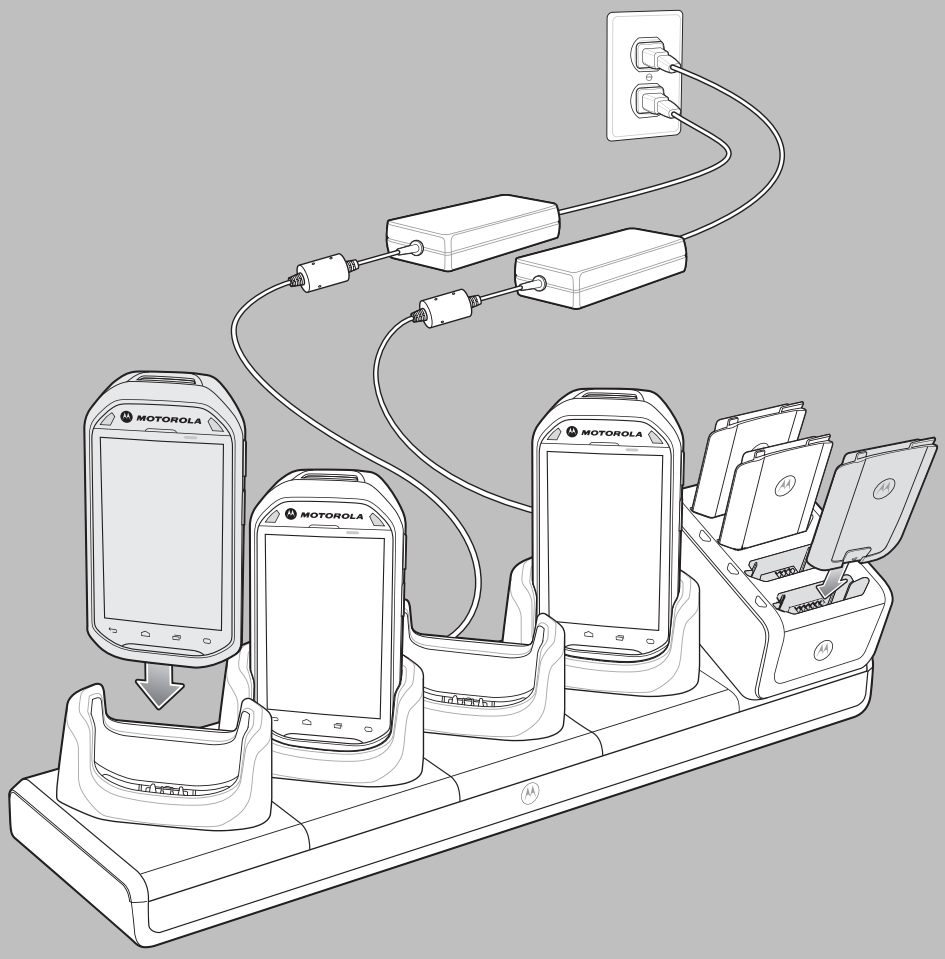
MC40
INTEGRATOR GUIDE



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 Motorola contact for further information.

Trademarks

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-A01 Rev A	10/04/2013	Initial release.

Contents

List of Tables

List of Figures

About This Guide

This guide provides information on using the MC40 and accessories.

NOTE

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

Documentation Set

The documentation set for the MC40 provides information for specific user needs, and includes:

- *MC40 Quick Start Guide* - describes how to get the device up and running.
- *MC40 Regulatory Guide* - provides required regulatory information.
- *MC40 User Guide* - describes how to use the device.
- *MC40 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
MC40	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	4.3” color WVGA	1 GB RAM / 8 GB Flash	camera and imager or camera, imager and MSR	Android-based, Android Open-Source Project 4.1.1

Software Versions

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.

The build number contains the software revision number and whether the MC40 is VoIP telephony ready.

Example Build Number: 0**z**-4AJ11–J-xxxx–xxxx–**y**0–M1–mmddyy

- **z** = software version number
- **y** = VoIP telephone ready

where:

- **0** = not VoIP telephony ready
- **V** = VoIP telephony ready.

Chapter Descriptions

Topics covered in this guide are as follows:

- 1 Getting Started, page 1-1 provides information on getting the MC40 up and running for the first time.
- 2 Accessories, page 2-1 describes the available accessories and how to use them with the MC40.
- 3 USB Communication, page 3-1 describes how to connect the MC40 to a host computer using USB.
- 4 DataWedge Configuration, page 4-1 describes how to use and configure the DataWedge application.
- 5 WLAN Configuration, page 5-1 describes the how to configure the MC40 to connect with a wireless LAN network.
- 6 Administrator Utilities, page 6-1 provides information for using the suite of administrative tools for configuring the MC40.
- 8 Settings, page 8-1 provides the settings for configuring the MC40.
- 9 Application Deployment, page 9-1 provides information for developing and managing applications.
- 10 Maintenance and Troubleshooting, page 10-1 includes instructions on cleaning and storing the MC40, and provides troubleshooting solutions for potential problems during MC40 operation.
- 11 Technical Specifications, page 11-1 provides the technical specifications for the MC40.
- 12 Keypad Remap Strings, page 12-1 provides a list of remap strings used when remapping keys.

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

- *MC40 Quick Start Guide*, p/n 72-166941-xx
- *MC40 Regulatory Guide*, p/n 72-166942-xx
- *MC40 Integrator Guide*, p/n 72E-166943-xx
- *MSP Client Software Guide*, p/n 72E-128805-xx
- *MSP Release Notes*, p/n 72E-100160-xx.

For the latest version of this guide and all guides, go to: http://supportcentral.motorolasolutions.com

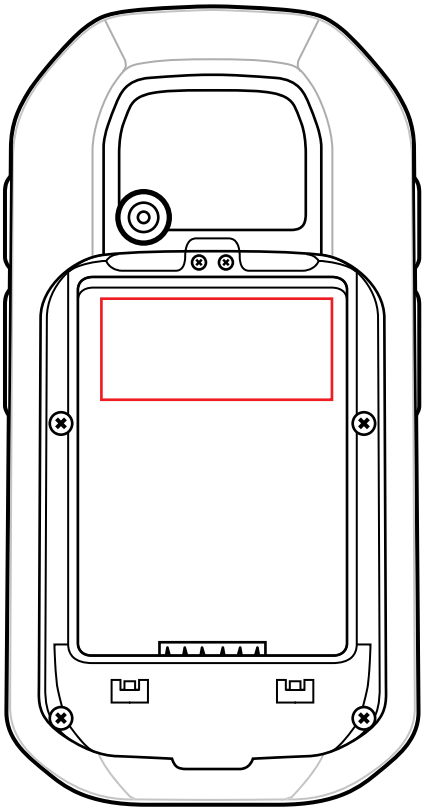
Service Information

If you have a problem with your equipment, contact Motorola Solutions Global Customer Support Center for your region. Contact information is available at: http://www.motorolasolutions.com/support.

When contacting Motorola Solutions Global Customer 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

Manufacturing Label Location



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

If your problem cannot be solved by Motorola Solutions Global Customer Support Center, you may need to return your equipment for servicing and will be given specific directions. Motorola 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 Motorola business partner, contact that business partner for support.

1 Getting Started

This chapter provides the features of the MC40 and explains how to set it up for the first time.

1.1 Unpacking

Carefully remove all protective material from the MC40 and save the shipping container for later storage and shipping.

Verify the following items are in the box:

- MC40
- Lithium-ion battery
- Quick Start Guide
- Regulatory Guide.

Inspect the equipment for damage. If any equipment is missing or damaged, contact the Motorola Solutions Global Customer Support Center immediately. See Service Information, page xv for contact information.

1.2 Setup

To start using the MC40 for the first time:

- Install the battery
- Charge the MC40
- Power on the MC40.

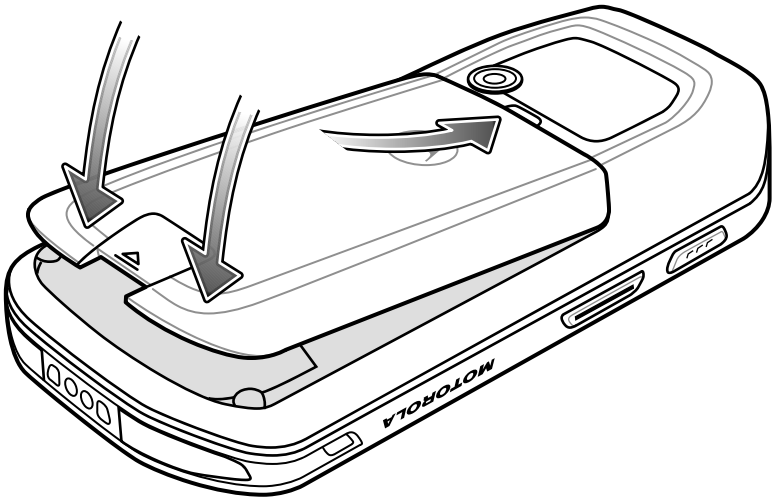
1.2.1 Installing the Battery

To install the battery:

Procedure Steps

1 Align the battery with the slots in the battery compartment.

Figure 1-1 Inserting the Battery



2 Lower the battery and press down until it snaps into place.

3 Press down on the battery latch.

4 Press the Power button to turn on the MC40.

1.2.2 Charging the Battery

CAUTION

Ensure that you follow the guidelines for battery safety described in 10.2 Battery Safety Guidelines, page 10-1.

Before using the MC40 for the first time, charge the main battery until the Right light emitting diode (LED) turns solid green (see Table 1-1 Battery Charge LED Status for charge status indications). To charge the MC40, use a cable or a cradle with the appropriate power supply. For information about the accessories available for the MC40, see 2 Accessories, page 2-1.

The MC40 is equipped with a memory backup battery that automatically charges from the fully-charged main battery. When using the MC40 for the first time, the backup battery requires approximately 36 hours to fully charge. This is also true any time the backup battery is discharged, which occurs when the main battery is removed for several hours. The backup battery retains random access memory (RAM) data in memory for at least 10 minutes (at room temperature) when the MC40's main battery is removed, when Battery Swap feature is used. When the MC40 reaches a very low battery state, the combination of main battery and backup battery retains RAM data in memory for at least 48 hours.

For cable and cradle setup and charging procedures refer to the MC40 Integrator Guide.

- Micro USB Cable
- Single Slot Charging Cradle
- Five Slot Charge Only Cradle.

Table 1-1 Battery Charge LED Status

Status	Indications
Off	MC40 is not charging. MC40 is not inserted correctly in the cradle. MC40 is not connected to a power source. Charger or cradle is not powered.
Slow Blinking Amber (3 blinks every 2 seconds)	MC40 is charging.
Solid Green	Charging complete.
Fast Blinking Amber (3 blinks/second)	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).
Flashes Amber once (when Power button pressed)	Critical battery state. Battery too low to boot device.
Fast Blinking Amber (when Power button pressed)	Battery over-temperature condition. Device shuts down. Battery will not charge until temperature returns to normal operating value.

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, touch  > ⓘ **About device** > **Battery Information**.

Note that charging is intelligently controlled by the MC40. To accomplish this, for small periods of time, the MC40 or accessory alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC40 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

Charging Spare Batteries

See 2 Accessories, page 2-1 for information on using accessories to charge spare batteries.

1.2.3 Powering On the MC40

If the MC40 did not turn on when the battery was installed, press the Power button until the Right and Left LEDs flash once. The splash screen displays for about a minute as the MC40 initializes its flash file system. Note that these windows also appear upon reset.

1.2.4 Replacing the Battery

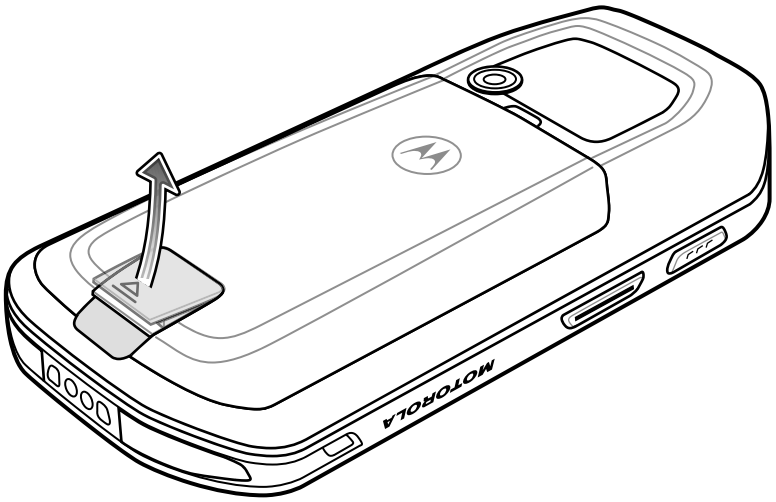
NOTE

Ensure that the Battery Swap mode procedures are followed, otherwise the backup battery will deplete quickly.

Procedure Steps

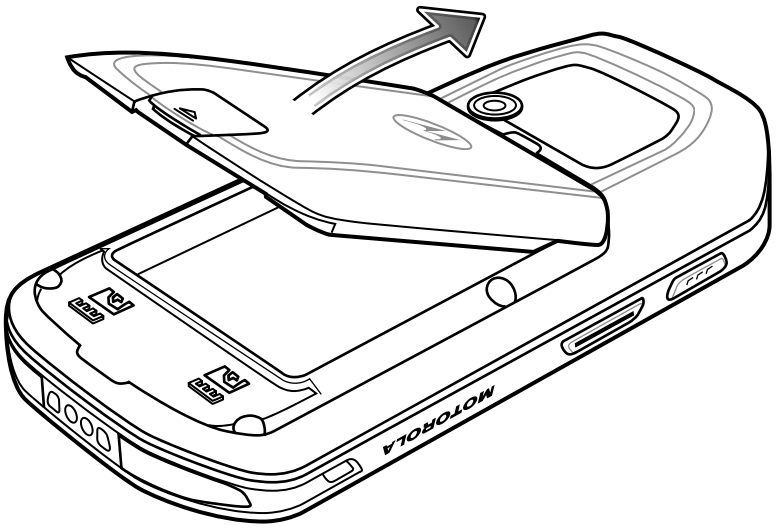
1. Press the Power button until the menu displays.
2. Touch **Battery swap**. The Right and Left LEDs light red.
3. Wait until the LEDs turns off.
4. Lift the battery latch.

Figure 1-2 Lift Battery Latch



5 Remove the battery out of the battery compartment.

Figure 1-3 Remove Battery



6 Align the replacement battery in the battery compartment.

7 Lower the battery and press down until it snaps into place.

8 Press down on the battery latch.

9 Press the Power button to turn on the MC40.

1.3 Resetting the Device

There are four reset functions:

- Soft Reset
- Hard Reset
- Enterprise Reset
- Factory Reset.

1.3.1 Performing a Soft Reset

Perform a soft reset if applications stop responding.

Procedure Steps

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

1.3.2 Performing a Hard Reset

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

Procedure Steps

1. Simultaneously press the Power, Left Scan/Action and Up Volume buttons.
2. The device shuts down and then reboots.

1.3.3 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. After the reset is complete, the MC40 installs the applications and copies the key remap configuration file back to the appropriate locations.

Procedure Steps

1. Download the Enterprise Reset file from Motorola Support Central web site.
2. Copy the **`40N0JxxERxxxxxxx.zip`** file to the root directory of the On-device Storage. See 3 USB Communication, page 3-1.
3. Press and hold the Power button until the **Device options** menu appears.
4. Touch **Reset**.
5. Touch **OK**. The device resets.
6. Press and hold the Left Scan/Action button.

7 When the Recovery Mode screen appears release the button.

Figure 1-4 Recovery Mode Screen

8 Touch ⌂. The System Recovery screen appears.

Figure 1-5 System Recovery Screen

9 Press the Up and Down Volume buttons to navigate to the **Apply update from /sdcard** option.

10 Press the PTT button.

11 Press the Up and Down Volume buttons to navigate to the **40N0JxxERxxxxxxx.zip** file.

12 Press the PTT button. The Enterprise Reset occurs and then the device resets.

1.3.4 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 9.5 Updating the System, page 9-7 for more information.

Procedure Steps

1 Download the Enterprise Reset file from Motorola Support Central web site.

2 Copy the **40N0JxxFRxxxxxxx.zip** file to the root directory of the On-device Storage. See 3 USB Communication, page 3-1.

3 Press and hold the Power button until the **Device options** menu appears.

4 Touch **Reset**.

5 Touch **OK**. The device resets.

6 Press and hold the Left Scan/Action button.

7 When the Recovery Mode screen appears release the Left Scan/Action button.

Figure 1-6 Recovery Mode Screen

8 Touch ⌂.

Figure 1-7 System Recovery Screen

9 Press the Up and Down volume buttons to navigate to the **Apply update from /sdcard** option.

10 Press the PTT button.

11 Press the Up and Down volume buttons to navigate to the **`40N0JxxFRxxxxxxx.zip`** file.

12 Press the PTT button. The Factory Reset occurs and then the device resets.

2 Accessories

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

2.1 MC40 Accessories

Table 2-1 lists the accessories available for the MC40.

Table 2-1 MC40 Accessories

Accessory	Part Number	Description
Cradles		
Single Slot Charge Only Cradle	CRDMC40XX-1000R	Charges the MC40.
Five Slot Charge Only Cradle Base	CRDUNIV-XX-5000R	Provides charging for up to five MC40 devices or four MC40 devices and one Four Slot Battery Charger using optional Charging Cups. Requires additional power supplies.
Five Slot Charge Only Cradle	CRDUNIV-40-5000R	Provides charging for up to five MC40 devices.
Chargers		
Four Slot Battery Charger	SACMC40XX-4000R	Charges up to four MC40 batteries.
Power Supply	PWRS-124306-01R	Provides power to the MC40 and Single Slot Charge Cradle.
Power Supply (12 VDC, 4.16 A)	PWRS-14000-148C	Provides power to the Five Slot Charge Only Cradle and the Four Slot Battery Charger.
Cables		
Micro USB Cable	25-MCXUSB-01R	Provides power to the MC40 and USB communication with a host computer.
US AC Line Cord (3-wire)	23844-00-00R	Provides power to the power supplies.
2-way DC Cable	25-122026-02R	Connects one power supply (PWRS-14000-148C) to two Four Slot Battery Chargers.
4-way DC Cable	25-85992-01R	Connects one power supply (PWRS-14000-241R) to four Four Slot Battery Chargers.
Miscellaneous		
Spare 2680 mAh lithium-ion battery	BTRY-MC40EAB0E	Replacement 2680 mAh battery.
	BTRY-MC40EAB0E-10R	Replacement 2680 mAh battery (10-pack)

Table 2-1 MC40 Accessories (cont'd.)

Accessory	Part Number	Description
Charging Cup	CUPMC40XX-1000R	Mounts onto the Five Slot Charge Only Cradle Base and provides MC40 charging slot (Single pack).
Battery Charger Cup	CUPUNIBTRY-1000R	Mounts on the Five Slot Charge Only Cradle Base and provides mounting for the Four Slot Battery Charger.
Universal Blank Slot Cover	CUPUNICVR-5000R	Mounts on the Five Slot Charge Only Cradle and covers a slot when a cup is not required (5-pack).
Protective Rubber Boot	SG-MC40-RBOOT-01R	Provides additional protection for the MC40.
	SG-MC40-RBOOT-10R	Provides additional protection for the MC40 (10–pack).
	SG-MC40-MBOOT-01R	Provides additional protection for the MC40 with MSR.
	SG-MC40-MBOOT-10R	Provides additional protection for the MC40 with MSR (10–pack).
Soft Hip Holster	SG-MC40HLSTR-02R	Mounts on belt and provides storage for the MC40.
Finger Strap	SG-MC40STRAP-01R	Mounts on the back of the MC40 and provides secure option for holding the device (Single pack or 10-pack).
	SG-MC40STRAP-10R	
Rack/Wall Mount Bracket	KT-UNIVLBRKT-01R	Provides for mounting the Five Slot Charge Only Cradle onto a standard rack or wall.
Mono Corded Headset	21-UNIV-HDSET1-01R	Use for PTT and VoIP telephony communications.
	21-UNIV-HDSET1-10R	Use for PTT and VoIP telephony communications (10–pack).

2.2 Single Slot Charge Only Cradle

The Single Slot Charge Only Cradle provides power for operating and charging the MC40.

NOTE

Do not connect the micro USB cable from the Single Slot Charge cradle to a host computer USB port. The cradle cannot charge the MC40 if connected to a host computer.

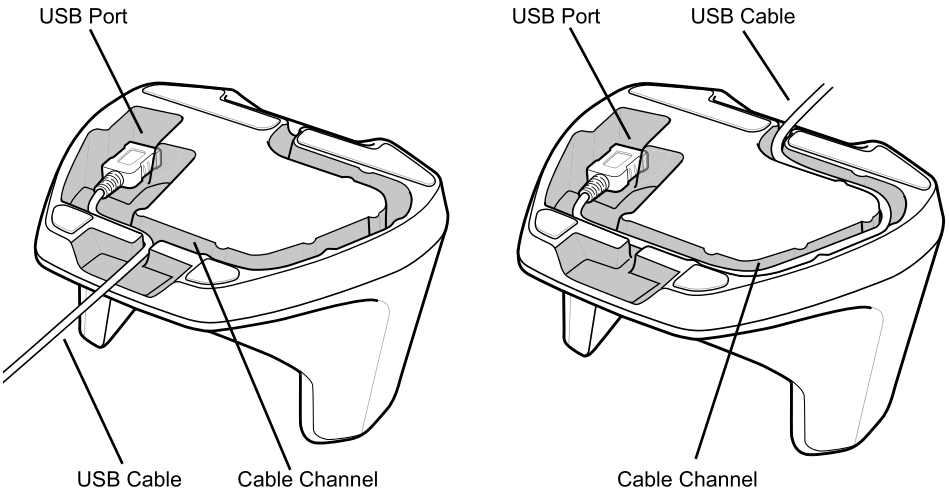
2.2.1 Single Slot Charge Cradle Setup

Procedure Steps

1 Plug the micro USB connector into the microUSB port on the cradle.

2 Route the micro USB end of the Micro USB Cable through the Cable Channel and exit either to the front or back of the cradle.

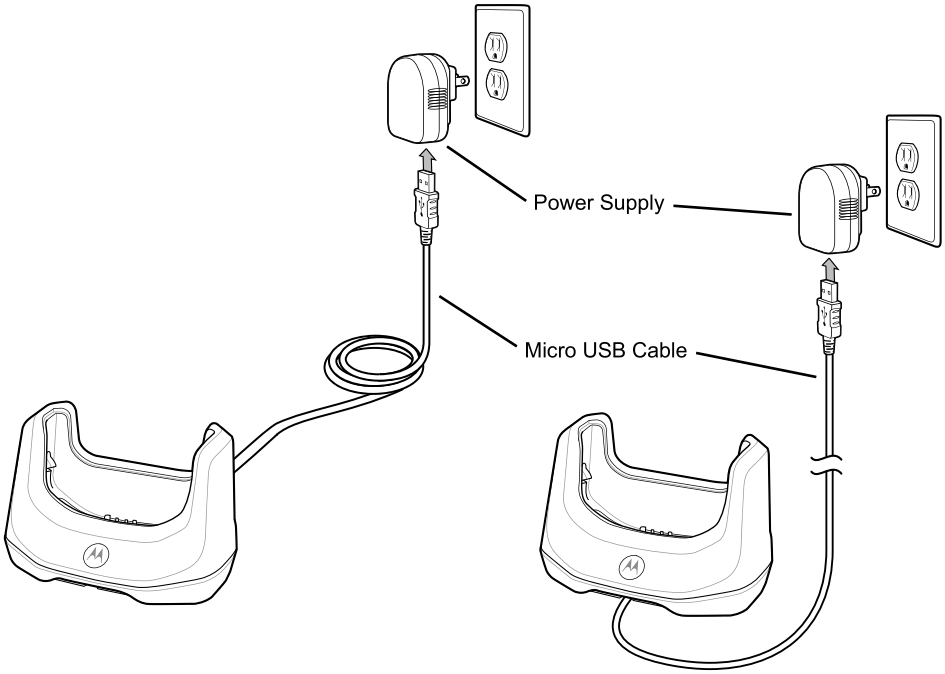
Figure 2-1 Micro USB Cable Installation



3 Plug the other end of the Micro USB Cable into the USB port on the power supply.

4 Plug the power supply into a wall outlet.

Figure 2-2 Single Slot Charge Only Cradle Setup

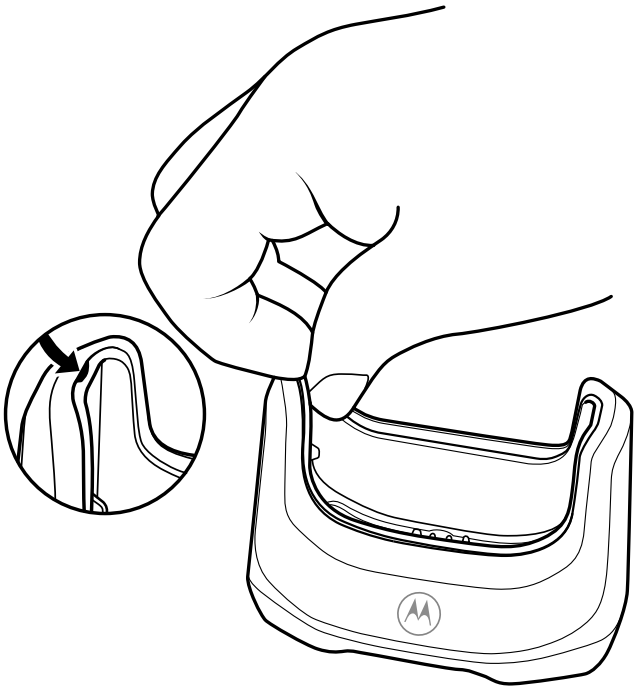


2.2.2 Removing Cradle Insert

Procedure Steps

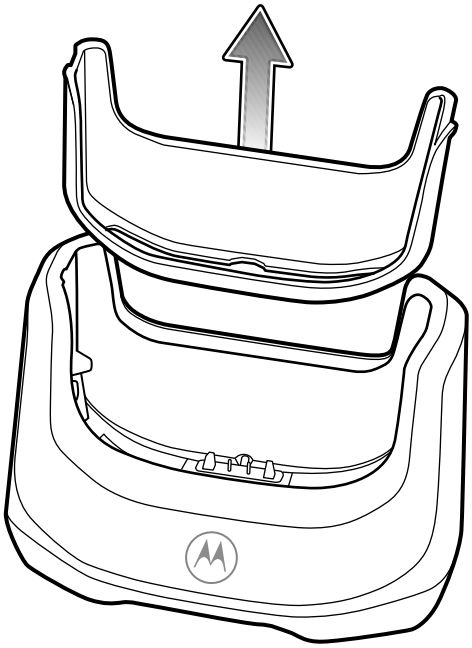
1 With finger nail, grasp insert notch.

Figure 2-3 Grasp Insert Notch



2 Pull insert out of cradle.

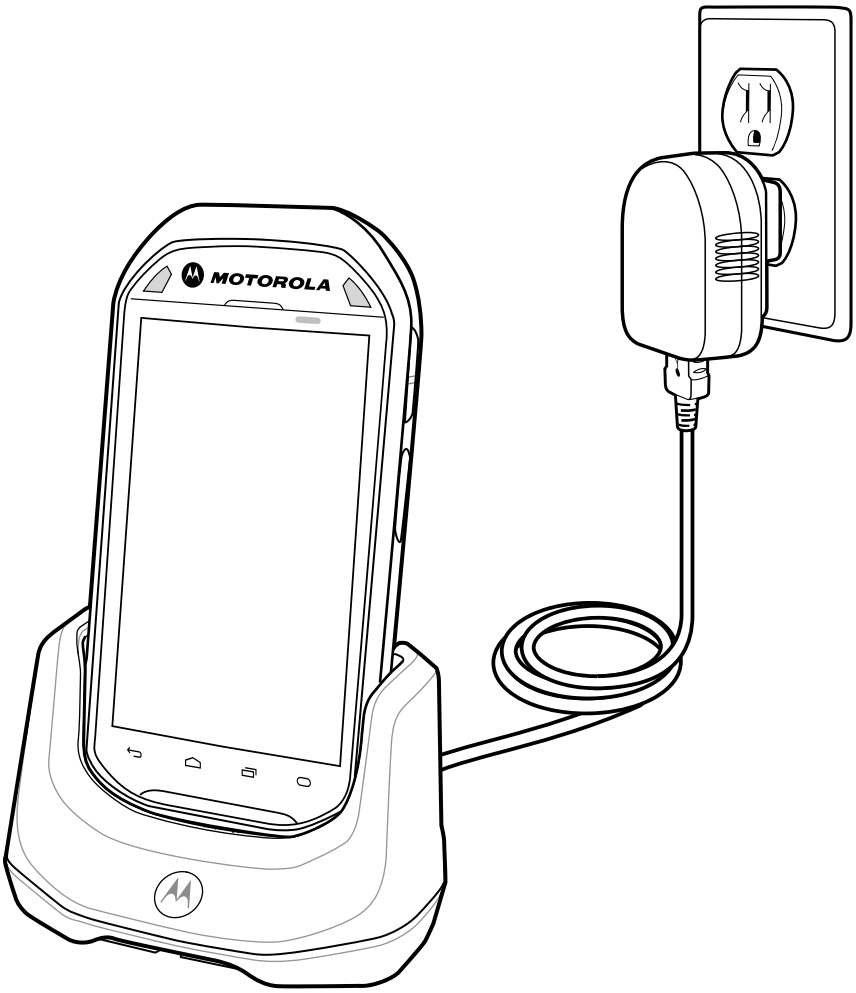
Figure 2-4 Remove Insert



2.2.3 Charging Using the Single Slot Charge Only Cradle

To charge the MC40 battery, place the MC40 into the cradle.

Figure 2-5 MC40 Battery Charging



The Right LED indicates the status of the battery charging. See Table 1-1 Battery Charge LED Status for charging status indications. The 2680 mAh battery charges in approximately four hours.

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, touch > **About device** > **Battery Information**. Charging is intelligently controlled by the MC40. To accomplish this, for small periods of time, the charger 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.

2.3 Four Slot Battery Charger

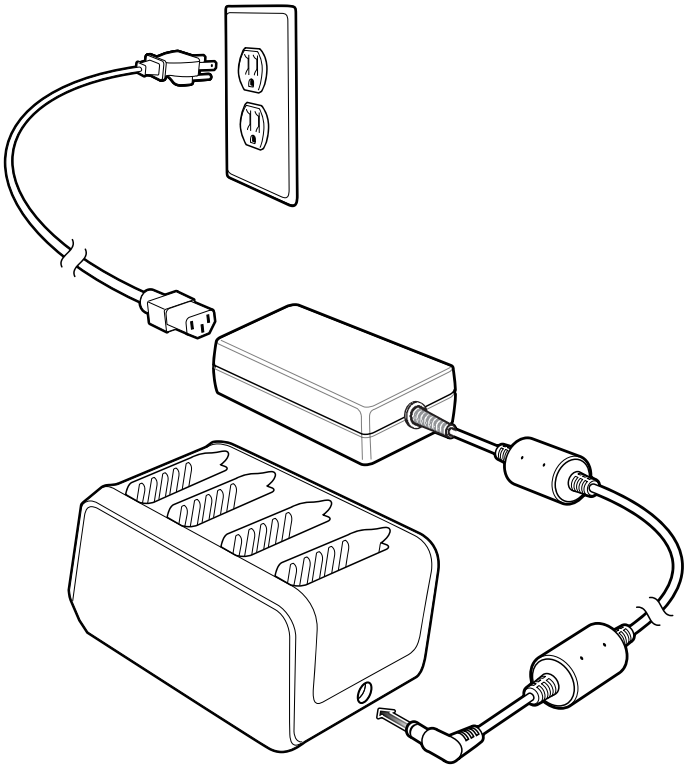
The Four Slot Battery Charger charges up to four MC40 spare batteries.

2.3.1 Single Charger Setup

Procedure Steps

1. Plug the power supply plug into the power port on the back of the charger.
2. Plug the AC line cord into the power supply.
3. Plug the AC line cord into an AC outlet.

Figure 2-6 Four Slot Battery Charger



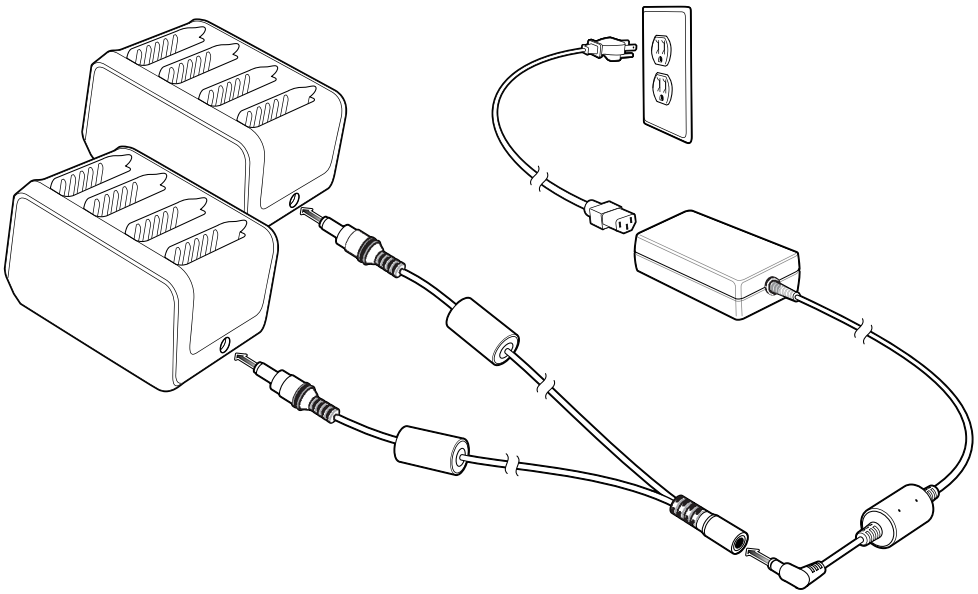
2.3.2 Two Charger Setup

Procedure Steps

1. Plug the 2-way DC Cable plugs into the power port on the back of the each charger.
2. Plug the power supply plug into the jack of the 2-way DC Cable.
3. Plug the AC line cord into the power supply.

4 Plug the AC line cord into an AC outlet.

Figure 2-7 Setup with 2–way DC Cable



2.3.3 Four Charger Setup

Procedure Steps

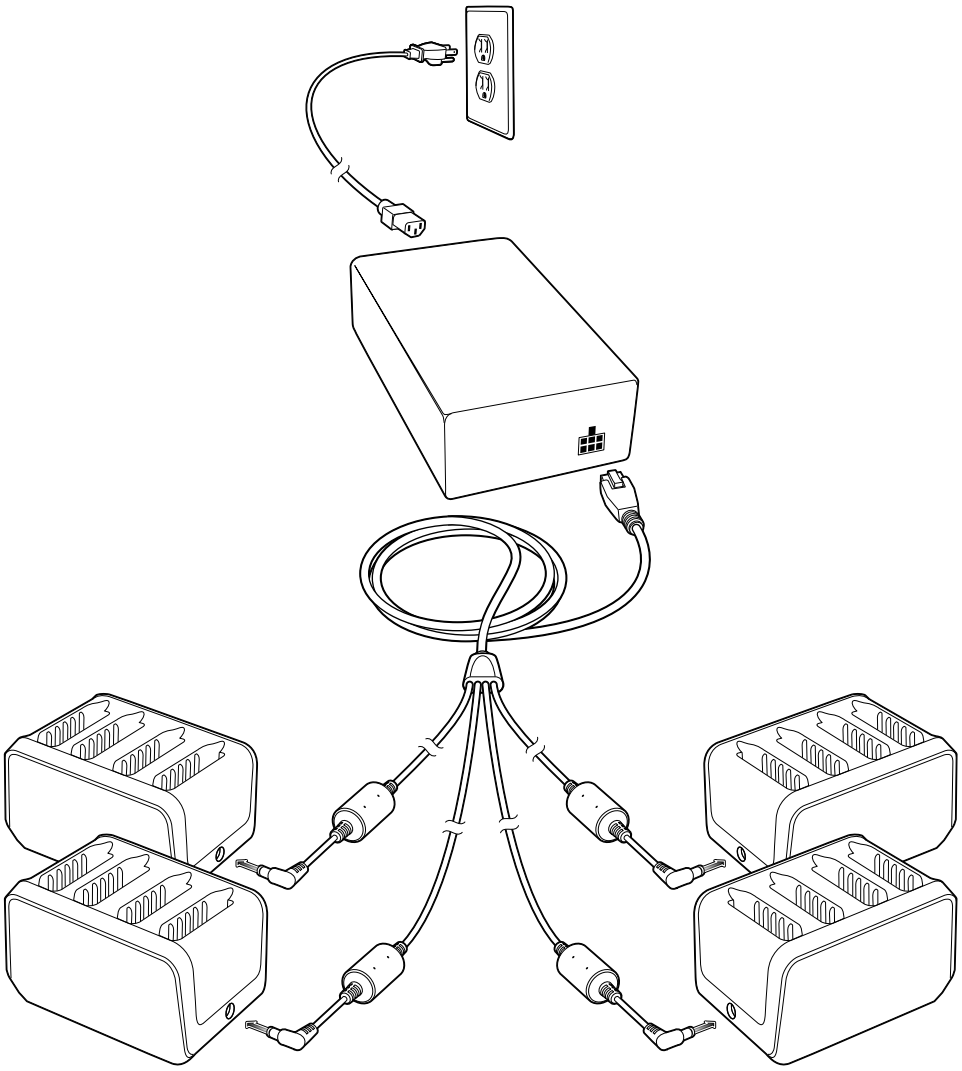
1 Plug the 4-way DC Cable plugs into the power port on the back of the each charger.

2 Plug the 4-way DC Cable connector into the power output of the power supply.

3 Plug the AC line cord into the power supply.

4 Plug the AC line cord into an AC outlet.

Figure 2-8 Setup with 4–way DC Cable

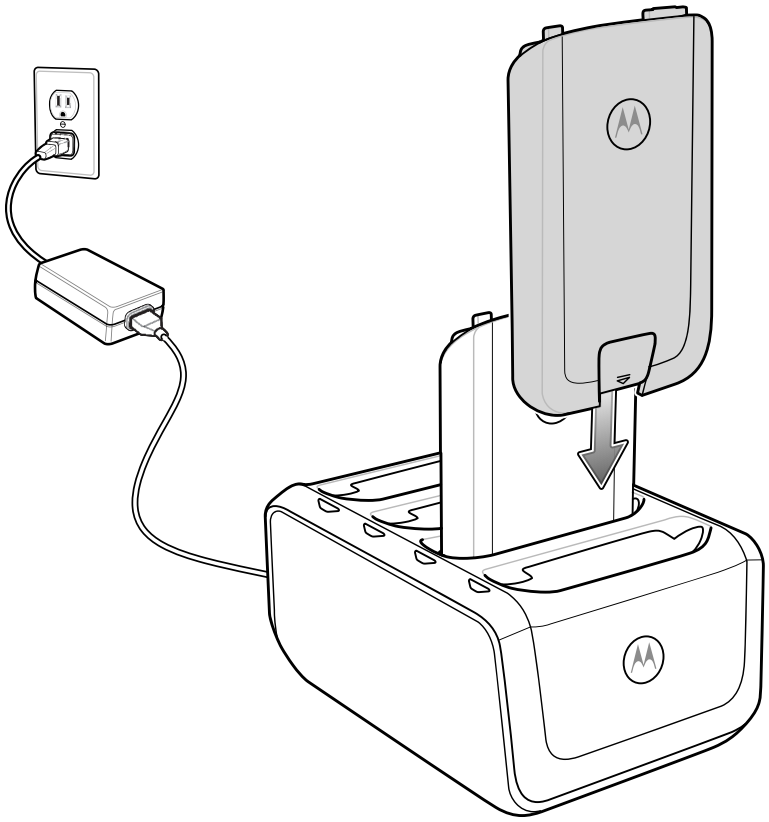


2.3.4 Charging with the Four Slot Battery Charger

To charge the spare batteries insert the spare battery into a spare battery charging well.

A Charge LED is provided for each battery charging well. See Table 2-2 Spare Battery Charge LED Status for charging status indications. The 2680 mAh battery charges in approximately four hours.

Figure 2-9 Charging Batteries



Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the charger in order to ensure safe operation and optimize long-term battery life. To accomplish this, for small periods of time, the charger 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 the Charge LED.

Table 2-2 Spare Battery Charge LED Status

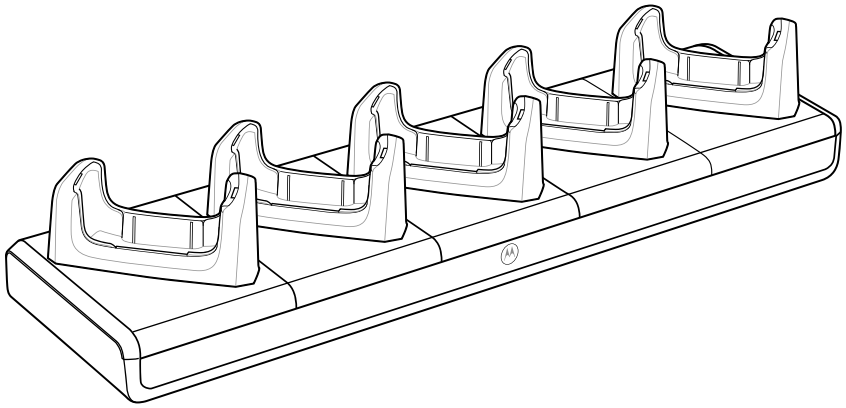
Status	Indications
Off	No battery a slot. Battery is not charging. Battery is not inserted correctly in the charger. Charger is not powered.
Slow Blinking Amber	Battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion.

2.4 Five Slot Charge Only Cradle

The Five Slot Charge Only cradle:

- Provides power for operating and charging the MC40.
- Simultaneously charges up to five MC40s.

Figure 2-10 Five Slot Charge Only Cradle



2.4.1 Installing a Cup

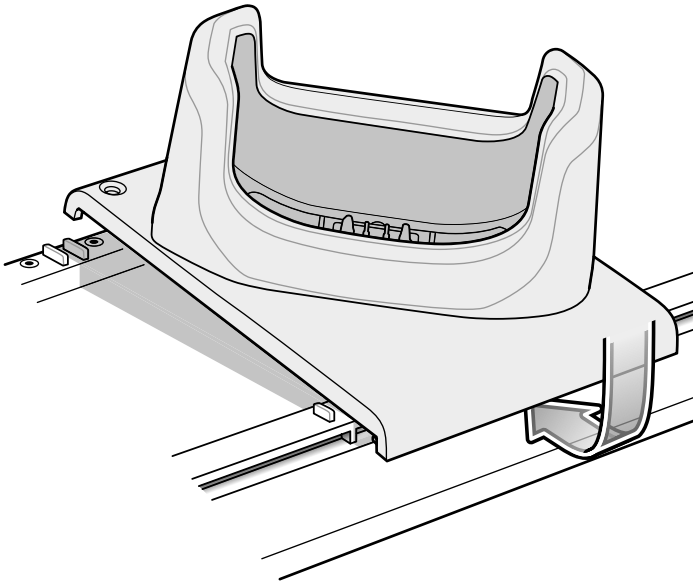
The Five Slot Charge Only Cradle ships without any cradle cups installed. To base accepts the MC40 Charging Cup, Battery Charger Cup and Blank Slot Cover. To install the cradle cups:

Procedure Steps

1 Remove power from the cradle base before installing cups.

2 Align the lip of the cup with the slot on the front of the cradle. Ensure that the cup is positioned within the Slot Alignment Tabs.

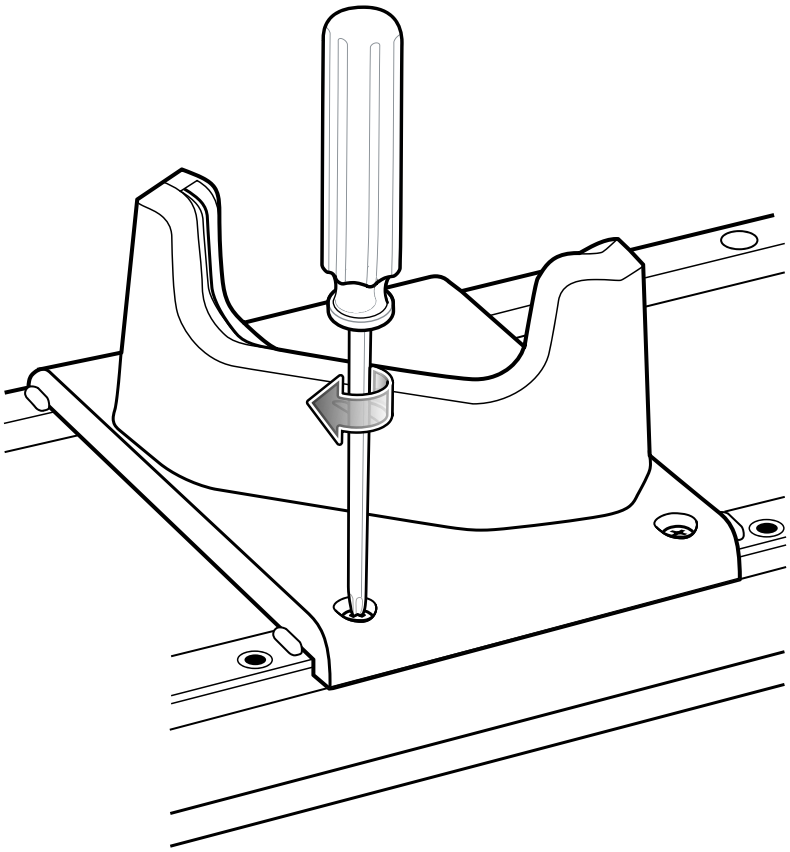
Figure 2-11 Five Slot Charge Only Cradle Cup Installation



3 Slide the lip into the slot and rotate the cup until it is flat on the cradle base.

4 Using a Phillips screwdriver, secure the cup to the charger base using the two screws provided with the cup.

Figure 2-12 Securing Cup to Base



5 Each slot on the Cradle Base must have a cup installed.

6 Repeat for each additional cup.

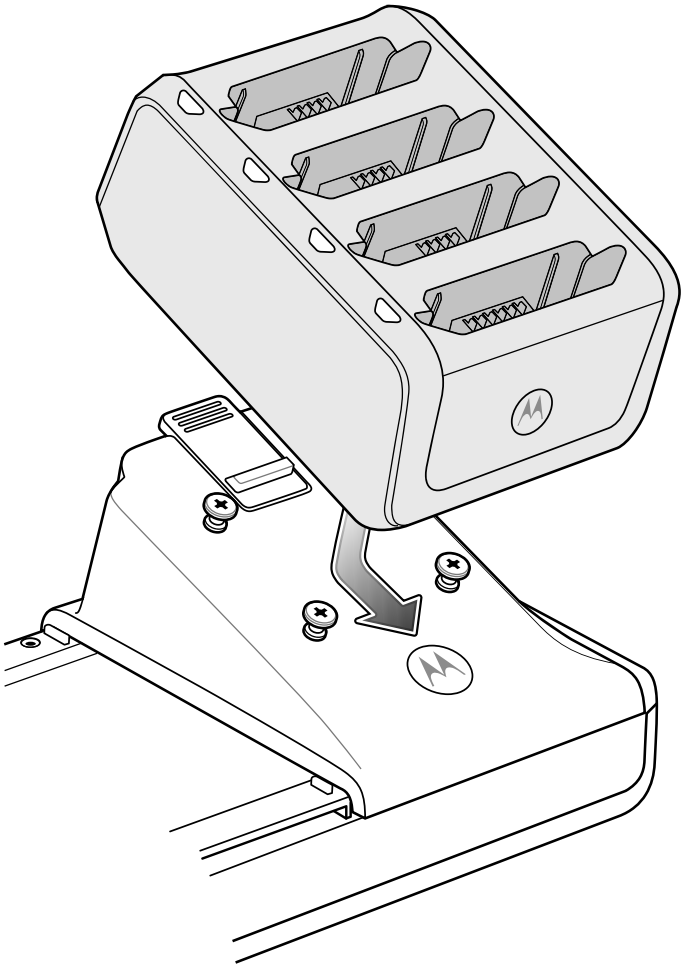
2.4.2 Installing a Four Slot Battery Charger

To install a Four Slot Battery Charger:

Procedure Steps

1. Install a Battery Charger Cup. See 2.4.1 Installing a Cup, page 2-11.
2. Align the mounting slots on the bottom of the Four Slot Battery Charger with the screws on the cup.
3. Slide the Four Slot Battery Charger down until it snaps into place.

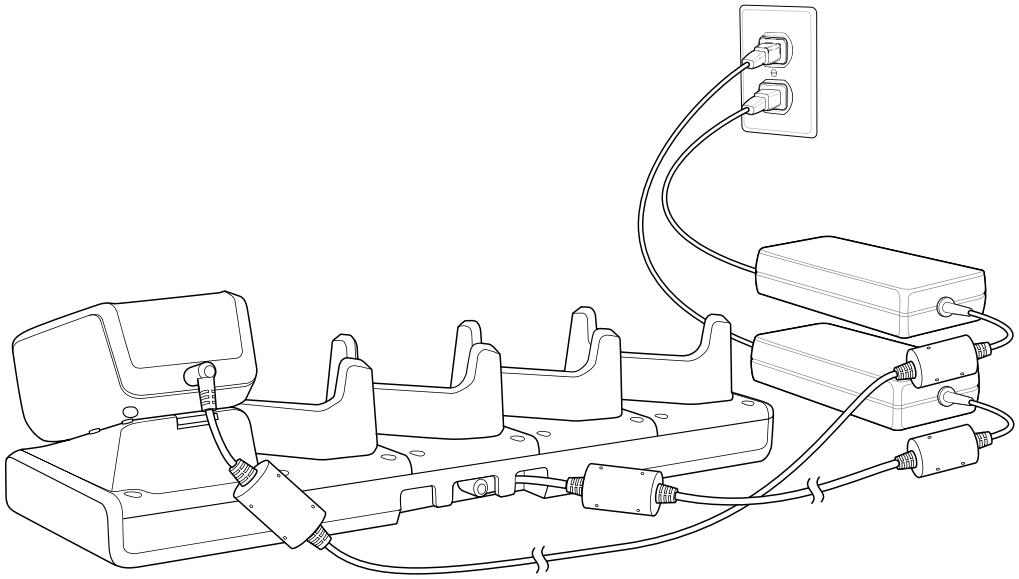
Figure 2-13 Multi Slot Charge Only Cradle Four Slot Battery Charger Installation



2.4.3 Power to Five Slot Charge Only Cradle

Use one power supply to provide power to the Charging Base to power the Charging Cups. A separate power supply is required for each Four Slot Battery Charger installed. The power supply is connected directly to the For Slot Battery Charger.

Figure 2-14 Five Slot Charge Only Cradle Power Connections

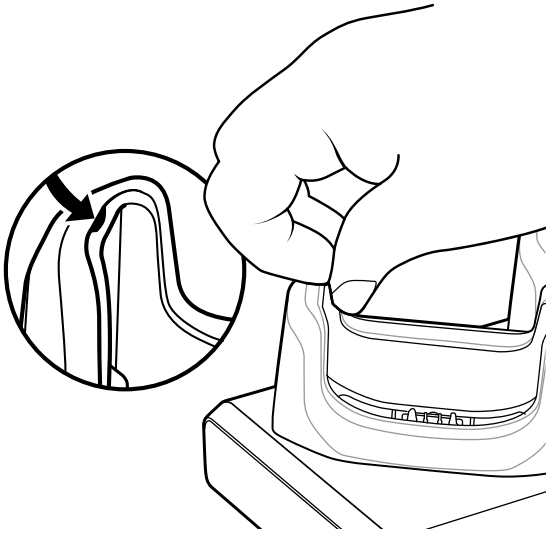


2.4.4 Removing Cradle Insert

Procedure Steps

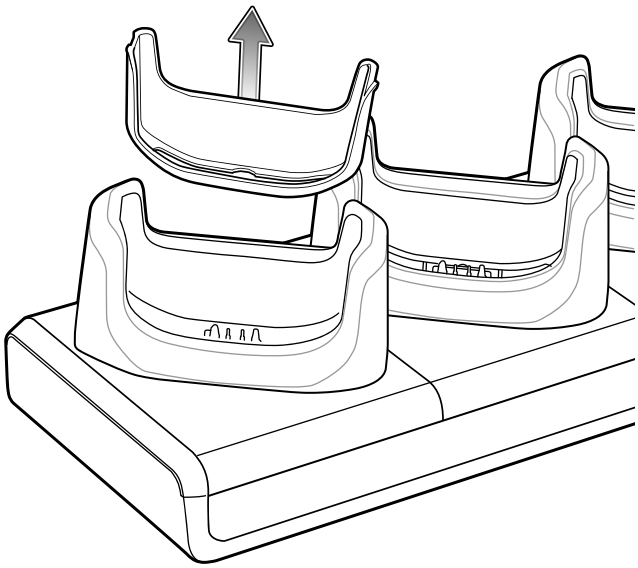
1 With finger nail, grasp insert notch.

Figure 2-15 Grasp Insert Notch



2 Pull insert out of cradle.

Figure 2-16 Remove Insert



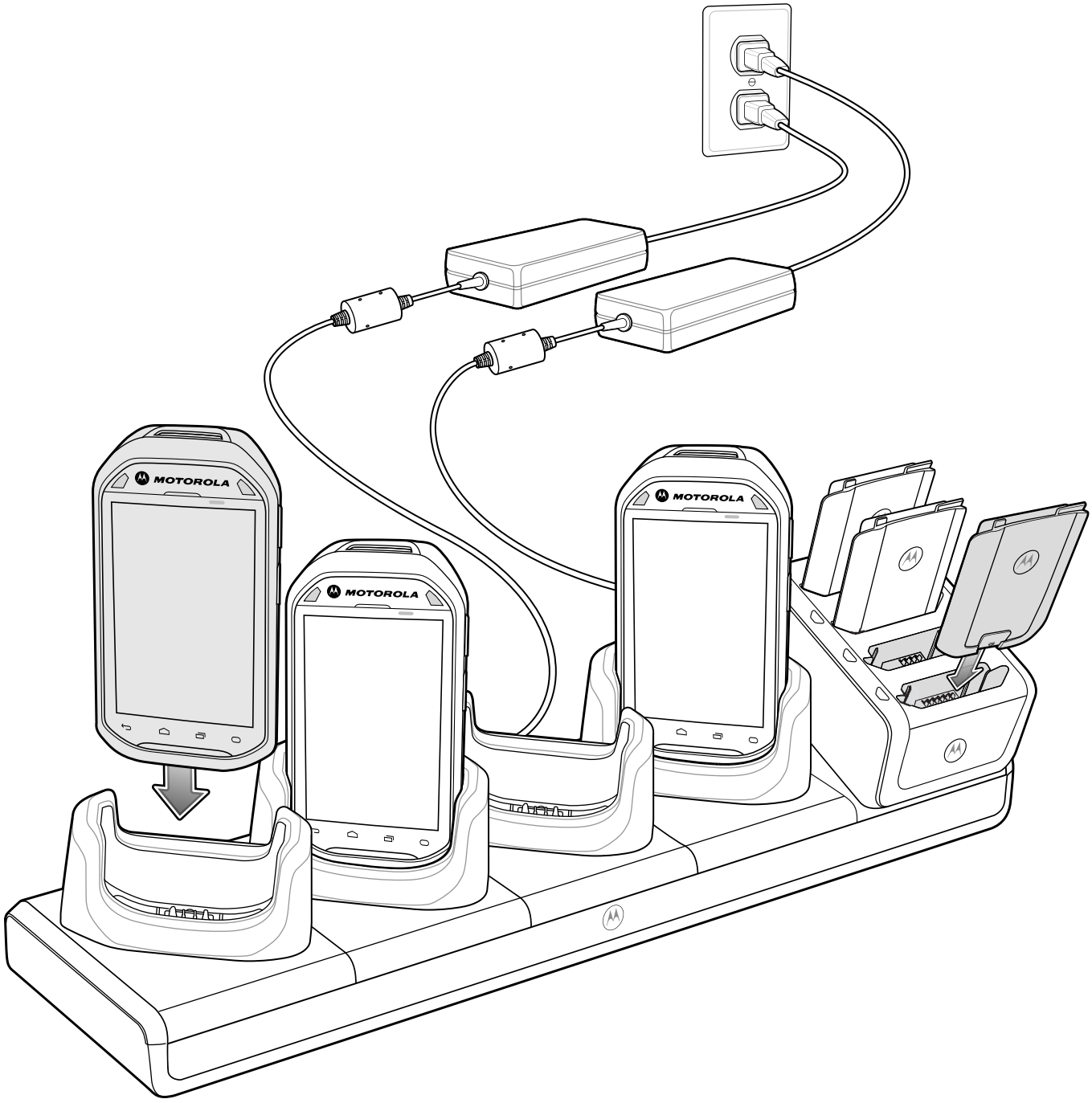
2.4.5 Charing Using the Five Slot Charge Only Cradle

Insert the MC40 into a slot to begin charging.

The Right LED indicates the status of the battery charging in the MC40. See Table 1-1 Battery Charge LED Status for charging status indications. The 2680 mAh battery charges in approximately four hours.

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, touch > **About device** > **Battery Information**. Charging is intelligently controlled by the MC40. To accomplish this, for small periods of time, the charger 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.

Figure 2-17 Charging MC40 and Spare Battery



2.5 Installing the Finger Strap

Use the optional finger strap to securely hold the MC40 while working.

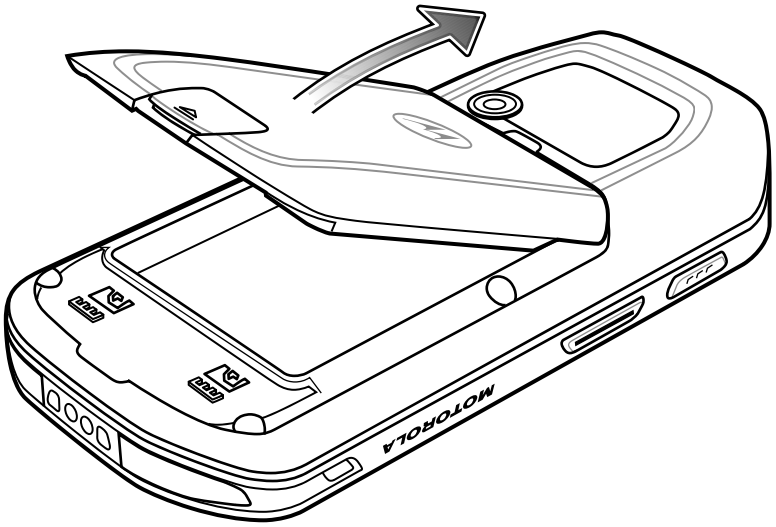
Procedure Steps

1 Press the Power button until the Device options menu appears.

2 Touch Power off.

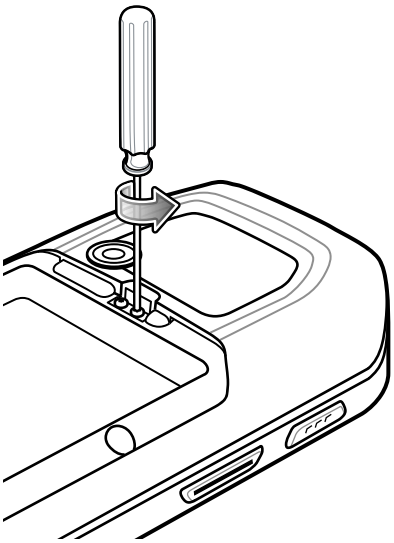
3 Remove the battery.

Figure 2-18 Remove Battery



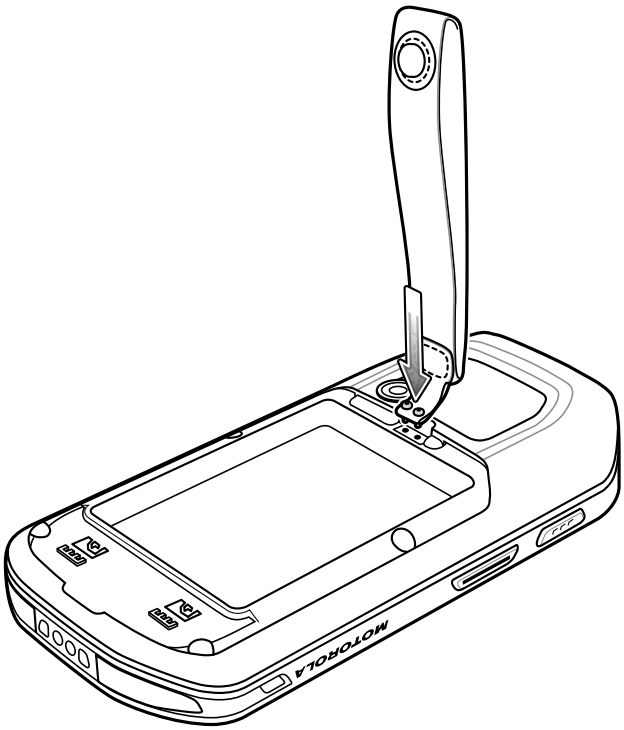
4 Using a Phillips screwdriver, remove the two screws securing the rubber plug to the MC40.

Figure 2-19 Remove Rubber Plug



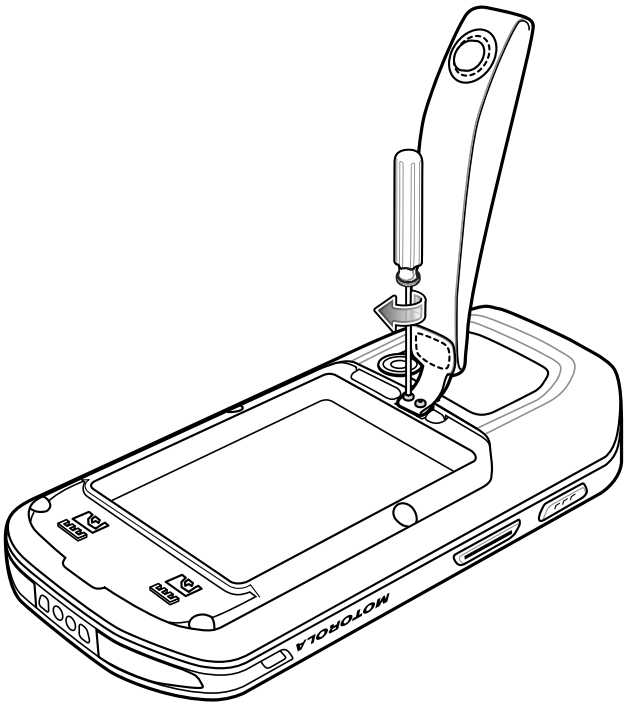
5 Align the screws in the bracket of the finger strap with the mounting holes on the MC40.

Figure 2-20 Align Finger Strap



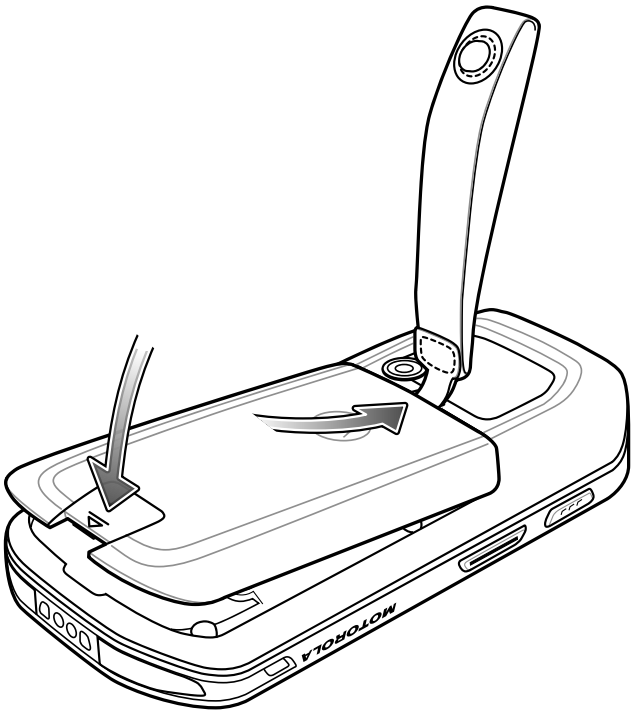
6 Secure the finger strap to the MC40 using a Phillips screwdriver.

Figure 2-21 Secure Finger Strap to MC40



7 Replace the battery.

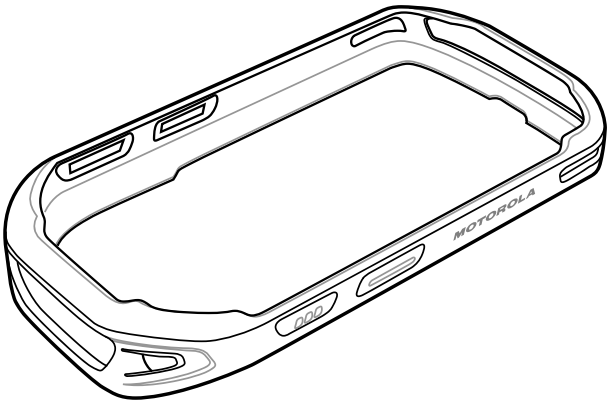
Figure 2-22 Install Battery



2.6 Installing the Rubber Boot

Use to rubber boot to add additional protection to the MC40.

Figure 2-23 Rubber Boot



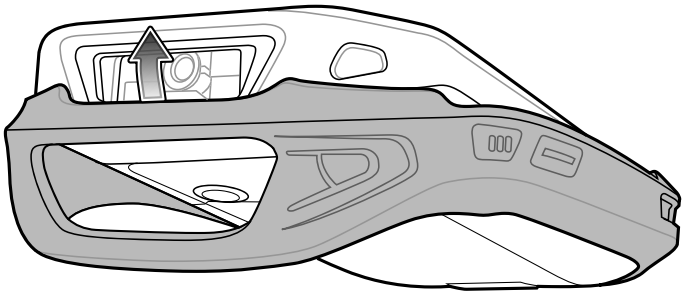
Procedure Steps

1 Insert the bottom of the MC40 into the bottom of the rubber boot.

Figure 2-24 Insert MC40 into Boot

2 Pull the top of the rubber boot over the top of the MC40.

Figure 2-25 Pull Boot Over MC40



3 Ensure that the rubber boot is sitting flat against the MC40.

3 USB Communication

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

3.1 Connecting to a Host Computer via USB

Connect the device to a host computer using the micro USB cable to transfer files between the MC40 and the host computer.

CAUTION

When connecting the MC40 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure Steps

1. Connect the micro USB connector to the USB port on the device. See 2 Accessories, page 2-1 for setup information.
2. Connect the USB A connector to the host computer USB port.

   Step result: Connected as a media device or **Connected as camera** appears on the Status bar.
3. If **Connected as a camera** appears, pull down the Notification shade and touch **Connected as a camera** and then touch **Media device (MTP)**.
4. 

   CAUTION

   Ensure that all applications are not running. Loss of data may occur.

   On the host computer, open a file explorer application.
5. 

   NOTE

   While USB storage is in use, access to the On-Device Storage is disabled.

   Locate the device as a portable device and open to view contents.
6. Copy or delete files as required.

3.2 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 Steps

1. On the host computer, unmount the device.
2. Remove the micro USB cable from the device.

4 DataWedge Configuration

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

4.1 Basic Scanning

Scanning can be performed using either the imager or the rear-facing camera.

4.1.1 Using the Camera

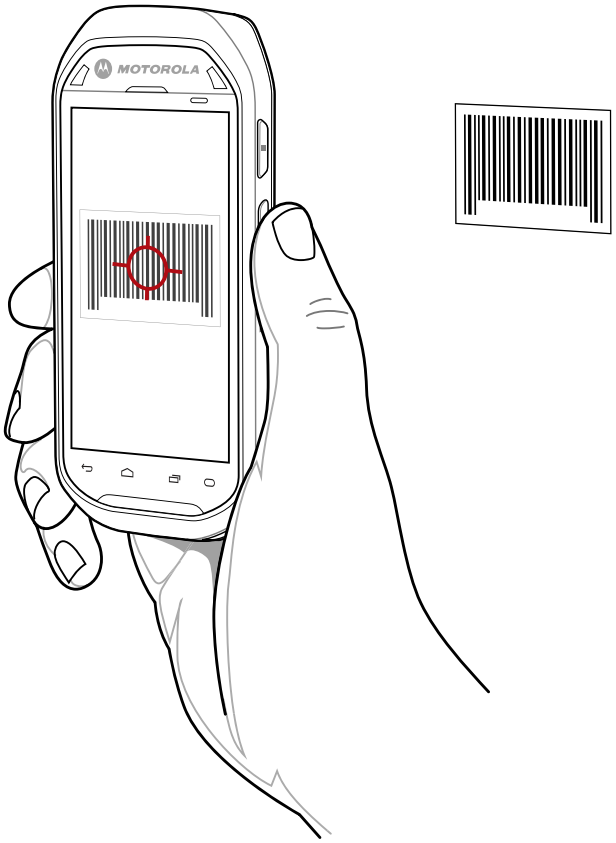
To capture bar code data:

Procedure Steps

1. Ensure that an application is open on the MC40 and a text field is in focus (text cursor in text field).
2. Aim the rear-facing camera at a bar code.

3 Press and hold the Right Scan/Action button. By default, a preview window appears on the screen. The Left and Right LEDs light red to indicate that data capture is in process.

Figure 4-1 Data Capture with Camera



4 Move the MC40 until the bar code is centered under the red target.

5 The Left and Right LEDs light green, a beep sounds and the MC40 vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

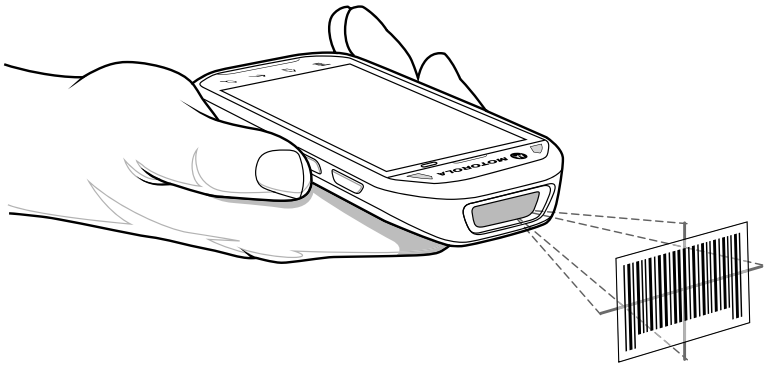
4.1.2 Using the Imager

To capture bar code data:

Procedure Steps

1. Ensure that an application is open on the MC40 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 Right Scan/Action 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 Left and Right LEDs light red to indicate that data capture is in process.

Figure 4-2 Data Capture



4. The Left and Right LEDs light green, a beep sounds and the MC40 vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

4.2 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.

4.3 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.
- **MSR Input Plug-in** – The Magnetic Stripe Reader (MSR) Input Plug-in is responsible for reading data from an MSR. Raw data read from the MSR can be processed or formatted using Process Plug-ins as required.

DataWedge has built-in feedback functionality for the MSR 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.

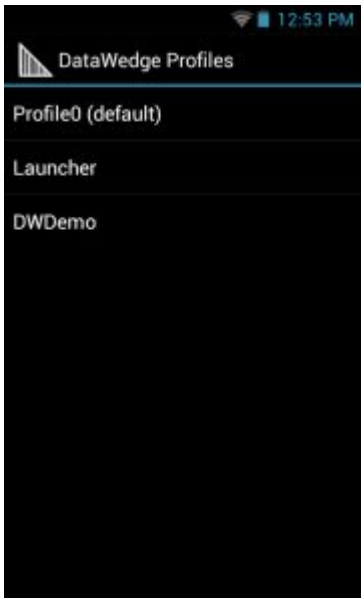
4.4 Profiles Screen

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 4-3 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.

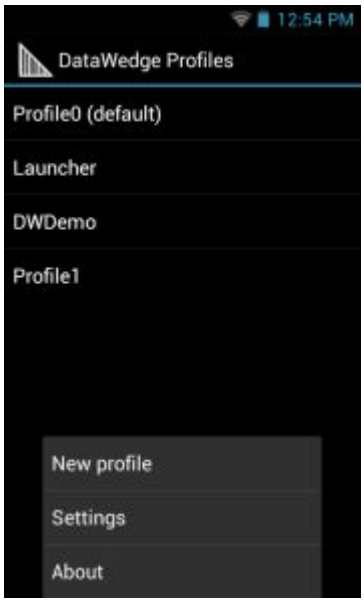
Figure 4-4 Profile Context Menu

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

Options Menu

Touch to open the options menu.

Figure 4-5 DataWedge Options Menu



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

4.4.1 Disabling DataWedge

Procedure Steps

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

4.5 Creating a New Profile

Procedure Steps

1 Touch .

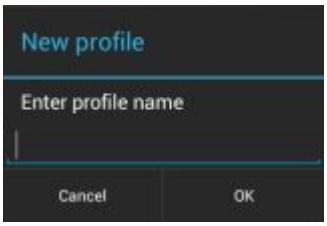
2 Touch .

3 Touch .

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 4-6 New Profile Name Dialog Box



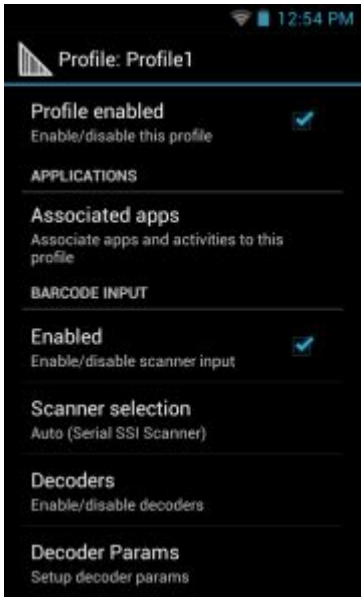
6 Touch **OK**.

Step result: The new profile name appears in the **DataWedge profile** screen.

4.6 Profile Configuration

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

Figure 4-7 Profile Configuration Screen



The configuration screen lists the following sections:

- Profile enabled
- Applications
- Barcode Input
- MSR Input
- Keystroke output
- Intent Output
- IP Output.

4.6.1 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.
- **Camera scanner** - Scanning is performed with the rear-facing camera.
- **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	

Touch ⮌ 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths 4 (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 10). See Decode Lengths, page 4-14 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).

- **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, page 4-14 for more information.

- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length 2** - Use to set decode lengths (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 14). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 55). See Decode Lengths, page 4-14 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, page 4-14 for more information.
  - **Length2** - Use to set decode lengths (default - 0). See Decode Lengths, page 4-14 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 or disable this option. 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.

    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.

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).

4.6.2 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.

4.6.3 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 or MSR 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 4.7 Generating Advanced Data Formatting Rules, page 4-25 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).

4.6.4 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
  - 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 4.7 Generating Advanced Data Formatting Rules, page 4-25 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).

4.6.4.1 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.getStringtExtra()` and `Intent.getSerializableExtra()` calls, using the following String tags:

- String LABEL_TYPE_TAG = "com.motorolasolutions.emdk.datawedge.label_type";
  - String contains the label type of the bar code.

- String DATA_STRING_TAG = “com.motorolasolutions.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.motorolasolutions.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.

The MSR related data added to the Intent's bundle can be retrieved using the Intent.getStringtExtra() and Intent.getSerializableExtra() calls, using the following String tags:

- String MSR_DATA_TAG = “com.motorolasolutions.emdk.datawedge.msr_data”;
  - String contains the output data as a String. The data from the MSR tracks is concatenated and sent out as a single string.
- String MSR_TRACK1_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1”;
  - MSR track 1 data is returned as a byte array.
- String MSR_TRACK2_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2”;
  - MSR track 2 data is returned as a byte array.
- String MSR_TRACK3_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3”;
  - MSR track 3 data is returned as a byte array.
- String MSR_TRACK1_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1_status”;
  - MSR track 1 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK2_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2_status”;
  - MSR track 2 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK3_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3_status”;
  - MSR track 3 decode status as an Integer where 0 indicates a successful decode.

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.

4.6.5 IP Output

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.

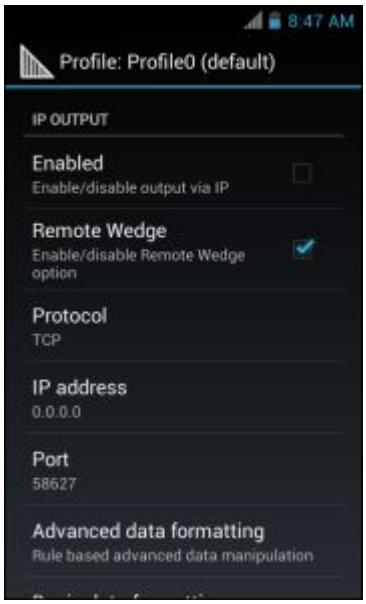
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.

- **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 4.7 Generating Advanced Data Formatting Rules, page 4-25 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 4-8 IP Output Screen



4.6.5.1 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 Steps

1. In **IP Output**, touch **Enabled**.

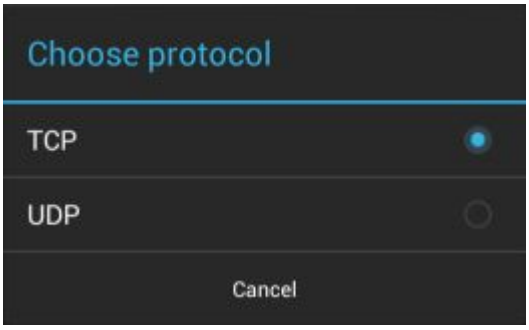
   Step result: A check appears in the checkbox.

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).

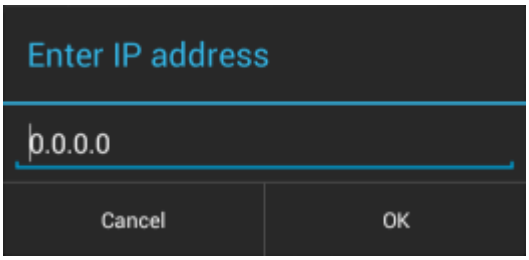
Figure 4-9 Protocol Selection



5 Touch **IP Address**.

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

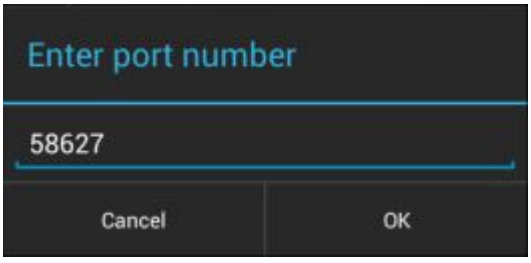
Figure 4-10 IP Address Entry



7 Touch **Port**.

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

Figure 4-11 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.

4.6.5.2 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 Steps

1 In **IP Output**, touch **Enabled**.

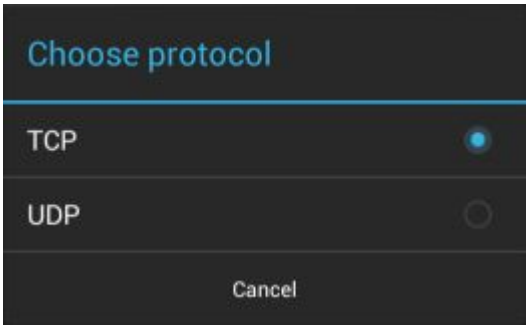
Step result: A check appears in the checkbox.

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).

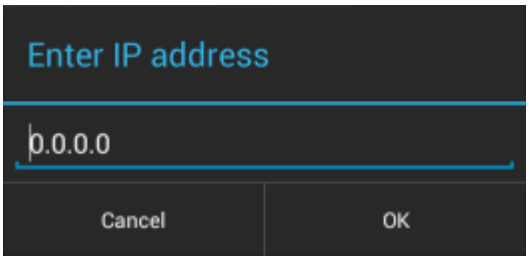
Figure 4-12 Protocol Selection



5 Touch **IP Address**.

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

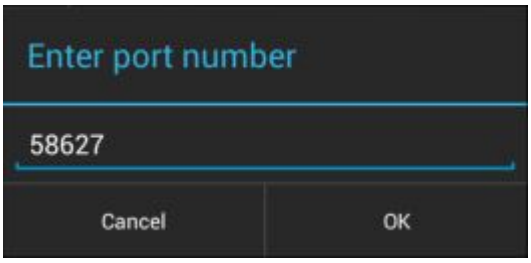
Figure 4-13 IP Address Entry



7 Touch **Port**.

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

Figure 4-14 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.

4.7 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.

4.7.1 Configuring ADF Plug-in

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

Procedure Steps

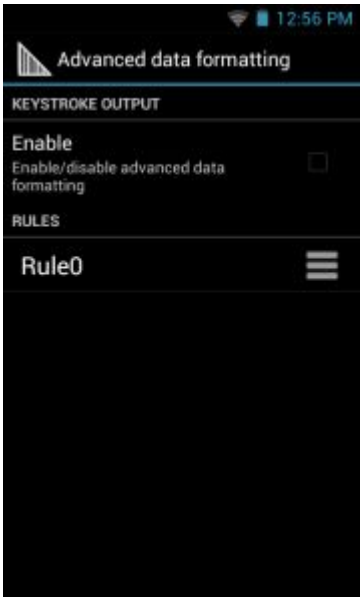
1 Touch .

2 Touch .

3 Touch a DataWedge profile.

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

Figure 4-15 Advanced Data Formatting Screen



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

4.7.1.1 Creating a Rule

NOTE

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

Procedure Steps

1 Touch the .

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**.

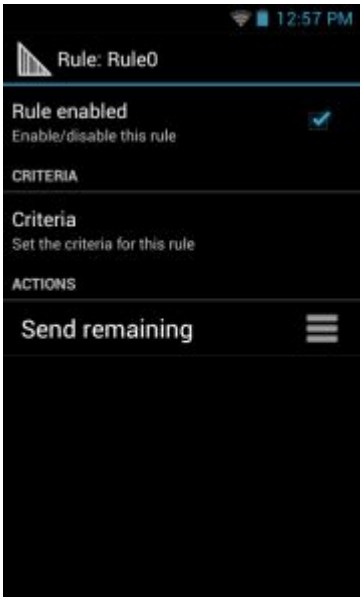
6 Touch **OK**.

4.7.1.2 Defining a Rule

Procedure Steps

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

Figure 4-16 Rule List Screen



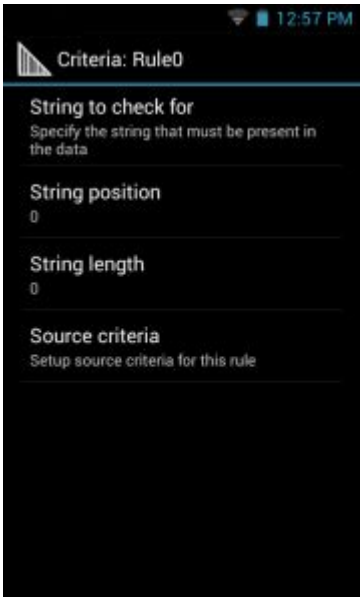
2 Touch the **Rule enabled** checkbox to enable the current rule.

4.7.1.3 Defining Criteria

Procedure Steps

1 Touch **Criteria**.

Figure 4-17 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.

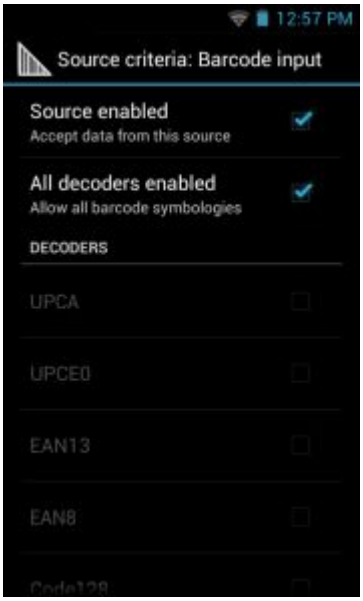
11 Touch **OK**.

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** or **MSR input**. Options vary depending upon the device configuration.

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

Figure 4-18 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 Touch ⮌ until the **Rule** screen appears.

17 If required, repeat steps to create another rule.

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

4.7.1.4 Defining an Action

NOTE

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

Procedure Steps

1. Touch  .
2. Touch **New action**.
3. In the **New action** menu, select an action to add to the **Actions** list. See Table 4-1 ADF Supported Actions 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. Touch  .
7. Touch  .

4.7.1.5 Deleting a Rule

Procedure Steps

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.

4.7.1.6 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 4-1 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.
	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).

4.7.1.6.1 Deleting an Action

Procedure Steps

1 Touch and hold the action name.

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

4.7.1.7 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 Steps

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 Touch ⮌ three times.

21 Touch and hold on the **Send remaining rule** until a menu appears.

22 Touch **Delete action**.

23 Touch ▭.

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 Touch ⮌ three times.

30 Touch ▭.

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 Touch ⮌ three times.

38 Touch ▭.

39 Touch **New action**.

40 Select **Send char**.

41 Touch **Send char** rule.

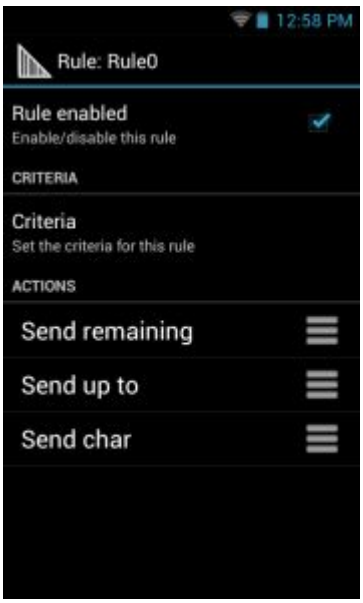
42 Touch **Character code**.

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

44 Touch **OK**.

45 Touch ⮌.

Figure 4-19 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 4-20 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 light green, a beep sounds and the device vibrates, by default, to indicate the bar code was decoded successfully. The formatted data 000129X<space>appears in the text field.

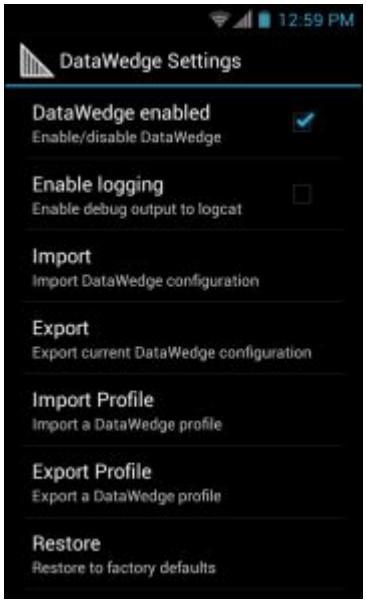
Scanning a Code 39 bar code of 1299X15598 does not transmit data (rule is ignored) because the bar code data did not meet the length criteria.

Figure 4-21 Formatted Data

4.8 DataWedge Settings

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

Figure 4-22 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.

4.8.1 Importing a Configuration File

Procedure Steps

1. Copy the configuration file to the root of the On-Device Storage.
2. Touch  .
3. Touch  .
4. Touch  .
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.

4.8.2 Exporting a Configuration File

Procedure Steps

1. Touch  .
2. Touch  .
3. Touch  .
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 MC40 On-device Storage.

4.8.3 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 Steps

1 Copy the profile file to the root of the On-Device Storage.

2 Touch .

3 Touch .

4 Touch .

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.

4.8.4 Exporting a Profile

Procedure Steps

1 Touch .

2 Touch .

3 Touch .

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 MC40 On-device Storage.

4.8.5 Restoring DataWedge

To restore DataWedge to the factory default configuration:

Procedure Steps

1 Touch  .

2 Touch  .

3 Touch  .

4 Touch **Settings**.

5 Touch **Restore**.

6 Touch **Yes**.

4.9 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 On-device Storage. 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 theOn—device Storage 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.

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.

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.

4.10 Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

4.10.1 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.

4.10.2 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.

4.10.3 Disable DataWedge on MC40 and Mass Deploy

To disable DataWedge and deploy onto multiple MC40 devices:

Procedure Steps

1. Touch  .
2. Touch **DataWedge**.
3. Touch  .
4. Touch **Settings**.
5. Unselect the **DataWedge enabled** check box.
6. Export the DataWedge configuration. See 4.8.2 Exporting a Configuration File, page 4-37 for instructions. See 4.9 Configuration and Profile File Management, page 4-39 for instructions for using the auto import feature.

4.10.4 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.motorolasolutions.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”

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

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

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

Sample

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

5 WLAN Configuration

The MC40 supports the following WLAN security options:

- Open
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)/WPA2 Personal (PSK)
- Extensible Authentication Protocol (EAP)
  - Lightweight Extensible Authentication Protocol (LEAP)
  - Protected Extensible Authentication Protocol (PEAP) - with Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) and Generic Token Card (GTC) authentication.
  - EAP-Flexible Authentication via Secure Tunneling (FAST) - with MSCHAPv2 and GTC authentication.
  - EAP-Transport Layer Security (TLS)
  - EAP-TTLS - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.

5.1 Connecting to a Wi-Fi Network

NOTE

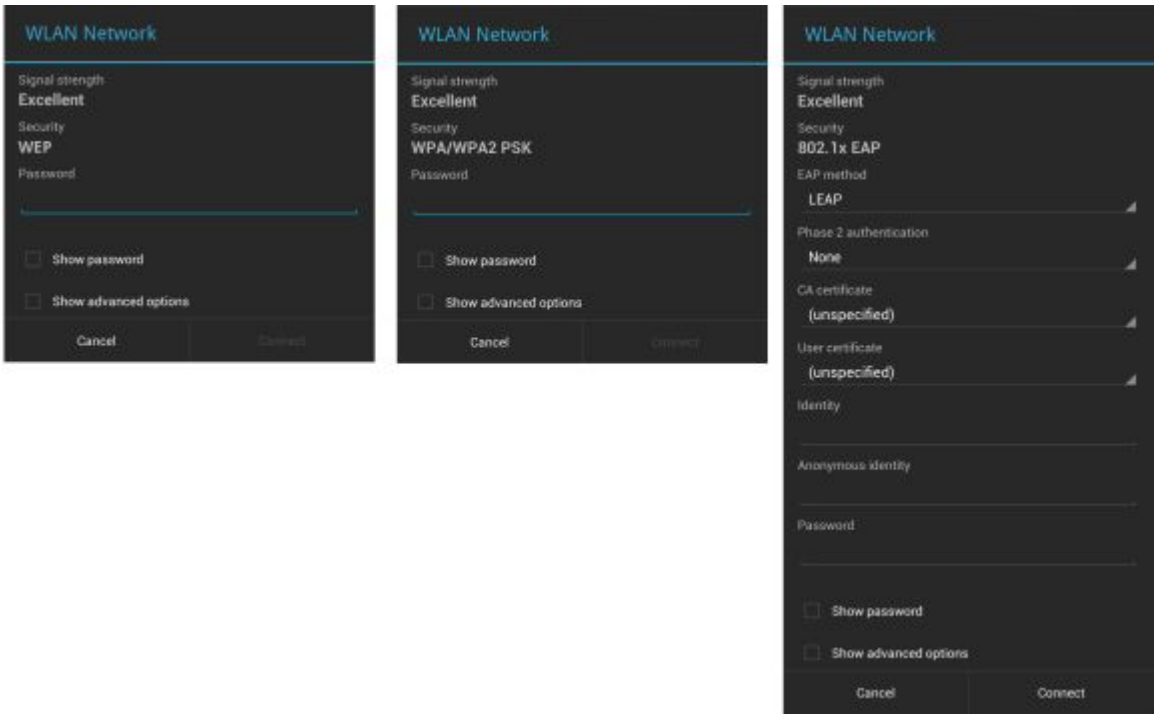
By default, the network Proxy is set to None and the IP settings is set to DHCP. See 5.3 Configuring for a Proxy Server, page 5-4 for setting connection to a proxy server and see 5.4 Configuring the Device to Use a Static IP Address, page 5-5 for setting the device to use a static IP address.

Procedure Steps

1. Touch  .
2. Touch  **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position. The device searches for WLANs in the area and displays them in the list. Open networks are indicated with  and secure networks are indicated with  .

4 Scroll through the list and touch the desired WLAN network.

Figure 5-1 WLAN Network Security Dialog Boxes



5 **NOTE**

Touch **Show password** checkbox to display password as it is entered.

Enter the required password. or other credentials then touch **Connect**. See the system administrator for more information.

6 The MC40 obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the MC40 with a fixed internet protocol (IP) address, see the *MC40 Integrator Guide*.

7 The MC40 obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the MC40 with a fixed internet protocol (IP) address, see the *MC40 Integrator Guide*.

8 When the device connects to the network, the network name appears at the top of the list and **Connected** appears below the network name.

5.2 Manually Adding a Wi-Fi Network

Manually add a Wi-Fi network if the network does not broadcast its name (SSID) or to add a Wi-Fi network when out of range.

Procedure Steps

1. Touch  .
2. Touch  **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Touch + at the bottom of the screen.
5. In the **Network SSID** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, select the type of security. Options:
   - **None**
   - **WEP**
   - **WPA/WPA2 PSK**
   - **802.1x EAP**.
7. If the network security is **None**, touch **Save**.
8. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password and then touch **Save**.
9. If the network security is **802.1x EAP**:
   - Touch the **EAP method** drop-down list and select **PEAP**, **TLS** or **TTLS**.
   - Touch the **Phase 2 authentication** drop-down list and select an authentication method.
   - If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
   - If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the **Security** settings.
   - If required, in the **Identity** text box, enter the username credentials.
   - If desired, in the **Anonymous** identity text box, enter an anonymous identity username.
   - If required, in the **Password** text box, enter the password for then given identity.

10 NOTE

By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See 5.3 Configuring for a Proxy Server, page 5-4 for setting connection to a proxy server and see 5.4 Configuring the Device to Use a Static IP Address, page 5-5 for setting the device to use a static IP address.

Touch **Connect**.

11 Touch .

5.3 Configuring for a Proxy Server

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

It is important for enterprise customers to be able to set up secure computing environments within their companies, and proxy configuration is an essential part of doing that. Proxy configuration acts as a security barrier ensuring that the proxy server monitors all traffic between the Internet and the intranet. This is normally an integral part of security enforcement in corporate firewalls within intranets.

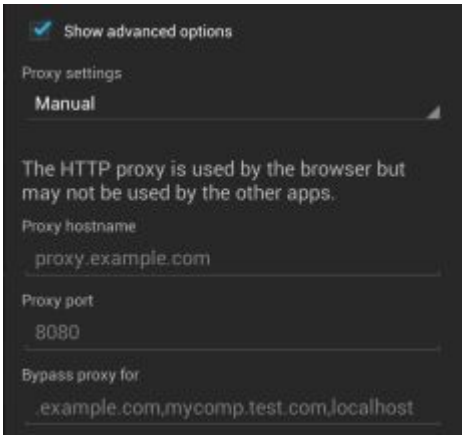
Procedure Steps

1 In the network dialog box, touch a network.

2 Touch **Show advanced options** checkbox.

3 Touch **Proxy settings** and select **Manual**.

Figure 5-2 Proxy Settings



4 In the **Proxy hostname** text box, enter the address of the proxy server.

5 In the **Proxy port** text box, enter the port number for the proxy server.

NOTE

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

6 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.

7 Touch **Connect**.

8 Touch .

5.4 Configuring the Device to Use a Static IP Address

By default, the device is configured to use Dynamic Host Configuration Protocol (DHCP) to assign an Internet protocol (IP) address when connecting to a wireless network. To configure the device to connect to a network using a static IP address:

Procedure Steps

1. In the network dialog box, touch a network.
2. Touch **Show advanced options** checkbox.
3. Touch **IP settings** and select **Static**.

Figure 5-3 Static IP Settings

4. In the **IP address** text box, enter an IP address for the device.
5. If required, in the **Gateway** text box, enter a gateway address for the device.
6. If required, in the **Network prefix length** text box, enter a the prefix length.
7. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
8. If required, in the **DNS 2** text box, enter a DNS address.
9. Touch **Connect**.
10. Touch .

5.5 Advanced Wi-Fi Settings

NOTE

Advanced Wi-Fi settings are for the device not for a specific wireless network.

Use the **Advanced** settings to configure additional Wi-Fi settings. Touch > **Advanced** to view the advanced settings.

- **General**
  - **Network notification** - When enabled, notifies the user when an open network is available.
  - **Keep Wi-Fi on during sleep** - Opens a menu to set whether and when the Wi-Fi radio turns off.
    - **Always On** - The radio stays on when the device enters suspend mode.
    - **Only when plugged in** - The radio stays on while the device is connected to external power.
    - **Never On** - The radio turns off when the device enters suspend mode (default).
  - **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **Regulatory**
  - **Enable 802.11d** - Enabled by default. The device obtains Regulatory information from the AP including country code. Displays the country code acquired from the AP.
  - **Enable 802.11d Strict mode** - Device will connect only if the acquired country matches the country broadcasted by the AP.
  - **Country selection** - Displays the acquired country code if 802.11d is enabled else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Use to select the frequency band. Options: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
  - **Available channels (2.4 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
  - **Available channels (5 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
- **About**
  - **Version** - Displays the current Fusion information.

5.6 Disabling 802.11d Feature

Procedure Steps

1. Touch  .
2. Touch **Wi-Fi**.
3. Slide the switch to the **ON** position.
4. Touch  .
5. Touch **Advanced**.
6. Uncheck **Enable 802.11d** checkbox.
7. On the **Warning!** dialog box, touch **Yes**.
8. Touch **Country Selection**.
9. In the **Country Selection** dialog box, select the country you are in.
10. Touch  .

5.7 Remove a Wi-Fi Network

To remove a remembered or connected network:

Procedure Steps

1. Touch  .
2. Touch  **Wi-Fi**.
3. In the **Wi-Fi networks** list, touch and hold the name of the network.
4. In the menu, touch **Forget network**.
5. Touch  .

6 Administrator Utilities

Motorola Solutions provides 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.

6.1 Required Software

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

6.2 On-device Application Installation

See 9.4 Application Installation, page 9-4 for instruction on installing applications onto the device.

6.3 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 6.7 Manual File Configuration, page 6-18 for more information.

6.4 Enterprise Administrator Application

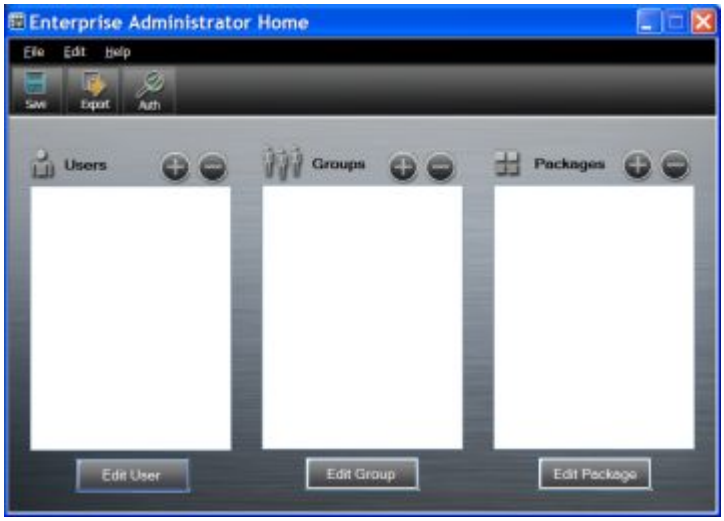
NOTE

.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 6-1 Enterprise Administrator Window



6.4.1 Creating Users

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

Procedure Steps

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

Figure 6-2 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.

6.4.2 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 Steps

1 Click + next to **Packages**.

NOTE

To get a list of all the applications (packages) on the device see 6.7.1 Determining Applications Installed on the Device, page 6-20.

Figure 6-3 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.

6.4.3 Creating Groups

Create groups of users that have access to specific applications.

Procedure Steps

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

Figure 6-4 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**.

6.4.4 Creating Remote Authentication

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

Procedure Steps

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

Figure 6-5 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**.

6.4.5 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*.

6.4.6 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 Steps

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**.
   Step result: The server file is saved in the **<user>_APP_DATA** folder.
5. Copy all the files to the root of the On-device Storage. See 3 USB Communication, page 3-1 for information on copying files to the device.

6.4.7 Importing User List

Procedure Steps

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**.
   Step result: The user information is populated into the **Users** list.

6.4.8 Importing Group List

Procedure Steps

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**.
   Step result: The group and package information is populated into the **Groups** and **Packages** list.

6.4.9 Importing Package List

To import a package list (see Package List File, page 6-20 for instructions for creating a Package List file):

Procedure Steps

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**.
   Step result: The package information is populated into the **Packages** list.

6.4.10 Editing a User

Procedure Steps

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

6.4.11 Deleting a User

Procedure Steps

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

6.4.12 Editing a Group

Procedure Steps

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

2 Click **Edit Group**.

3 Make changes and then click **OK**.

6.4.13 Deleting a Group

Procedure Steps

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

2 Click **-**.

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

6.4.14 Editing a Package

Procedure Steps

1 Select a package in the **Packages** list.

2 Click **Edit Package**.

3 Make changes and then click **OK**.

6.4.15 Deleting a Package

Procedure Steps

1 Select a package in the **Packages** list.

2 Click **-**. The package name is removed from the list.

6.5 MultiUser Administrator

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

6.5.1 Importing a Password

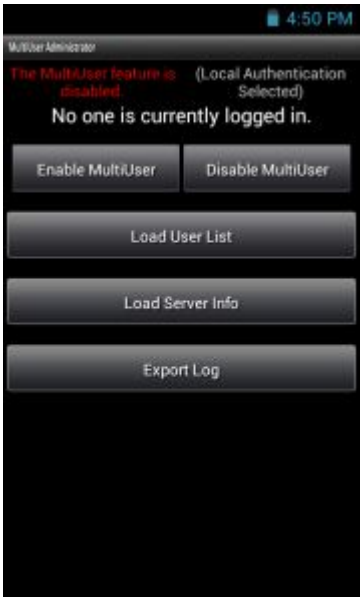
When the MultiUser Administrator is used for the first time, the password file must be imported.

Procedure Steps

1 Touch .

2 Touch .

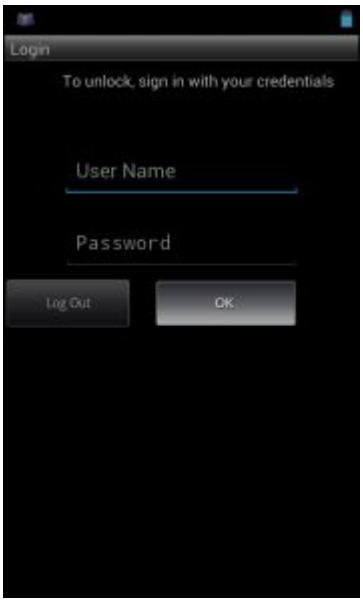
Figure 6-6 MultiUser Administrator Screen



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 6-7 MultiUser Login Screen



5 In the **Login** text box, enter the username.

6 In the **Password** text box, enter the password.

7 Touch **OK**.

6.5.2 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 Steps

1 Touch .

2 Touch .

3 Touch **Disable MultiUser**.

Step result: The Multi-user feature is disabled immediately.

6.5.3 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 Steps

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 Touch .

5 Touch **Enable Remote Authentication**.

Step result: The device accesses the remote server and then Login screen appears.

6.5.4 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 Steps

1 Touch  .

2 Touch  .

3 Touch  .

4 Touch **Disable Remote Authentication**.

Step result: The remote authentication feature is disabled immediately. The device suspends. When resumed, the login screen appears.

6.5.5 Enabling Data Separation

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 Steps

1 Touch  .

2 Touch  .

3 Touch  .

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

6.5.6 Disabling Data Separation

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

Procedure Steps

1 Touch .

2 Touch .

3 Touch .

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

6.5.7 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 Steps

1 Touch .

2 Touch .

3 Touch .

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.

6.5.8 Capturing a Log File

Procedure Steps

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.

6.6 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.

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

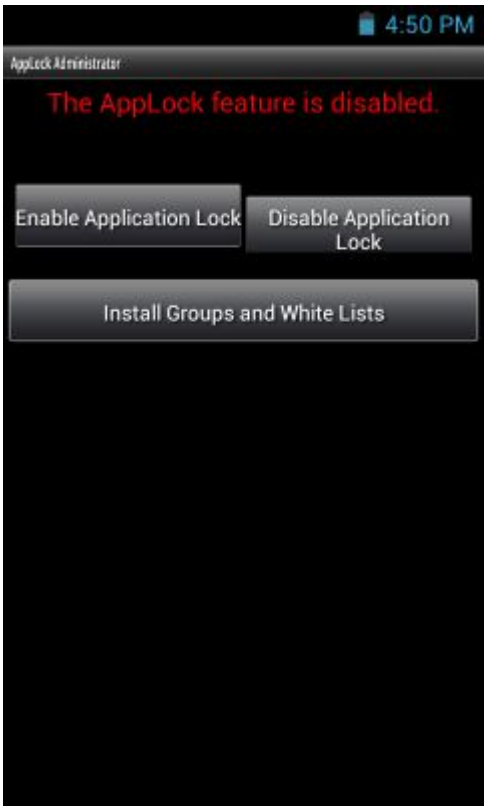
6.6.1 Installing Groups and White Lists

Procedure Steps

1 Touch 

2 Touch 

Figure 6-8 AppLock Administrator Screen



NOTE

When the application launches the current status of the Application Lock feature displays (enabled or disabled).

Log off and then log in again for the feature to take affect.

3 Touch **Install Groups and White Lists** to read the contents of the Groups and White List files from the root of the On—device Storage and push its contents into the AppLock framework.

Result:
Once the Group and White List files are imported and the feature enabled, the next time a user logs in, the device will be configured accordingly.

6.6.2 Enabling Application Lock

Procedure Steps

1 Touch .

2 Touch .

3 Touch **Enable Application Lock**.

6.6.3 Disabling Application Lock

Procedure Steps

1 Touch .

2 Touch .

3 Touch **Disable Application Lock**.

6.7 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 6.5 MultiUser Administrator, page 6-9 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.motorolasolutions.*`

where:

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

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

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

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

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.motorolasolutions.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.motorolasolutions.example1
com.motorolasolutions.example2
com.motorolasolutions.example3
com.motorolasolutions.example4
```

6.7.1 Determining Applications Installed on the Device

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

Procedure Steps

1 Connect the device to the host computer.

NOTE

See 9.2 Development Tools, page 9-2 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 On-device Storage. The file lists all the .apk files installed with their package names.

6.8 Secure Storage

Secure Storage Administrator application allows:

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

6.8.1 Installing a Key

Procedure Steps

1. Touch .
2. Touch .
3. Touch **Install Key**.
4. Touch **Manual**.
5. Touch **OK**.

Figure 6-9 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.

6.8.2 Viewing Key List

Procedure Steps

1 Touch **Key List**.

Figure 6-10 List of Keys

2 Touch **OK**.

6.8.3 Deleting a Key

Procedure Steps

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.

6.8.4 Volumes

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

6.8.4.1 Creating Volume Using EFS File

Procedure Steps

1. Create an efs file. See 6.8.5 Creating an EFS File, page 6-26 for instruction on creating the efs file.
2. Copy the **`keyfile`** and **`efsfile`** files to root of the microSD card. See 3 USB Communication, page 3-1.
3. Touch **Create Volume**.
4. Touch **Import**.
5. Touch **OK**. The message **Successfully Created the Volume** appears briefly.

6.8.4.2 Creating a Volume Manually

Procedure Steps

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 6-11 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.

6.8.4.3 Mounting a Volume

Procedure Steps

1 Touch **Mount Volume**.

2 Touch **sdcard** or **internal**.

3 Touch **OK**.

4 Select a volume.

5 Touch **OK**.

6.8.4.4 Listing Volumes

Procedure Steps

1 Touch **Volume List**.

2 Touch **sdcard** to list volumes on the On-device Storage 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**.

6.8.4.5 Unmounting a Volume

Procedure Steps

1 Touch **Unmount Volume**.

2 Touch **sdcard** to list the mounted volumes on the On—device Storage or **internal** to list the mounted volumes on internal storage.

3 Touch **OK**.

4 Select the volume to un-mount.

5 Touch **OK**.

6.8.4.6 Deleting a Volume

Procedure Steps

1 If the encrypted volume is mounted, unmount it.

2 Touch **Delete Volume**.

3 Touch **sdcard** to list the unmounted volumes on the On-device Storage or **internal** to list the unmounted volumes on internal storage.

4 Select the volume to delete.

5 Touch **OK**.

6.8.4.7 Encrypting an SD Card

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

Procedure Steps

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.

6.8.5 Creating an EFS File

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

Procedure Steps

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`**.

6.8.6 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:
```

6.8.6.1 Creating an Image

Procedure Steps

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.

6.8.6.2 Mounting an Image

Procedure Steps

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.

6.8.6.3 Unmounting an Image

Procedure Steps

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.

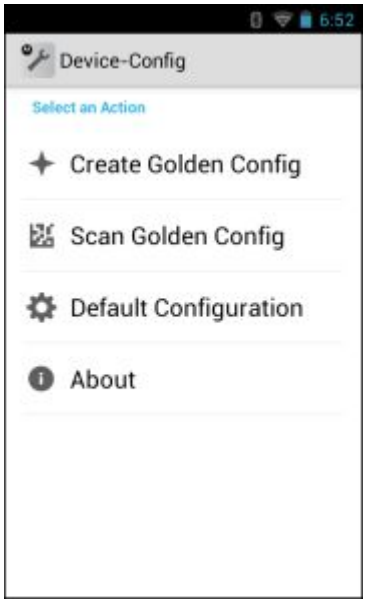
3 Press **Enter**.

7 Device-Config Utility

Use the Device-Config utility to create a master device configuration and then transfer the master settings to other MC40 devices by scanning a QR bar code. The utility supports configuring:

- Device settings
- Bluetooth settings
- DataWedge Profile settings
- Button remapping
- user installed applications.

Figure 7-1 Select Action Window



The utility does not support configuring:

- Location & security
  - Screen unlock
  - Use secure credential
- Wi-Fi settings
- Device administrators
- Credential storage
- Application Development settings
  - USB Debugging
- Date & Time
  - Select time zone

  - Set time.
- Language & keyboard settings.

7.1 Creating a Golden Configuration

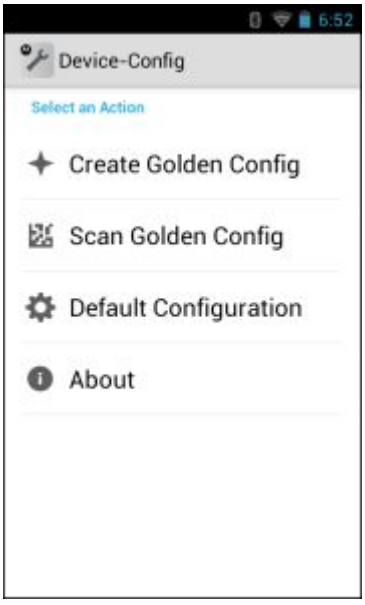
NOTE

If MC40 device settings are to be part of the Golden Configuration, change the settings prior to creating the Golden Configuration.

Procedure Steps

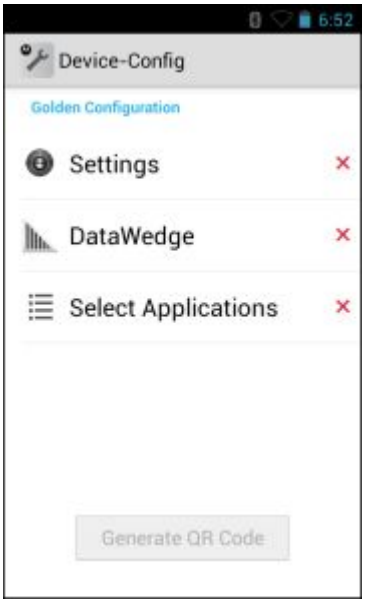
1. Ensure that the Wi-Fi radio is on.
2. Ensure that the Bluetooth radio is on.
3. Touch .
4. Touch .

Figure 7-2 Select an Action Window



5 Touch **Create Golden Config**. If configuration files already exist on the device, dialog boxes appears. Touch **Yes** to delete the configuration file.

Figure 7-3 Golden Configuration Window



6 Touch **Settings**.

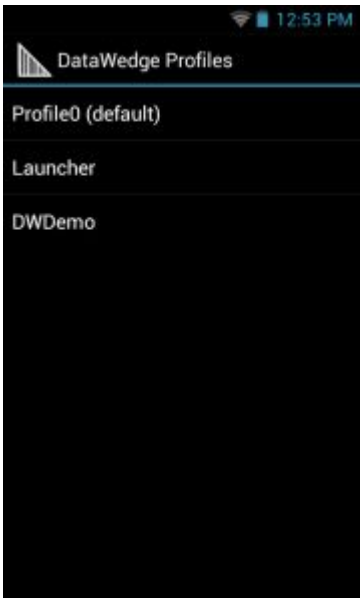
Step result: A green check mark appears indicating that Settings is part of the Golden Configuration.

7 Touch **DataWedge**.

Step result: A **DataWedge** dialog box appears notifying the user to export the DataWedge database file after configuring DataWedge.

8 Touch **OK**.

Figure 7-4 DataWedge Profiles Window



9 Make changes to DataWedge. See 4 DataWedge Configuration, page 4-1 for more information.

10 After changing DataWedge settings, touch ⮌ until the **DataWedge Profiles** window appears.

11 Touch ▭.

12 Touch **Settings**.

13 Touch **Export**.

14 In the **Export to..** dialog box, touch **Export**.

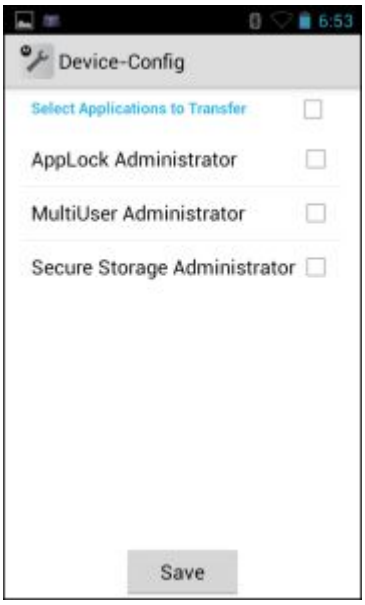
15 Touch ⮌.

16 Touch ⮌.

Step result: The **Golden Configuration** window appears with a green check mark next to **DataWedge**.

17 Touch **Select Applications**.

Figure 7-5 Select APKs to Transfer Window



18 **NOTE**

If there are no user installed application on the MC40, a dialog appears indicating that there are none. Touch **OK**.

Touch the checkbox next to each application or touch the top checkbox to select all applications.

19 Touch **Save**.

20 In the **Select Applications** dialog box, touch **OK**.

Step result: The **Golden Configuration** dialog box appears with a green check mark next to **Select Applications**.

21 Touch **Generate QR Code**.

Figure 7-6 QR Code Generation Screen

22 The Golden Configuration is now ready for transfer to other MC40 devices.

7.2 Transferring a Golden Configuration

Once a golden configuration is created on a master MC40, the data can be transferred to other MC40 devices.

Procedure Steps

1 On both the client devices, ensure that Bluetooth is on.

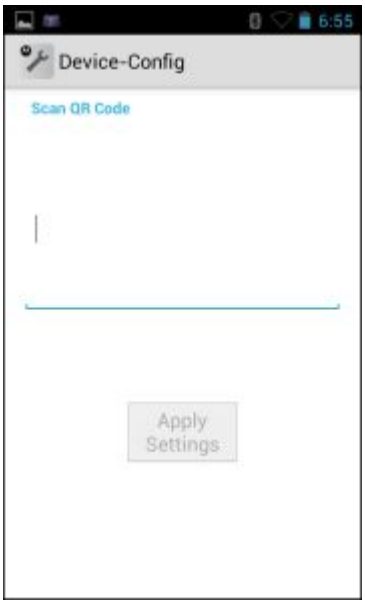
2 Touch OK on both devices. The QRCode window appears on the master MC40.

3 On the client device, touch .

4 Touch .

5 Touch **Scan Golden Config**.

Figure 7-7 Scan QR Code Window



6 Press the Right Scan button.

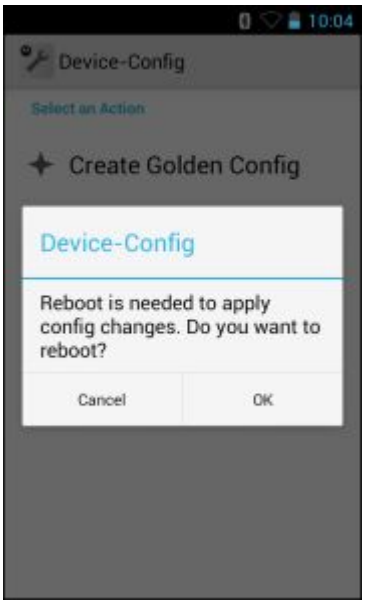
7 Point the top of the MC40 at the display of the master MC40. The LEDs light indicating that the data was read and the text field fills with text.

8 Touch **Apply Settings**.

Step result: The client device connects to the master device and transfers the configuration information. A rotating cirle appears in the top right corner indicating data transfer.

9 In the **Device-Config** dialog box, touch **OK**.

Figure 7-8 Reboot Confirmation Dialog Box



10 The device powers off and then reboots and the new configuration settings are applied.

7.3 Returning to the Default Configuration

To return either the master or client the MC40 to the default configuration:

Procedure Steps

1 Touch .

2 Touch .

3 Touch **Default Configuration**.

4 Touch **OK** to return the device to the default settings.
Step result: The device powers off and then reboots.

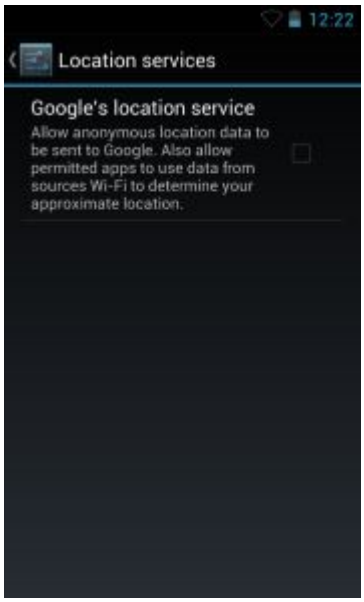
8 Settings

This chapter describes settings available for configuring the device.

8.1 Location Settings

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

Figure 8-1 Location Services Window



Check **Google's location service** checkbox to use information from Wi-Fi networks to determine approximate location.

8.2 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.
  - **Pattern** - Draw a pattern to unlock screen. See 8.2.1.3 Set Screen Unlock Using Pattern, page 8-4 for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See 8.2.1.1 Set Screen Unlock Using PIN, page 8-2 for more information.
  - **Password** - Enter a password to unlock screen. See 8.2.1.2 Set Screen Unlock Using Password, page 8-3 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.

8.2.1 Single User Mode

When locked, a slide, pattern, 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 Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.

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

8.2.1.1 Set Screen Unlock Using PIN

Procedure Steps

1 Touch  .

2 Touch  **Security**.

3 Touch **Screen lock**.

4 Touch **PIN**.

5 Touch in the text field.

6 Enter a PIN (between 4 and 16 characters) then touch **Next**.

7 Re-enter PIN and then touch **Next**.

8 On the **Security** screen, touch **Vibrate on touch** to enable vibration when the user enters PIN.

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

Figure 8-2 PIN Screen

8.2.1.2 Set Screen Unlock Using Password

Procedure Steps

1 Touch .

2 Touch **Security**.

3 Touch **Screen lock**.

4 Touch **Password**.

5 Touch in the text field.

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

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

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

Figure 8-3 Password Screen

8.2.1.3 Set Screen Unlock Using Pattern

Procedure Steps

1 Touch .

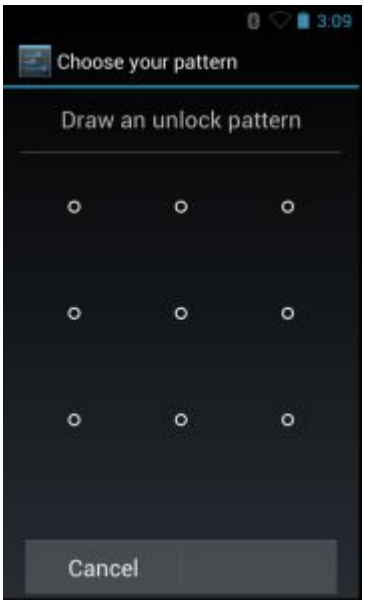
2 Touch **Security**.

3 Touch **Screen lock**.

4 Touch **Pattern**.

5 Draw a pattern connecting at least four dots.

Figure 8-4 Choose Your Pattern Screen



6 Touch **Continue**.

7 Re-draw the pattern.

8 Touch **Confirm**.

9 On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.

10 Touch **Vibrate on touch** to enable vibration when drawing the pattern.

11 Touch ⌂.

The next time the device goes into suspend mode a Pattern is required upon waking.

Figure 8-5 Pattern Screen

8.2.2 Multiple User Mode

For Multi-user Mode configuration, see 6 Administrator Utilities, page 6-1.

8.3 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.

8.4 Button Remapping

The MC40's buttons can be programmed to perform different functions or shortcuts to installed applications.

- Trigger 1- Left Scan/Action button
- Trigger 2 - Volume up button
- Trigger 3 - Right Scan button
- Trigger 4 - PTT button
- Trigger 5 - Volume down button
- Search Key - button below display.
- Headset Key - Button on Headset.

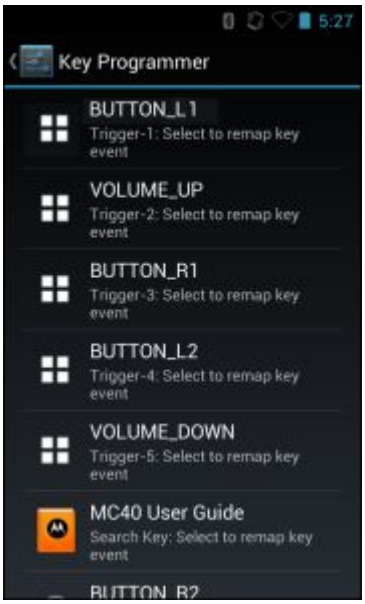
8.4.1 Remapping a Button

Procedure Steps

1 Touch .

2 Touch **Key Programmer**.

Figure 8-6 Key Programmer Screen



3 Select the button to remap.

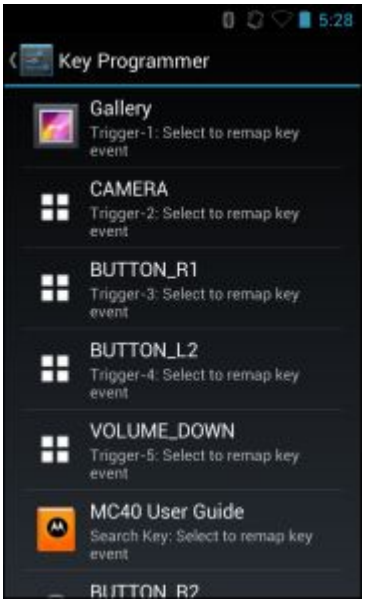
4 Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.

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 8-7 Remapped Button



6 Touch .

8.4.2 Setting the Headset Key

NOTE

Headset Key is only available on Voice Telephony Ready configurations.

When using a headset with the MC40, the headset button can be mapped to function as a PTT button or as a audio control button. By default the Headset key is mapped to the PTT button (R2_Button). When PTT Express is enabled, a single press of the headset button acts as a Group Response key. A double press acts as a Private Response key. If an application is designed to use the headset button to control audio playback, the Headset button is set to **Headset Hook**.

Procedure Steps

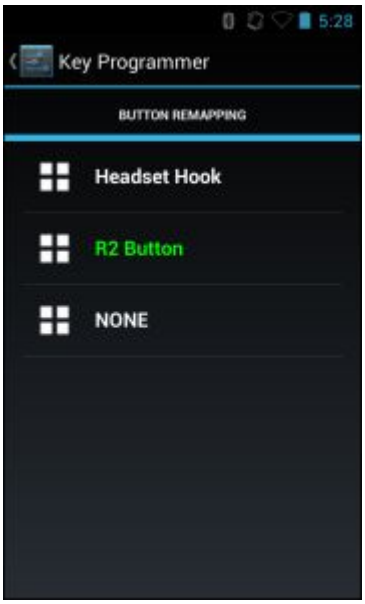
1 Touch .

2 Touch **Key Programmer**.

3 Select the Headset button.

4 In the **BUTTON REMAPPING** screen, select **Headset Hook**, **R2 Button** or **NONE**.

Figure 8-8 Headset Button Remapping



5 Touch .

8.4.3 Exporting a Configuration File

The Button Remapping configuration can be exported to an xml file and imported into other MC40 devices.

Procedure Steps

1 Touch  .

2 Touch **Key Programmer**.

3 Touch .

4 Touch **Export**.

Step result: 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 3 USB Communication, page 3-1 for more information.

8.4.4 Importing a Configuration File

Procedure Steps

1 Copy the configuration file (**`key-config.xml`**) from a host computer to the root of the On-device Storage. See 3 USB Communication, page 3-1 for more information.

2 On the MC40, use **File Browser** to move the file from the root of the On-device Storage to the folder: **`/enterprise/usr`**.

3 Touch  .

4 Touch **Key Programmer**.

5 Touch .

6 Touch **Import**.

8.4.5 Creating a Remap File

The administrator can create an xml configuration file and import it into any MC40 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>VOLUME_UPREMAP_CODE>VOLUME_UP>
     <EXTRA_SHORTCUT>MPA3_TRIGGER_2</EXTRA_SHORTCUT>
     <EXTRA_TITLE>Music</EXTRA_TITLE>
     <EXTRA_PACKAGE_NAME>com.android.music</EXTRA_PACKAGE_NAME>
</trigger_2>
<trigger_3 mode="Remap Button">
     <REMAP_CODE>BUTTON_R1</REMAP_CODE>
     <EXTRA_SHORTCUT>MPA3_TRIGGER_3</EXTRA_SHORTCUT>
     <EXTRA_TITLE/>
     <EXTRA_PACKAGE_NAME/>
</trigger_3>
<trigger_4 mode="Remap Button">
     <REMAP_CODE>BUTTON_L2</REMAP_CODE>
     <EXTRA_SHORTCUT>MPA3_TRIGGER_4</EXTRA_SHORTCUT>
     <EXTRA_TITLE/>
     <EXTRA_PACKAGE_NAME/>
</trigger_4>
<trigger_5 mode="Shortcut">
     <REMAP_CODE>VOLUME_DOWN</REMAP_CODE>
     <EXTRA_SHORTCUT>MPA3_TRIGGER_5</EXTRA_SHORTCUT>
     <EXTRA_TITLE>File Browser<EXTRA_TITLE/>
     <EXTRA_PACKAGE_NAME>com.motorolasolutions.software.filexp
     </EXTRA_PACKAGE_NAME>
</trigger_5>
<search_key mode="Remap Button">
     <REMAP_CODE>SEARCH</REMAP_CODE>
     <EXTRA_SHORTCUT>SEARCH_KEY</EXTRA_SHORTCUT>
     <EXTRA_TITLE/>
     </EXTRA_PACKAGE_NAME>
</search_key>
<headset mode="Remap Button">
     <REMAP_CODE>BUTTON_R2</REMAP_CODE>
```

```
    </headset>
</Button_Remap>
```

Replace the options for each trigger. See 12 Keypad Remap Strings, page 12-1 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.

8.5 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.

- **General sync settings**
  - **Background data** - Check to permit applications to synchronize data in the background. Unchecking this setting can save battery power.
  - **Auto-sync** - Check to permit applications to synchronize data on their own schedule. If unchecked, touch ☰ > **Sync now** to synchronize data for that account. Synchronizing data automatically is disabled if **Background data** is unchecked. In that case, the Auto-sync checkbox is dimmed.
- **Manage accounts** - Lists accounts added to the device. Touch an account to open its account screen.

8.6 Language Usage

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

8.6.1 Changing the Language Setting

Procedure Steps

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

Result:
The operating system text changes to the selected language.

8.6.2 Adding Words to the Dictionary

Procedure Steps

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.

8.7 Keyboard Settings

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

- Android Keyboard
- Chinese keyboard

8.8 About Device

Use **About device** settings to view information about the Mc40. 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 MC40 has been running since being turned on.
- **Battery information** - Displays information about the battery.
- **Hardware config** - Lists part number for various hardware on the MC40.
- **Legal information** - Opens a screen to view legal information about the software included on the MC40.
- **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.

8.9 PTT Express Configuration

The system administrator can manually configure PTT Express by creating an xml file and loading it onto the MC40. Table 7-1 list all the key options for the PTT Express application. The filename of the xml file must be: **`te_settings.xml`**. The xml file must be located in the folder: = **`/enterprise/device/settings/te`**.

Table 8-1 PPT Express Configuration File Keys

Key	Range	Default	Description
te_enable	True or False	False	Enable or disable the PTT Express service.
te_channel	1 through 32	1	Sets the default Talk Group Channel.
te_TalkTime-Out	10,000 .through 90,000	60,000	In a group call, the amount of time the user is allowed to hold the floor (talk without interruption). Decimal value in milliseconds. Disable = 0.
te_pvtTalk-TimeOut	10,000 .through 90,000	60,000	In a private call, the amount of time the user is allowed to hold the floor (talk without interruption). Decimal value in milliseconds. Disable = 0.
te_END_SES-SION	1,000 through 10,000	10,000	The amount of time that has to elapse after which a Private Response cannot be made to the last known talker in the session. Decimal value in milliseconds.
te_PvtHang-TimerDuration	1,000 through 10,000	10,000	The amount of time that has to elapse after which the Private Response will terminate. Decimal value in milliseconds.
te_PvtLocal-Port		4,080	IP Port to be used for Private Response communications. Decimal value.

Table 8-1 PPT Express Configuration File Keys (cont'd.)

Key	Range	Default	Description
te_ipgroup		239.192.2.2	Multicast address to be used for Group Broadcast communications.
te_IP_PORT_BASE		5,000	IP Port number of the multicast address being used for Group Broadcast communications. Decimal value.
ignoreKeysIn-LockMode	True or False	False	Ignore hard keys in locked screen mode.
groupCallKey	L1, L2	L2	The Group Call Key intent. L2 = PTT Key L1 = Left Trigger
privateCal-lKey	L1, L2	L1	The Private Call Key intent. L2 = PTT Key L1 = Left Trigger
pttHead-SetKey	R2	R2	The PTT Headset Key Intent.
log_level	None, Error, Warning, Info, Debug	None	Log Level for logs generated at /sdcard/te

The administrator can edit an xml configuration file and import it into any MC40 device. Use any text editor to create or edit an xml file. Use the sample below to create the xml file.

```
<?xml version="1.0" encoding="UTF-8"?>



<TeSettingList>


     <setting>
          <te_enable>true</te_enable>
          <explanation>Enable or disable the TE service.</explanation>
     </setting>
     <setting>
          <disablePrivateCall>false</disablePrivateCall>
          <explanation>explanation>Disable or enable private call.  Default
is false.</explanation>
     </setting>
     <setting>
          <keyConfiguration>2</keyConfiguration>
          <explanation>Number of hard keys.  The default is 2.  If it is 1,
use the GC key.  If it is 0, use the two soft keys.</explanation>
```

```
     </setting>
     <setting>
          <oneKeyTimerDelay>600</oneKeyTimerDelay>
          <explanation>One key timer delay.  The range is 400 and 1000 ms.
The default is 600 ms.</explanation>
     </setting>
     <setting>
          <te_channel>1</te_channel>
          <explanation>Talk group channel.</explanation>
     </setting>
     <setting>
          <te_TalkTimeOut>60000</te_TalkTimeOut>
          <explanation>In a group call, the amount of time the user is
allowed to hold the floor (talk without interruption).  Decimal value in
milliseconds.  disable = 0.</explanation>
     </setting>
     <setting>
          <te_pvtTalkTimeOut>60000</te_pvtTalkTimeOut>
          <explanation>In a private call, the amount of time the user is
allowed to hold the floor in the private call (talk without interruption).
Decimal value in milliseconds.  disable = 0.</explanation>
     </setting>
     <setting>
          <te_END_SESSION>1000</te_END_SESSION>
          <explanation>The amount of time that has to elapse after which a
Private Response cannot be made to the last known talker in the session.
Decimal value in milliseconds.</explanation>
     </setting>
     <setting>
          <te_PvtHangTimerDuration>10000</te_PvtHangTimerDuration>
          <explanation>The amount of time that has to elapse after
which the Private Response will terminate.  Decimal value in
milliseconds.</explanation>
     </setting>
     <setting>
          <te_PvtLocalPort>4080</te_PvtLocalPort>
          <explanation>SIP IP Port to be used for Private Response
communications.  Decimal value.</explanation>
     </setting>
     <setting>
```

```
          <te_ipgroup>239.192.2.2</te_ipgroup>
          <explanation>Multicast address to be used for Group Broadcast
communications.</explanation>
     </setting>
     <setting>
          <te__IP_PORT_BASE>5000__IP_PORT_BASE>
          <explanation>IP Port number of the multicast address being used for
Group Broadcast communications.  Decimal value.</explanation>
     </setting>
     <setting>
          <log_level>None</log_level>
          <explanation>Log level:  None, Error, Warning, Info, Debug.  The
default is None.</explanation>
     </setting>
     <setting>
          <groupCallKey>L2</groupCallKey>
          <explanation>The button for group call.  The default is
L2.</explanation>
     </setting>
     <setting>
          <privateCallKey>L1</privateCallKey>
          <explanation>The button for private call.  The default is
L1.</explanation>
     </setting>
     <setting>
          <pttHeadsetKey>R2</pttHeadsetKey>
          <explanation>The headset button for group call.  The default is
R2.</explanation>
     </setting>
     <setting>
          <ignoreKeysInLockMode>false</ignoreKeysInLockMode>
          <explanation>Ignore keys in lock mode.  The default is
false.</explanation>
     </setting>
     <setting>
          <gcJitterSize>3</gcJitterSize>
          <explanation>One group call packet holds 200 ms data.  The default
jitter buffer size is 3 which means the maximum data the jitter holds is 600
ms.</explanation>
```

```
    </setting>
    <setting>
        <pcJitterSize>3</pcJitterSize>
        <explanation>One private call packet holds 100 ms data.  The
default jitter buffer size is 3 which means the maximum data the jitter holds
is 300 ms.</explanation>
    </setting>
</TeSettingList>
```

8.9.1 Importing a PTT Express Configuration File

Procedure Steps

1. Copy the configuration file **`te_settings.xml`** from a host computer to the root of the On-device Storage. See 3 Chapter 3, USB Communication, page 3-1.

2. On the MC40, use File Browser to move the **`te_settings.xml`** file from the root of the On-device Storage to the folder: **`/enterprise/device/settings/te`**.

   NOTE

   The configuration file can also be loaded on the MC40 using ADB. See 9.4.2 Using Android Debug Bridge on page 8-6, page 9-5.

9 Application Deployment

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

9.1 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).

9.1.1 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.

9.1.2 Installing a Secure Certificate

Procedure Steps

1. Copy the certificate from the host computer to the root of the On-device Storage. See 3 USB Communication, page 3-1 for information about connecting the device to a host computer and copying files.
2. Touch  .
3. Touch  **Security**.
4. Touch **Install from On-device Storage**.
5. Touch the filename of the certificate to install. Only the names of certificates not already installed are displayed.
6. If prompted, enter the certificate's password and touch **OK**.
7. 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**.

   The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the On-device Storage.

9.1.3 Configuring Credential Storage Settings

Procedure Steps

1. Touch  .
2. Touch  **Security**.
   - **Trusted credentials** - Touch to display the trusted system and user credentials.
   - **Install from On-device Storage** - Touch to install a secure certificate from the On-device Storage.
   - **Clear credentials** - Deletes all secure certificates and related credentials.

9.2 Development Tools

Get tools 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.

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

Touch  > { } **Developer options**. Slide the switch to the **ON** position to enable developer options. The following developer options are available:

- **Desktop backup password**
- **Stay awake**
- **Protect SD card**
- **Debugging**
  - **USB debugging**
  - **Select debug app**
  - **Wake for debugger**
- **Input**
  - **Show touches**
  - **Pointer location**
- **Drawing**
  - **Show layout bounds**
  - **Show GPU view updates**
  - **Show surface updates**
  - **Window animation scale**
  - **Transition animation scale**

  - **Animator duration scale**
  - **Disable HW overlays**
  - **Force GPU rendering**
- **Monitoring**
  - **Strict mode enabled**
  - **Show CPU usage**
  - **Profile GPU rendering**
  - **Enable traces**
- **Apps**
  - **Don’t keep activities**
  - **Background process limit**
  - **Show all ANRs**

9.3 ADB USB Setup

To use the ADB, the USB driver has to be modified. 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 Motorola Solutions Support Central web site at http://supportcentral.motorolasolutions.com. 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.

9.4 Application Installation

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

- USB connection, see 9.4.1 Installing Applications Using the USB Connection, page 9-4.
- Android Debug Bridge, see 9.4.2 Installing Applications Using the Android Debug Bridge, page 9-5.
- Mobility Services Platform (MSP) for Android.

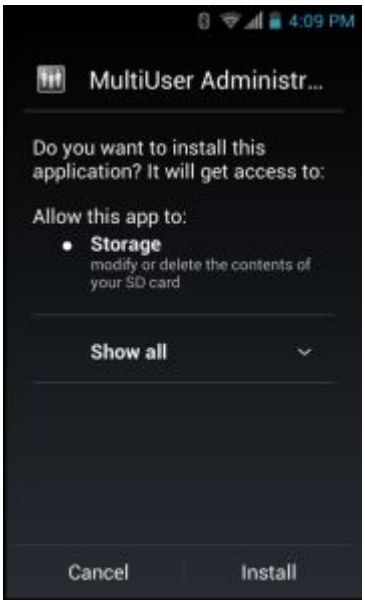
9.4.1 Installing Applications Using the USB Connection

When connecting the device to a host computer and mounting its On-device Storage, follow the host computer’s instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure Steps

1. Connect the device to a host computer using USB. See 3 USB Communication, page 3-1.
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 3 USB Communication, page 3-1
4. On the device, touch .
5. Touch to view files on the On-device 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 9-1 Accept Installation Screen



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

9.4.2 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 On-device Storage , 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 9.3 ADB USB Setup, page 9-4.

Procedure Steps

1. Connect the device to a host computer using USB. See 3 USB Communication, page 3-1.
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 3 USB Communication, page 3-1.

9.4.3 Mobility Services Platform

The MSP Client Software is a set of software components that come pre-installed on the device. The MSP Client software consists of the following components:

- The **Rapid Deployment** application provides support for MSP Staging functionality, provides support for the MSP Legacy Staging process, and provides support for backward-compatible legacy MSP 2.x Legacy Staging functionality.
- The **MSP Agent** application provides MSP Provisioning functionality and Control functionality when used with MSP Control Edition.

Refer to the *Mobility Services Platform User's Guide*, p/n 72E-100158-xx, for instructions for using the Rapid Deployment and MSP Agent clients.

9.4.4 Uninstalling an Application

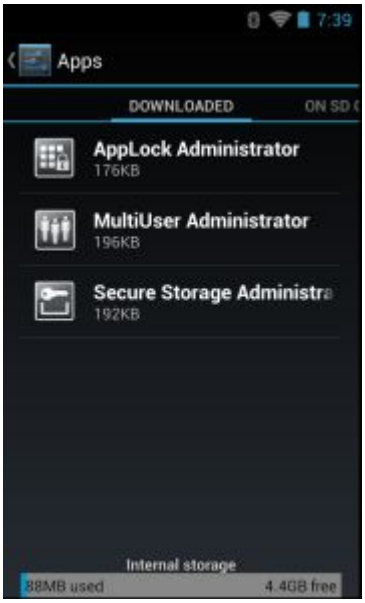
Procedure Steps

1 Touch .

2 Touch **Apps**.

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

Figure 9-2 Downloaded Screen



4 Touch the application to uninstall.

5 Touch **Uninstall**.

6 Touch **OK** to confirm.

9.5 Updating the System

System Update packages can contain either partial or complete updates for the operating system. Motorola Solutions distributes the System Update packages on the Support Central web site.

Before performing a system update, copy all applications and the key remap configuration file that you want to persist after the update into the **`/enterprise/usr/persist`** folder. After the update is complete, the MC40 installs the applications and copies the key remap configuration file back to the appropriate locations.

Procedure Steps

1. Download the system update package:
   a. Go to the Motorola Support Central web site, http://supportcentral.motorolasolutions.com.
   b. Download the appropriate System Update package to a host computer.
2. Locate the System Update package file on the host computer and un-compress the file into a separate directory.
3. Copy the **`40N0JxxRUxxxxxxxx.zip`** file to the root directory of the On-device Storage. See 3 USB Communication, page 3-1 for more information.
4. Press and hold the Power button until the menu appears.
5. Touch **Reset**.
6. Press and hold the Left Scan button.
7. When the Recovery Mode screen appears, release the button.

Figure 9-3 Recovery Mode Screen

8 Touch ⌂.

Figure 9-4 System Recovery Screen

9 Press the Volume Up and Volume Down buttons to navigate to the **apply update from /sdcard** option.

10 Press the PTT button.

11 Press the Volume Up and Volume Down buttons to navigate to the **`40N0JxxRUxxxxxxx.zip`** file.

12 Press the PTT button. The System Update installs and then the MC40 resets.

9.6 Upgrading the Operating System from GingerBread to JellyBean

The MC40 GingerBread (AOSP V2.3) operating system can be upgraded to JellyBean (AOSP V4.1.1) operating system.

Customers who purchased a Service Agreement option for the MC40 GingerBread version, are entitled to a one-time, operating system upgrade via the Motorola Solutions Global Customer Support web site: http://supportcentral.motorolasolutions.com. Customers must enter the serial number for each device to be upgraded. Motorola will then provide a secure web site link for the downloading the software. Customers can then install the upgrade using their own Mobile Device Management (MDM) client and or service center.

Customers who did not purchase a Service Agreement and want to upgrade to Jelly Bean, an Operating System Upgrade must be purchased separately. The software will be delivered after the customer order is placed. The link will be provided to customers by email. Customer's email address must be entered at the time the order is placed. Serial numbers for the MC40's must also be entered. Customers will install the upgrade using their own MDM client and or service center.

Refer to the MDM Client documentation for information on upgrade the MC40 using an MDM. The upgrade can be performed on an individual device using the procedure below.

NOTE

Only MC40 with Rev. B operating system (Build number: 02-271301-G-1600-0018-x0-M1-041913) is supported for upgrade to MC40 Jelly Bean. If the MC40 has an earlier operating system, first upgrade to Rev B, before starting this procedure.

The MC40 with JellyBean (V4.1.1) supports 802.11d and is enabled by default. This prevents connection with 802.11d disabled infrastructure. For deployments having 802.11d disabled infrastructure, 802.11d should be disabled in the MC40. See 5.6 Disabling 802.11d Feature, page 5-8 for more information.

CAUTION

Backup all data and applications prior to performing the upgrade. See 9.6.1 Copying Applications and Configuration Files, page 9-12 for information on copying applications and configuration files to the Enterprise folder before performing the upgrade. Data on the Internal Storage and in the /Enterprise folder will persist after the upgrade.

Ensure that power is applied to the MC40 during the system update procedure.

Procedure Steps

1 Download the System Upgrade package:

a. Go to the Motorola Support Central web site, http://supportcentral.motorolasolutions.com.

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

If...	Then...
MC40 Non-voice	40N0G2JNRU01060905.zip
MC40 Voice	40N0G2JVRU01060905.zip

2 Copy the zip files to the root directory of the On-device Storage. See 3 USB Communication, page 3-1 for more information.

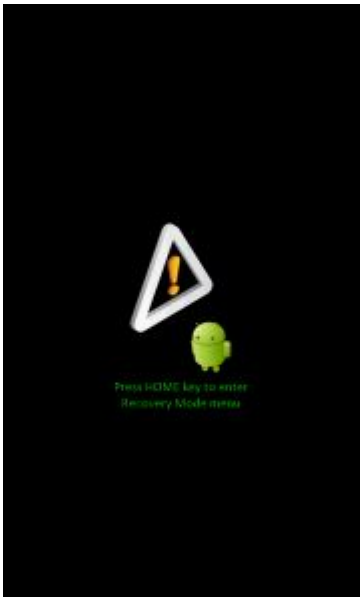
3 Press and hold the Power button until the **Device options** menu appears.

4 Touch **Reset**.

5 Press and hold the Left Scan button.

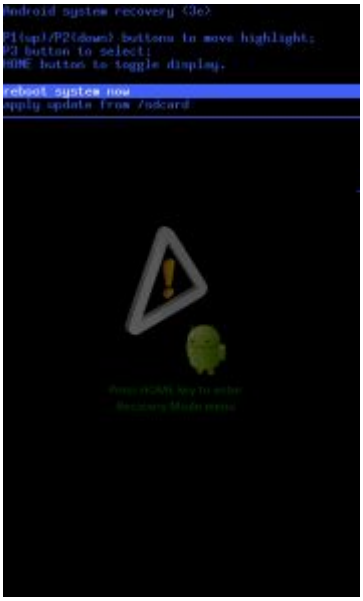
6 When the Recovery Mode screen appears, release the Left Scan button.

Figure 9-5 Recovery Mode Screen



7 Touch ⌂.

Figure 9-6 System Recovery Screen



8 Press the Volume Up and Volume Down buttons to navigate to the **apply update from /sdcard** option.

9 Press the PTT button.

10 Press the Volume Up and Volume Down buttons to navigate to the **40N0G2JxRU01060905.zip** file.

11 Press the PTT button.

Step result: The System Update installs and then the MC40 reboots into the new operating system.

9.6.1 Copying Applications and Configuration Files

Before performing an upgrade from GingerBread to JellyBean, copy all applications and key remap configuration file that you want to persist after the upgrade. After the upgrade is complete, the MC40 installs the applications and copies the key remap configuration file back to the appropriate locations.

Procedure Steps

1 Touch  .

2 Touch  .

3 Navigate to the **/enterprise/user** folder.

4 Touch  .

5 Touch **New Folder**.

6 In the **Create a New Folder** dialog box, enter **persist**.

7 Touch **OK**.

8 Locate application .APK files and configuration .xml files and copy into the **/enterprise/user/persist** folder.

9 Touch  .

9.7 Storage

The device contains four types of file storage:

- Random Access Memory (RAM)
- On-device Storage
- Internal storage
- Enterprise folder.

9.7.1 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 9-7 Running Screen

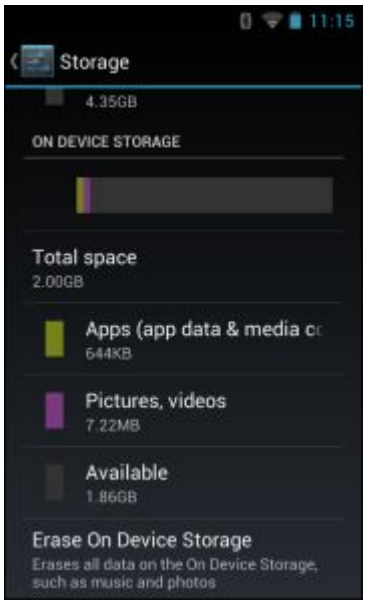
The bar at the bottom of the screen displays the amount of used and free RAM.

9.7.2 On-Device Storage

The MC40 has internal On-device Storage. The On-device Storage content can be viewed and files copied to and from when the MC40 is connected to a host computer. Some applications are designed to be stored on the On-device Storage rather than in internal memory.

To view the used and available space on the On-device Storage, touch > **Storage**.

Figure 9-8 On-Device Storage Screen



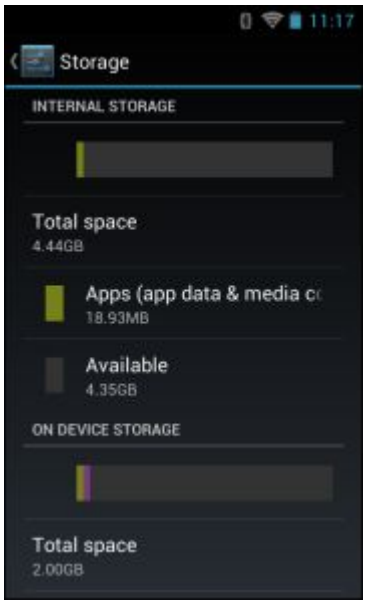
- **On Device Storage**
  - **Total space** - Displays the total amount of space on On-device Storage.
    - **Apps** - Displays the available space used for applications and media content on On-device Storage.
    - **Pictures, videos** - Displays the available space used for pictures and videos on On-device Storage.
    - **Available** - Displays the available space on On-device Storage.
- **Erase On Device Storage** - Permanently erases everything on the installed On-device Storage.

9.7.3 Internal Storage

The MC40 has internal On-device Storage. The On-device Storage content can be viewed and files copied to and from when the MC40 is connected to a host computer. Some applications are designed to be stored on the On-device Storage rather than in internal memory.

To view the used and available space on the On-device Storage, touch > **Storage**.

Figure 9-9 Internal Storage Screen



- **Internal Storage**
  - **Total space** - Displays the total amount of space on internal storage.
    - **Apps** - Displays the available space used for applications and media content on internal storage.
    - **Pictures, videos** - Displays the available space used for pictures and videos on internal storage.
    - **Available** - Displays the available space on internal storage.
- **Erase On Device Storage** - Permanently erases everything on the installed On-device Storage.

9.7.4 Enterprise Folder

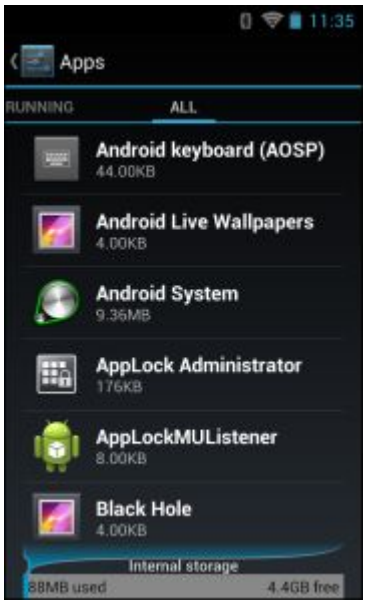
The Enterprise folder (within internal storage) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 MB (formatted). Applications can persist data after an Enterprise Reset by saving data to the enterprise/user folder.

9.8 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.

From the Home screen touch > **Manage apps**.

Figure 9-10 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 On-device Storage. A check mark indicates that the application is installed on On-device Storage. Unchecked items are installed in internal storage and can be moved to On-device Storage.
- 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, touch > **Sort by size** to switch the order of the list.

9.8.1 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 9.4.4 Uninstalling an Application, page 9-7 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 Steps

1 Touch  > **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.

9.8.2 Stopping an Application

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

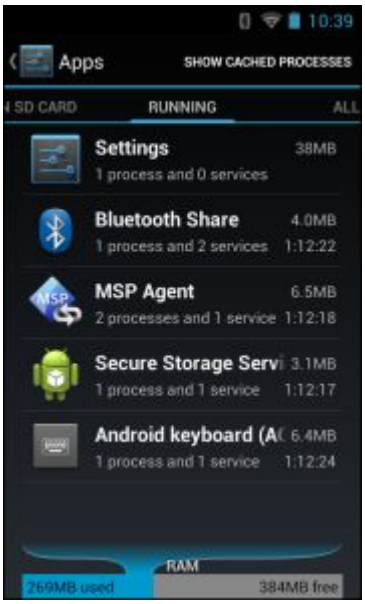
Procedure Steps

1 Touch > **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 9-11 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**.

9.8.3 Changing Application Location

Some applications are designed to be stored on On-device Storage, 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 Steps

1. Touch > **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 On-device Storage. 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 On-device Storagecard are checked.

   The graph at the bottom shows the amount of memory used and free of On-device Storage: 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 On-device Storage** to move the bulk of the application from the device's internal storage to the On-device Storage.
5. Touch **Move to phone** to move the application back to the device's internal storage.

9.8.4 Managing Downloads

Files and applications downloaded in the Browser or Email are stored on On—device Storage in the Download directory. Use the **Downloads** application to view, open, or delete downloaded items.

Procedure Steps

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.

10 Maintenance and Troubleshooting

This chapter includes instructions on cleaning and storing the device, and provides troubleshooting solutions for potential problems during operation.

10.1 Maintaining the MC40

For trouble-free service, observe the following tips when using the MC40:

- Do not scratch the screen of the MC40. When working with the MC40, use only a finger. Never use an actual pen or pencil or other sharp object on the surface of the MC40 screen.
- The touch-sensitive screen of the MC40 is glass. Do not to drop the MC40 or subject it to strong impact.
- Protect the MC40 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 MC40 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the MC40. If the surface of the MC40 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.

10.2 Battery Safety Guidelines

- 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 Motorola Solutions Global Customer Support Center.
- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- 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.
- 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 Motorola Solutions Global Customer Support Center to arrange for inspection.

10.3 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 Motorola 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, hydrogen peroxide or mild dish soap.

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.

10.3.1 Cleaning the MC40

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.

Exit and Camera Window

Wipe the camera window periodically with a lens tissue or other material suitable for cleaning optical material such as eyeglasses.

10.3.1.1 Connector Cleaning

To clean the connectors:

Procedure Steps

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.

   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.

10.3.2 Cleaning Cradle Connectors

To clean the connectors on a cradle:

Procedure Steps

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.

10.4 Troubleshooting

The following tables provides typical problems that might arise and the solution for correcting the problem.

10.4.1 Troubleshooting the MC40

Table 10-1 Troubleshooting the MC40

Problem	Cause	Solution
When the user presses the Power button, the MC40 does not turn on.	Battery is completely discharged.	Re-charge or replace the battery.
	Battery not installed properly.	Install the battery properly. See 1.2.1 Installing the Battery, page 1-1.
	Power button not held down long enough.	Press the Power button until the Right LED flashes once.
	MC40 not responding.	Perform a hard reset. See 1.3 Resetting the Device, page 1-5.
When the user presses the Power button the MC40 does not turn on but the Decode LED blinks amber.	Battery charge level is very low.	Re-charge or replace the battery.
Battery did not charge.	Battery failed.	Replace battery. If the MC40 still does not operate, perform a hardware reset. See 1.3 Resetting the Device, page 1-5.
	MC40 was removed from power while battery was charging.	Insert MC40 in cradle. The 2680 mAh battery fully charges in less than four hours.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
During data communication, no data transmitted, or transmitted data was incomplete.	MC40 disconnected from host computer during communication.	Reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
No sound.	Volume setting is low or turned off.	Adjust the volume.
MC40 turns off.	MC40 is inactive.	The display turns off after a period of inactivity. Set this period to 15 seconds, 30 seconds, 1, 2, 10, or 30 minutes.
	Battery is depleted.	Recharge or replace the battery.

Table 10-1 Troubleshooting the MC40 (cont'd.)

Problem	Cause	Solution
A message appears stating not enough storage memory.	Too many applications installed on the MC40.	Remove user-installed applications on the MC40 to recover memory. Touch > **Apps** > **Downloaded**. Select the unused programs and touch **Uninstall**.
The MC40 does not decode when reading bar code.	DataWedge is not enabled.	Ensure that DataWedge is enabled and configured properly. Refer to the *MC40 Integrator Guide* for more information.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between the MC40 and bar code is incorrect.	Place the MC40 within proper scanning range.
	MC40 is not programmed for the bar code type.	Program the MC40 to accept the type of bar code being scanned. Refer to the *MC40 Integrator Guide* for DataWedge configuration.
	MC40 is not programmed to generate a beep.	If the MC40 does not beep on a good decode, set the application to generate a beep on good decode.
MC40 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 (30 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.
MC40 does not read magnetic stripe card.	Magnetic stripe on the card is facing the wrong way.	Ensure that magnetic stripe card is oriented correctly. Magnetic stripe on the card should be facing the display.
Cannot connect to WLAN.	Access Point (AP) does not broadcast country code.	Disable 802.11d feature. Touch > **Wi-Fi** > > **Advanced**. Deselect the **Enable 802.11d** checkbox.
Wired headset is not working as headset hook or not able to initiate a PTT call even through wired headset.	Wired headset not connected properly.	Ensure that the wired headset is connected properly.

10.4.2 Single-Slot Charge Cradle Troubleshooting

Table 10-2 Troubleshooting the Single-slot Charge Cradle

Problem	Cause	Solution
MC40 battery is not charging.	MC40 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure MC40 is seated correctly. Confirm the battery is charging. The 2680 mAh battery charges in approximately four hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The MC40 is not fully seated in the cradle.	Remove and re-insert the MC40 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).

10.4.3 Five-Slot Charge Only Cradle CRDUNIV-40–5000R Troubleshooting

Table 10-3 Troubleshooting the Five-Slot Charge Only Cradle

Problem	Cause	Solution
Battery is not charging.	MC40 removed from the cradle too soon.	Replace the MC40 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 MC40 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).
Spare batteries are not charging in Four Slot Battery Charger.	Missing Four Slot Battery Charger power supply.	The Four Slot Battery Charger requires a separate power supply. Obtain the correct power supply and connect to the charger.

10.4.4 Four-Slot Battery Charger SACMC40XX-4000R Troubleshooting

Table 10-4 Troubleshooting the Four-slot Battery Charger

Problem	Cause	Solution
Battery not charging.	Battery was removed from the charger or charger was unplugged from AC power too soon.	Re-insert the battery in the charger or re-connect the charger's power supply. The 2680 mAh battery charges in approximately four hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Battery contacts not connected to charger.	Verify that the battery is seated in the battery well correctly with the contacts facing down.

11 Technical Specifications

The following sections provide technical specification for the device.

11.1 MC40 Technical Specifications

The following table summarizes the MC40's intended operating environment and technical hardware specifications.

Table 11-1 MC40 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions	Height: 143.9 mm (5.66 in.) Width: 72.8 mm (2.87 in.) Non-MSR: Depth: 20.1 mm (0.79 in.) MSR: Depth: 31.8 mm (1.25 in.)
Weight	Non-MSR: 257.7 g (9.09 oz.) MSR: 266.1 g (9.38 oz.)
Display	4.3 in. capacitive; 480 x 800; 300 nit
Touch Panel	Capacitive dual-touch
Backlight	LED backlight
Battery	Rechargeable Lithium Ion 3.7V, 2680 mAh Smart battery.
Backup Battery	NiMH battery (rechargeable) 15 mAh 3.6 V (not user accessible).
Connectivity	One USB 2.0 OTG connector.
Notification	LED, audio and vibration.
Keypad Options	On-screen keyboard.
Audio	Speakers, microphone and headset connector (mono, 2.5 mm jack with microphone). Stereo audio through Bluetooth stereo headsets.
Communications	All models: Push-to-Talk. PTT Express Client pre-loaded. VoIP Telephony Ready models: Optimized for VoIP telephony. VoIP client not included.
Performance Characteristics	
CPU	Texas Instruments OMAP 4430 @ 800 MHz, dual-core.
Operating System	Android-based ASOP 4.1.1.
Memory	1 GB RAM, 8 GB Flash.
Output Power (USB)	Docking Connector: 5 VDC @ 500 mA max.
User Environment	

Table 11-1 MC40 Technical Specifications (cont'd.)

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% RH non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) drops to plywood per MIL-STD 810G specifications. Multiple 0.9 m (3 ft.) drops to tile.
Electrostatic Discharge (ESD)	+/-15kVdc air discharge, +/-8kVdc direct discharge, +/-2kVdc indirect discharge
Sealing	IP54
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 Mbps 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:** Legacy, WPA and WPA2 **Encryption:** WEP (40 and 128 bit), TKIP and AES **Authentication:** TLS, TTLS (MSCHAP), TTLS (MSCHAPV2), TTLS (PAP), PEAP (MSCHAPV2), PEAP (GTC), FAST (MSCHAPV2), FAST (GTC), LEAP. CCXv4 certified.
Spreading Technique	Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM)
Wireless PAN Data and Voice Communications	
Bluetooth	Class II, v 2.1 with EDR; integrated antenna.
Data Capture	
Imager	Captures 1D and 2D bar codes.
Rear-facing Camera	For bar code scanning and image capture: 8 MP auto-focus camera with aiming; captures 1D and 2D bar codes, photographs, video, signatures and documents.
Magnetic Stripe Reader	Reads data on magnetic stripe cards.
Sensors	
Motion Sensor	3-axis accelerometer that enables motion sensing applications for dynamic screen orientation and power management.

Table 11-1 MC40 Technical Specifications (cont'd.)

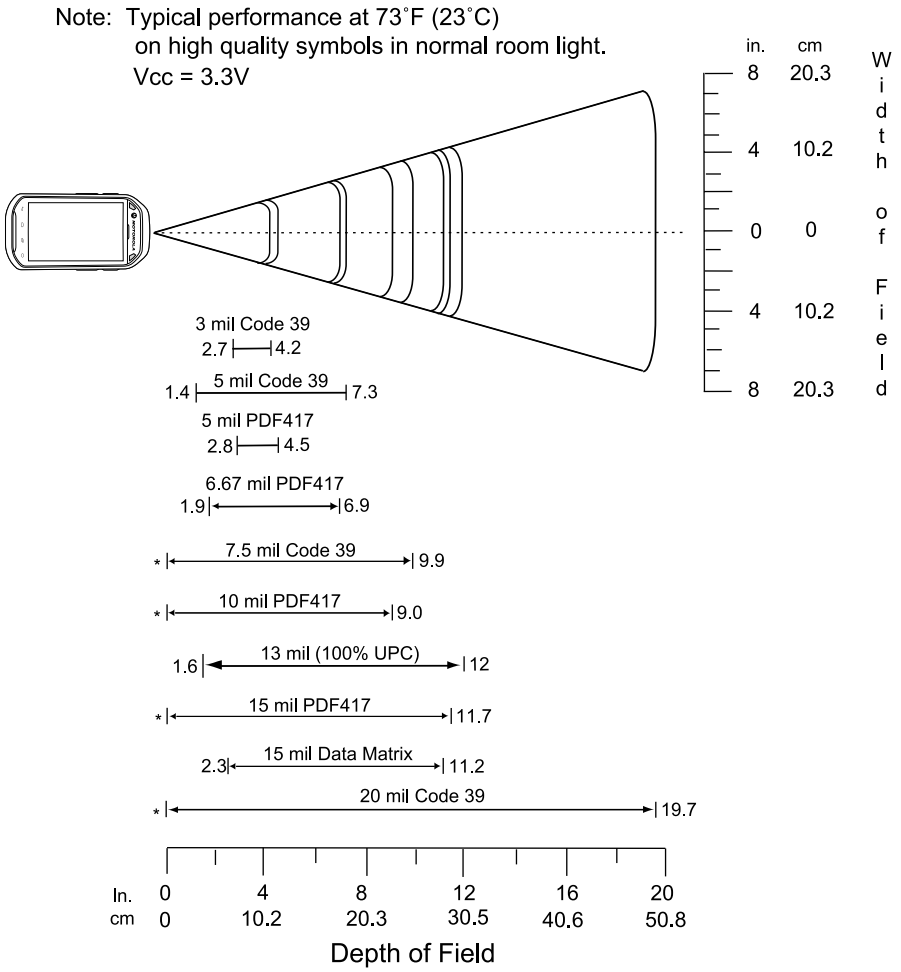
Item	Description
Ambient Light/Proximity Sensor	Automatically adjusts display brightness and turns off the display during PTT calls.
Imager (SE4500-DL) Specifications	
Field of View	Horizontal - 39.2° Vertical - 25.4°
Optical Resolution	WVGA 752 H x 480 V pixels (gray scale)
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Indoor: 450 ft. candles (4845 lux) Outdoor: 9000 ft. candles (96,900 lux) Sunlight: 8000 ft. candles Fluorescent: 450 ft. candles
Focal Distance	From center of exit window: 18.5 cm (7.3 in.)
Aiming Element (VLD)	655 nm +/- 10 nm
Illumination Element (LED)	625 nm +/- 5 nm
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.

11.2 MC40 Decode Zone

SE4500-DL

Figure A-2 shows the decode zone for the SE4500-DL. Typical values appear. Table 11-2 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.

Figure 11-1 SE4500–DL Decode Zone



* Minimum distance determined by symbol length and scan angle.

Table 11-2 SE4500-DL Decode Distances

Symbol Density/ Bar Code Type	Bar Code Content/ Contrast Note 2	Typical Working Ranges	
		Near	Far
3.0 mil Code 39	80% MRD	2.7 in 6.86 cm	4.2 in 10.67 cm
5.0 mil Code 39	ABCDEFGH 80% MRD	1.4 in 3.56 cm	7.3 in 18.54 cm
5.0 mil PDF417	80% MRD	2.8 in 7.11 cm	4.5 in 11.43 cm
6.67 mil PDF417	4 Col, 20 Rows 80% MRD	1.9 in 4.83 cm	6.9 in 17.53 cm
7.5 mil Code 39	ABCDEF 80% MRD	Note 1	9.9 in 25.15 cm

Table 11-2 SE4500-DL Decode Distances (cont'd.)

Symbol Density/ Bar Code Type	Bar Code Content/ Contrast Note 2	Typical Working Ranges	
		Near	Far
10 mil PDF417	3 Col, 17 Rows 80% MRD	Note 1	9.0 in 22.86 cm
13 mil UPC-A	012345678905 80% MRD	1.6 in 5.08 cm	12.0 in 30.48 cm
15 mil PDF417	80% MRD	Note 1	11.7 in 29.72 cm
15 mil Data Matrix	18 x 18 Modules 80% MRD	2.3 in 5.84 cm	11.2 in 28.45 cm
20 mil Code 39	123 80% MRD	Note 1	19.7 in 50.04 cm

NOTE

1. Near distances are FOV limited.
2. Contrast is measured as Mean Reflective Difference (MRD) at 670 nm
3. Working range specifications at temperature = 23°C, pitch=18°, roll=0°, skew=0°, photographic quality, ambient light ~30 ft-c, humidity 45-70%RH.
4. Distances measured from front edge of scan engine chassis.

11.3 MC40 Connector Pin-Outs

Headset Connector

Figure 11-2 Headset Connector

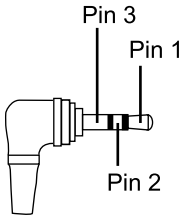


Table 11-3 Headset Connector Pin-Outs

Pin	Signal name	Description
1	Mic +	Microphone positive
2	Speaker +	peaker positive (32 ohm, 0.05 W, mono)
3	GND	Ground

Power Connector

Figure 11-3 Power Connector

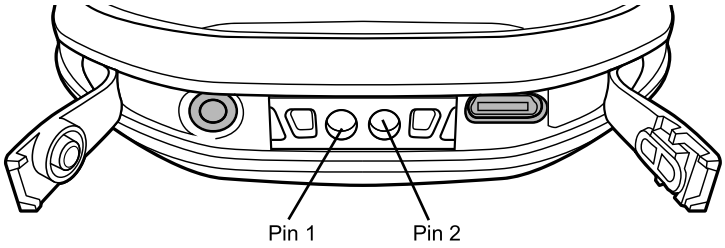


Table 11-4 Power Connector Pin-Outs

Pin	Description
1	+5 VDC input power.
2	Ground

USB Connector

Figure 11-4 micro-B USB Connector

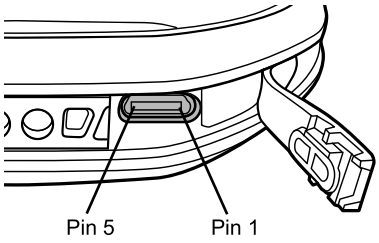


Table 11-5 micro-B USB Connector Pin-Outs

Pin	Description
1	+5 VDC
2	Data -
3	Data +
4	Permits distinction of host connection from slave
5	Signal ground

11.4 Single-Slot Charge Cradle CRDMC40XX-1000R Technical Specifications

Table 11-6 Single-slot Charge Cradle 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 (with MC40)	6 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.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

11.5 Five-Slot Charge Only Cradle CRDUNIV-40-5000R Technical Specifications

Table 11-7 Five-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions (Base only)	Height: 40.2 mm (1.6 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)
Dimensions (Base with five Charging Cups)	Height: 90.1 mm (3.5 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)
Dimensions (Base with four Charging Cups and one Battery Charger Cup	Height: 77.0 mm (3.0 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)

Table 11-7 Five-Slot Charge Only Cradle Technical Specifications (cont'd.)

Item	Description
Weight (Base only)	0.93 kg (20.5 lbs.)
Weight (Base with five Charging Cups))	1.31 kg (2.89 lbs.)
Weight (Base with four Charging Cups and one Battery Charger Cup)	1.30 kg (2.86 lbs.)
Input Voltage	12 VDC
Power Consumption (with MC40)	37.5 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	0% 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

11.6 Four-Slot Battery Charger SACMC40XX-4000R Technical Specifications

Table 11-8 Four-slot Battery Charger Technical Specifications

Item	Description
Dimensions (with USB Host Expansion Module)	Height: 59.9 mm (2.36 in.) Width: 84.0 mm (3.31 in.) Depth: 116.3 mm (4.58 in.)
Weight	257 g (9.07 in.)
Input Voltage	12 VDC
Power Consumption (with MC40)	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	0% to 95% non-condensing

Table 11-8 Four-slot Battery Charger Technical Specifications (cont'd.)

Item	Description
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

12 Keypad Remap Strings

Table 12-1 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
DPAD_RIGHT	106
DPAD_CENTER	232
VOLUME_UP	115
VOLUME_DOWN	114
CAMERA	212
A	30
B	48
C	46
D	32

Table 12-1 Remap Key Event/Scancodes (cont'd.)

Key Event	Scancode
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
SHIFT_LEFT	42
SHIFT_RIGHT	54
TAB	15
SPACE	57
EXPLORER	150
ENVELOPE	155
ENTER	28

Table 12-1 Remap Key Event/Scancodes (cont'd.)

Key Event	Scancode
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
BUTTON_THUMBL	187
BUTTON_THUMBR	188
BUTTON_START	189
BUTTON_SELECT	190
BUTTON_MODE	191

Index