Table continued…

Problem	Cause	Solution
Battery did not charge.	Battery failed.	Replace battery. If the mobile computer still does not operate, try a soft reset , then a hard reset. See *Getting Started on page 19*.
	Mobile computer removed from cradle while battery was charging.	Insert mobile computer in cradle and begin charging. The Standard Battery requires up to five hours to recharge fully and the Extended Life Battery requires up to eight hours to recharge fully.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 32 °F (0 °C) or above 104 °F (40 °C).
Cannot see characters on screen.	Mobile computer not powered on.	Press the Power button.
During data communication, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle or unplugged from host computer during communication.	Replace the mobile computer in the cradle, or reattach the cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
Mobile computer does not emit sound.	Volume setting is low or turned off.	Click on the speaker icon to increase the volume.
MC32N0 turns itself off.	MC32N0 is inactive.	The mobile computer turns off after a period of inactivity. This period can be set from 15 seconds to 30 minutes.
	Battery is depleted.	Recharge or replace the battery.
A message appears stating that the mobile computer memory is full.	Too many applications installed on the mobile computer.	Remove user-installed applications on the MC32N0 to recover memory. On Android devices, select  >  **Apps** > **Downloaded**. Select the unused programs and touch **Uninstall**. On WinCE devices, touch **Start** > **Settings** > **Control Panel** > **Remove Programs**. Select the unused program and touch **Remove**.
The MC32N0 does not decode when reading bar code.	DataWedge is not enabled.	Ensure that DataWedge is enabled and configured properly.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between the MC32N0 and bar code is incorrect.	Place the MC32N0 within proper scanning range.
	MC32N0 is not programmed for the bar code type.	Program the MC32N0 to accept the type of bar code being scanned.

Table continued…

Problem	Cause	Solution
	MC32N0 is not programmed to generate a beep.	If the MC32N0 does not beep on a good decode, set the application to generate a beep on good decode.
MC32N0 cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (32.8 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
Cannot connect to WLAN.	Access Point (AP) does not broadcast country code.	Disable 802.11d feature. On Android devices, touch  > **Wi-Fi** >  > **Advanced**. Deselect the **Enable 802.11d** checkbox. On WinCe devices, Fusion icon, **Options** > **Regulatory** option from drop-down list. Deselect **Enable 802.11d**.
When trying to open File Browser or other applications, the application automatically closes.	The Internal Memory is full.	Connect the MC32N0 to a host computer and delete files from Internal Memory using the host computer.

Single Slot Serial/USB Cradle Troubleshooting

Table 13: Troubleshooting the Single Slot Serial/USB Charge Cradle

Problem	Cause	Solution
MC32N0 amber Charge LED Indicator does not light when MC32N0 inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	MC32N0 is not correctly seated.	Remove and re-insert the MC32N0 into the cradle, ensuring it is correctly seated.
Spare Battery Charging LED does not light when spare battery is inserted.	Spare battery not correctly seated.	Remove and re-insert the spare battery into the battery adapter, ensuring it is correctly seated.
	Battery adapter not correctly seated.	Remove and re-insert the battery adapter into the charging slot, ensuring it is correctly seated.
MC32N0 battery is not charging.	MC32N0 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure the MC32N0 is seated correctly. If the MC32N0 battery is fully depleted, it can take up to five hours to fully recharge a Standard Battery and it can take up to eight hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

Table continued…

Problem	Cause	Solution
	The MC32N0 is not fully seated in the cradle.	Remove and re-insert the MC32N0 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
Spare battery is not charging.	Battery not fully seated in charging slot.	Remove and re-insert the spare battery into the cradle, ensuring it is correctly seated.
	Battery inserted incorrectly.	Ensure the contacts are facing down and toward the back of the cradle.
	Battery adapter not correctly seated.	Remove and re-insert the battery adapter into the charging slot, ensuring it is correctly seated.
During data communication, no data was transmitted, or transmitted data was incomplete.	MC32N0 removed from cradle during communication.	Replace MC32N0 in cradle and retransmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software is not installed or configured properly.	See the system administrator.

Four Slot Charge Only Cradle CRD3000–4000CR Troubleshooting

Table 14: Troubleshooting the Four Slot Charge Only Cradle

Problem	Cause	Solution
Mobile computer amber Charge LED Indicator does not light when mobile computer inserted.	Cradle is not receiving power.	Replace the MC3200 in the cradle. The 2680 mAh battery charges in approximately four hours. Touch  >  **About device** > **Status** to view battery status.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	MC40 is not inserted correctly in the cradle.	Remove the MC3200 and reinsert it correctly. Verify charging is active. Touch  >  **About device** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between 0 °C (32 °F) and 35 °C (95 °F).

Four Slot Ethernet Cradle CRD3X01–4001ER

Table 15: Troubleshooting the Four Slot Ethernet Cradle

Symptom	Cause	Solution
During communication, no data transmits, or transmitted data was incomplete.	MC32N0 removed from cradle during communications.	Replace MC32N0 in cradle and retransmit.
	MC32N0 has no active connection.	An icon is visible in the status bar if a connection is currently active.
	Ethernet connection error. Link LED is not lit.	See the system administrator. Probable Ethernet connection error.
Mobile computer amber Charge LED Indicator does not light when mobile computer inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Mobile computer is not correctly seated.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.
Battery is not charging.	MC32N0 removed from the cradle too soon.	Replace the MC32N0 in the cradle. The Standard Life Battery fully charges in less than hours and the Extended Life Battery fully charges in less than eight hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	MC32N0 is not inserted correctly in the cradle.	Remove the MC32N0 and reinsert it correctly.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between 0°C (32°F) and 50°C (122°F).

Four Slot Battery Charger SAC7X00-4000R Troubleshooting

Table 16: Troubleshooting the Four Slot Battery Charger

Problem	Cause	Solution
Spare Battery Charging LED does not light when spare battery is inserted.	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charging slot, ensuring it is correctly seated.
Spare Battery not charging.	Charger is not receiving power.	Ensure the power cable is connected securely to both the charger and to AC power.
	Spare battery is not correctly seated.	Remove and re-insert the battery into the battery adapter, ensuring it is correctly seated.
	Battery adapter is not seated properly.	Remove and re-insert the battery adapter into the charger, ensuring it is correctly seated.
	Battery was removed from the charger or charger was unplugged	Ensure charger is receiving power. Ensure the spare battery is seated correctly. If a battery is fully depleted, it can take up to five hours to fully recharge a Standard Battery and it can take up to eight hours to fully recharge an Extended Life Battery.

Table continued…

Problem	Cause	Solution
	from AC power too soon.	
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

Cables

Table 17: Troubleshooting the Cables

Symptom	Possible Cause	Action
MC32N0 amber Charge LED Indicator does not light when MC32N0 is attached.	Cable is not receiving power.	Ensure the power cable is connected securely to both the cable and to AC power.
	MC32N0 is not seated correctly in the cable cup.	Remove and re-insert the MC32N0 into the MC32N0 cable cup, ensuring it is correctly seated.
MC32N0 battery is not charging.	MC32N0 was detached from cable or cable was unplugged from AC power too soon.	Ensure the cable is receiving power. Ensure MC32N0 is seated correctly. If the MC32N0 battery is fully depleted, it can take up to five hours to fully recharge a Standard Battery and it can take up to eight hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The MC32N0 is not fully seated in the cable.	Remove and re-insert the MC32N0 into the cable cup, ensuring it is correctly seated.
During data communication, no data transmits, or transmitted data was incomplete.	Cable was disconnected from MC32N0 during communications.	Re-attach the cable and retransmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software is not installed or configured properly.	See the system administrator.

Chapter 12

Technical Specifications

The following sections provide technical specification for the device.

MC32N0 Technical Specifications

The following table summarizes the MC32N0's intended operating environment and technical hardware specifications.

Table 18: MC32N0 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions	**MC32N0-S:** 7.49 in L x 3.22 in W x 1.78 in D (190.4 mm L x 81.9 mm W x 45.2 mm D) **MC32N0-R:** 8.37 in L x 3.22 in W x 1.57 in D (212.6 mm L x 81.9 mm W x 40.0 mm D) **MC32N0-G:** 7.59 in L x 3.18 in W x 6.5 in D (192.7 mm L x 80.8 mm W x 166.0 mm H)
Weight	MC32N0-R (with standard battery) - 13.1 oz (372 g) MC32N0-S (with standard battery) - 12.88 oz (365 g) MC32N0-G (with extended battery) - 18.0 oz (509 g)
Display	3.0 inch Color (TFT) (320 x 320) display
Touch Panel	Chemically strengthened glass, resistive touch
Backlight	LED backlight
Battery	Standard: Rechargeable Lithium-Ion 2740 mAh minimum (3.7V) Extended Life: Rechargeable Lithium-Ion 4800 mAh minimum (3.7V)
Expansion Slot	User accessible microSD slot. Supports up to 32 GB microSDHC.

Table continued…

Item	Description
Network Connections	Full-speed USB client, full-speed USB host, Bluetooth and WiFi. USB host mode available with appropriate cables only.
Notification	LEDs and audio notifications
Keypad Options	28-key Numeric 38-key Shifted Alpha (calculator-style integrated numeric keypad) 48-key Alpha-Numeric (calculator-style integrated numeric keypad)
Audio	Speaker, microphone, and headset connector (2.5 mm jack).
Performance Characteristics	
CPU	Dual core, OMAP 4 @ 800 MHz (Standard). Dual core, OMAP 4 @ 1 GHz (Premium).
Operating System	Android-based ASOP 4.1.1 (Premium only) or Windows CE 7
Memory	512 MB RAM, 2 GB Flash (Standard). 1 GB RAM, 4 GB Flash (Premium).
Output Power (USB)	USB: 5 VDC @ 500 mA max.
User Environment	
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F) without battery
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	10% to 95% RH non-condensing
Drop Specification	Multiple 4 ft./1.2 m drop to concrete across the operating temperature range. Multiple 5 ft/1.5 m drops to concrete at ambient temperature 73 °F/23 °C. Meets and exceeds MIL-STD 810G.
Electrostatic Discharge (ESD)	±20kVdc air discharge, ± 10kVdc direct discharge, ± 10kVdc indirect discharge
Sealing	IP54 per IEC specification.
Wireless LAN Data Communications	
Wireless Local Area Network (WLAN) radio	IEEE® 802.11a/b/g/n with internal antenna
Data Rates Supported	802.11b: 1, 2, 5.5, 11 Mbps 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n: 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 72 Mbps (with SGI) Note that 802.11n data rates may be higher.
Operating Channels	Chan 36 - 165 (5180 – 5825 MHz), Chan 1 - 13 (2412 - 2472 MHz); actual operating channels/frequencies depend on regulatory rules and certification agency.
Security	**Security Modes:**WPA and WPA2 (Personal or Enterprise)

Table continued…

Item	Description
	Encryption: WEP40/WEP104, TKIP and AES **Authentication:**TLS; TTLS (CHAP*, MSCHAP, MSCHAPv2, PAP or MD5*); PEAP (TLS*, MSCHAPv2, GTC); LEAP; FAST (TLS*, MSCHAPv2, GTC). **Other:** Wi-Fi, CCXv4 certified, and supports IPv6 FIPS 140–2 certified (Android), Q4–2014 (WinCE) * WinCE only
Wireless PAN Data	
Bluetooth	Class II, v 2.1 with EDR; integrated antenna.
Sensors (WinCE only)	
Motion Sensor (WinCE only)	3-axis accelerometer that enables motion sensing applications for dynamic screen orientation and power management.
Ambient Light/Proximity Sensor (WinCE only)	Automatically adjusts display brightness and turns off the display during PTT calls.
Data Capture	
Laser scanner	Captures 1D bar codes.
Imager	Captures 1D and 2D bar codes.
Laser Scanner (SE965) Specifications	
Optical Resolution	0.005 in. minimum element width
Roll	Condition: 20 mil Code 39 at 10 in. ± 35° from vertical
Pitch Angle	Condition: 20 mil Code 39 at 10 in. ± 65° from normal
Skew Tolerance	Condition: 20 mil Code 39 at 10 in. ± 40° from normal
Ambient Light	Tolerant to typical artificial indoor and natural outdoor (direct sunlight) lighting conditions. Fluorescent, Incandescent, Mercury Vapor, Sodium Vapor, LED: 450 ft. Candles (4,844 Lux) Sunlight: 10,000 Ft Candles (107,640 Lux) Note: LED lighting with high AC ripple content can impact scanning performance.
Scan Repetition Rate	104 (± 14) scans/sec (bidirectional)
Scan Angle	Wide (Default): 47° (typical) Medium: 35° (typical)

Table continued…

Item	Description
	Narrow: 10° (typical)
2D Imager Engine (SE4750) Specifications	
Field of View	Horizontal - 48.0° Vertical - 36.7°
Image Resolution	1280 horizontal X 960 vertical pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles (107,639 lux)
Focal Distance	From front of engine: 17.7 cm (7.0 in.)
Laser Aiming Element	Visible Laser Diode (VLD): 655 nm +/- 10 nm Central Dot Optical Power: 0.6 mW (typical) Pattern Angle: 48.0º horizontal, 38.0º vertical
Illumination System	LEDs: Warm white LED Pattern Angle: 80° at 505 intensity
Supported Symbologies	
1D	Chinese 2 of 5, Codabar, Code 11, Code 128, Code 39, Code 93, Discrete 2 of 5, EAN-8, EAN-13, GS1 DataBar, GS1 DataBar Expanded, GS1 DataBar Limited, Interleaved 2 of 5, Korean 2 of 5, MSI, TLC 39, Matrix 2 of 5, Trioptic, UPCA, UPCE, UPCE1, Web Code.
2D	Australian Postal, Aztec, Canadian Postal, Composite AB, Composite C, Data Matrix, Dutch Postal, Japan Postal, Maxicode, Micro PDF, Micro QR, PDF, QR Code, UK Postal, US Planet, US Postnet, US4State, US4State FICS.

SE965 Decode Zone

The table below lists the typical distances for selected bar code densities. The minimum element width (or "symbol density") is the width in mils of the narrowest element (bar or space) in the symbol.

Table 19: SE965 Decode Distances

Symbol Density/ Bar Code Type	Bar Code Content/ Contrast [Note 1]	Typical Working Ranges	
		Near	Far
5.0 mil Code 128	1234 80% MRD	1.2 in 3.05 cm	7.7 in 19.56 cm

Table continued…

Symbol Density/ Bar Code Type	Bar Code Content/ Contrast Note 1	Typical Working Ranges	
		Near	Far
5.0 mil Code 39	ABCDEFGH 80% MRD	1.2 in 3.05 cm	12.5 in 31.75 cm
7.5 mil Code 39	ABCDEF 80% MRD	1.1 in 2.79 cm	18.5 in 46.99 cm
10 mil Code 128	1234 80% MRD	1.2 in 3.05 cm Note 3	19.0 in 48.26 cm
13 mil 100% UPC	012345678905 80% MRD	1.6 in 4.06 cm	27.0 in 68.58 cm
15 mil Code 128	1234 80% MRD	1.0 in 2.54 cm Note 3	29.5 in 74.93 cm
20 mil Code 39	123 80% MRD	1.4 in 3.56 cm Note 3	52.0 in 132.08 cm
55 mil Code 39	CD 80% MRD	31.4 in 8.64 cm Note 3	100.0 in 254.0 cm
100 mil Code 39	123456 80% MRD	2.0 ft 60.96 cm Note 3	17 ft 518.16 cm

Note:

1. Contrast is measured as Mean Reflective Difference (MRD) at 650 nm.
2. Working range specifications at temperature = 23°C, pitch=18°, roll=0°, skew=0°, photographic quality, ambient light ~150 ft-c, humidity 45-70% RH.
3. Dependent upon width of bar code.
4. Distances measured from front edge of scan engine chassis.

SE4750-SR Decode Zone

The table below lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

Table 20: SE4750-SR Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
3.0 mil Code 39	2.8 in 7.11 cm	6.2 in 15.75 cm
5.0 mil Code 128	2.3 in 5.84 cm	8.7 in 22.10 cm
5.0 mil PDF417	3.0 in 7.62 cm	8.1 in 20.57 cm
6.67 mil PDF417	2.2 in 5.89 cm	10.6 in 26.92 cm
10. mil Data Matrix	2.4 in 6.10 cm	10.6 in 26.92 cm
100% UPCA	1.6 in 4.06 cm Note 2	21.6 in 54.86 cm
15 mil Code 128	2.4 in 6.10 cm Note 2	21.3 in 54.10 cm
20 mil Code 39	1.6 in 4.06 cm Note 2	28.5 in 72.39 cm

Note:

1 Photographic quality bar code at 18° pitch angle under 0.1 fcd ambient illumination.

2 Dependent upon width of bar code.

MC32N0 Connector Pin-Out

Figure 137: I/O Connector

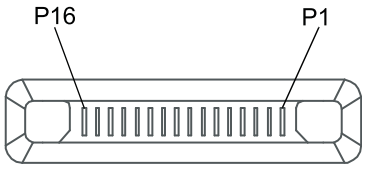


Table 21: I/O Connector Pin-Outs

Pin	Signal Name	Description
1	GND	Ground/Return

Table continued…

Pin	Signal Name	Description
2	Cradle_IN*	When grounded, the MC32N0 detects it is in the cradle.
3	DCD	RS232 DCD (into MC32N0)
4	USB_N	USB negative
5	USB_P	USB positive
6	GND	Ground/Return
7	BOTG_VBUS2	USB power out
8	USB_P2_7_SCTR	USB ID
9	U1_TXD_RS232	RS232 TXD (out of MC32N0)
10	U1_RXD_RS232	RS232 RXD (into MC32N0)
11	U1_RTS_RS232	RS232 RTS (out of MC32N0)
12	U1_CTS_RS232	RS232 CTS (into MC32N0)
13	U1_DTR_RS232	RS232 DTR (out of MC32N0)
14	U1_DSR_RS232	RS232 DSR (into MC32N0)
15	VCC5_CAM	5V power to RS232 accessories
16	POWER_JACK_ACC	Power into MC32N0.

MC32N0 Accessory Specifications

The following sections provide technical specifications for the MC32N0 accessories.

Single Slot Serial/USB Cradle CRD3000-1001R Technical Specifications

Table 22: Single Slot Charge Cradle CRD3000-1001R Technical Specifications

Item	Description
Dimensions	Height: 69.4 mm (2.73 in.) Width: 102.5 mm (4.04 in.) Depth: 88.9 mm (3.50 in.)
Weight	274 g (9.67 oz)
Input Voltage	5 VDC
Power Consumption	30 watts
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.

Table continued…

Item	Description
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact +/- 8 kV indirect discharge

Four Slot Charge Only Cradle CHS3000-4001CR Technical Specifications

Table 23: CHS3000-4001CR Technical Specifications

Item	Description
Dimensions	Height: 12.0 cm (5.0 in.) Width: 45.7 cm 18.0 in.) Depth: 10.1 cm (4.0 in.)
Weight	1.02 kg (2.25 lbs)
Input Voltage	12 VDC
Power Consumption	36 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact +/- 8 kV indirect discharge

Four Slot Ethernet Cradle CRD30X01-4001ER Technical Specifications

Table 24: CRD30X01-4001ER Technical Specifications

Item	Description
Dimensions	Height: 12.0 cm (5.0 in.) Width: 45.7 cm 18.0 in.) Depth: 10.1 cm (4.0 in.)
Weight	1.08 kg (2.38 lbs)
Input Voltage	12 VDC
Power Consumption	100 watts

Table continued…

Item	Description
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact +/- 8 kV indirect discharge

Four Slot Battery Charger SAC7X00-4000CR Technical Specifications

Table 25: Four Slot Battery Charger SAC7X00-4000CR Technical Specifications

Item	Description
Dimensions	Height: 4.32 cm (1.7 in.) Width: 20.96 cm (8.5 in.) Depth: 15.24 cm (6.0 in.)
Weight	386 g (13.6 oz.)
Input Voltage	12 VDC
Power Consumption	25 watts
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact +/- 8 kV indirect discharge

Chapter 13

Keypad Remap Strings

Note: This chapter applies to Android devices only.wince

Keypad Remap Strings

Table 26: Remap Key Event/Scancodes

Key Event	Scancode
SOFT_LEFT	105
SOFT_RIGHT	106
HOME	102
BACK	158
CALL	231
ENDCALL	107
0	11
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
STAR227	227
POUND	228
DPAD_UP	103
DPAD_DOWN	108
DPAD_LEFT	105

Table continued…

Key Event	Scancode
DPAD_RIGHT	106
DPAD_CENTER	232
VOLUME_UP	115
VOLUME_DOWN	114
CAMERA	212
A	30
B	48
C	46
D	32
E	18
F	33
G	34
H	35
I	23
J	36
K	37
L	38
M	50
N	49
O	24
P	25
Q	16
R	19
S	31
T	20
U	22
V	47
W	17
X	45
Y	21
Z	44
COMMA	51
PERIOD	52
ALT_LEFT	56
ALT_RIGHT	100

Table continued...

Key Event	Scancode
SHIFT_LEFT	42
SHIFT_RIGHT	54
TAB	15
SPACE	57
EXPLORER	150
ENVELOPE	155
ENTER	28
DEL	111
GRAVE	399
MINUS	12
EQUALS	13
LEFT_BRACKET	26
RIGHT_BRACKET	27
BACKSLASH	43
SEMICOLON	39
APOSTROPHE	40
SLASH	53
AT	215
PLUS	78
MENU	139
SEARCH	217
PAGE_UP	59
PAGE_DOWN	60
PICTSYMBOLS	61
SWITCH_CHARSET	62
BUTTON_A	63
BUTTON_B	64
BUTTON_C	65
BUTTON_X	66
BUTTON_Y	67
BUTTON_Z	68
BUTTON_L1	183
BUTTON_R1	184
BUTTON_L2	185
BUTTON_R2	186

Table continued…

Key Event	Scancode
BUTTON_THUMBL	187
BUTTON_THUMBR	188
BUTTON_START	189
BUTTON_SELECT	190
BUTTON_MODE	191