



# MC40

## Mobile Computer

---

### Integrator Guide for AOSP Version 5.1.1



# **ZEBRA**



# **MC40 MOBILE COMPUTER INTEGRATOR GUIDE FOR AOSP VERSION 5.1.1**

MN-002877-04

Rev. A

April 2018

---

## Copyrights

The products described in this document may include copyrighted computer programs. Laws in the United States and other countries preserve for certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted computer programs contained in the products described in this document may not be copied or reproduced in any manner without the express written permission.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission.

Furthermore, the purchase of our products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

---

## Disclaimer

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

---

## Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev. A	7/2016	Initial release.
-02 Rev. A	12/2016	Updated to include operating system changes.
-03 Rev. A	4/2017	Correct Enterprise Reset description on page 1-5.
-04 Rev. A	4/2018	Update approved cleanser active ingredients.

# TABLE OF CONTENTS

Copyrights .....	ii
Disclaimer .....	ii
Trademarks .....	ii
Revision History .....	ii

## About This Guide

Documentation Set .....	7
Configurations .....	7
Software Versions .....	8
Build Number .....	8
Chapter Descriptions .....	8
Notational Conventions .....	9
Icon Conventions .....	9
Related Documents .....	10
Service Information .....	10

## Chapter 1: Getting Started

Unpacking .....	1-1
Setup .....	1-1
Installing the Battery .....	1-1
Charging the Battery .....	1-2
Charging Temperature .....	1-3
Charging Spare Batteries .....	1-3
Powering On the MC40 .....	1-3
Replacing the Battery .....	1-3
Resetting the Device .....	1-5
Performing a Soft Reset .....	1-5
Performing a Hard Reset .....	1-5
Performing an Enterprise Reset .....	1-5
Performing a Factory Reset .....	1-6

**Chapter 2: Accessories**

MC40 Accessories .....	2-1
Single Slot Charge Only Cradle .....	2-3
Single Slot Charge Cradle Setup .....	2-3
Removing Cradle Insert .....	2-4
Charging Using the Single Slot Charge Only Cradle .....	2-5
Four Slot Battery Charger .....	2-7
Single Charger Setup .....	2-7
Two Charger Setup .....	2-7
Four Charger Setup .....	2-8
Charging with the Four Slot Battery Charger .....	2-9
Five Slot Charge Only Cradle .....	2-11
Installing a Cup .....	2-11
Installing a Four Slot Battery Charger .....	2-12
Power to Five Slot Charge Only Cradle .....	2-13
Removing Cradle Insert .....	2-14
Charging Using the Five Slot Charge Only Cradle .....	2-15
Installing the Finger Strap .....	2-16
Installing the Rubber Boot .....	2-19
Ethernet Settings .....	2-21
Configuring Ethernet Proxy Settings .....	2-21
Configuring Ethernet Static IP Address .....	2-22

**Chapter 3: USB Communication**

Connecting to a Host Computer via USB .....	3-1
Disconnect from the Host Computer .....	3-2

**Chapter 4: DataWedge Configuration**

DataWedge Configuration .....	4-1
Basic Scanning .....	4-1
Using the Imager .....	4-1
Using the Camera .....	4-2
Profiles .....	4-2
Profile0 .....	4-3
Plug-ins .....	4-3
Input Plug-ins .....	4-3
Output Plug-ins .....	4-4
Process Plug-ins .....	4-4
Profiles Screen .....	4-4
Profile Context Menu .....	4-5
Options Menu .....	4-6
Disabling DataWedge .....	4-6
Creating a New Profile .....	4-6
Profile Configuration .....	4-7
Associating Applications .....	4-7
Data Capture Plus .....	4-11
Bar Code Input .....	4-14
Enabled .....	4-14

Scanner Selection .....	4-14
Decoders .....	4-14
Decoder Params .....	4-16
Decode Lengths .....	4-22
UPC EAN Params .....	4-22
Reader Params .....	4-24
Scan Params .....	4-26
Keep enabled on suspend .....	4-27
MSR Input .....	4-27
Keystroke Output .....	4-28
Intent Output .....	4-28
Intent Overview .....	4-29
IP Output .....	4-31
Usage .....	4-31
Using IP Output with IPWedge .....	4-32
Using IP Output without IPWedge .....	4-33
Generating Advanced Data Formatting Rules .....	4-35
Configuring ADF Plug-in .....	4-35
Creating a Rule .....	4-36
Defining a Rule .....	4-36
Defining Criteria .....	4-37
Defining an Action .....	4-39
Deleting a Rule .....	4-39
Order Rules List .....	4-40
ADF Example .....	4-41
DataWedge Settings .....	4-44
Importing a Configuration File .....	4-45
Exporting a Configuration File .....	4-46
Importing a Profile File .....	4-46
Exporting a Profile .....	4-46
Restoring DataWedge .....	4-46
Configuration and Profile File Management .....	4-47
Enterprise Folder .....	4-47
Auto Import .....	4-47
Programming Notes .....	4-47
Capture Data and Taking a Photo in the Same Application .....	4-48
Disable DataWedge on MC40 and Mass Deploy .....	4-48
Soft Scan Feature .....	4-48
Sample .....	4-48

## Chapter 5: WLAN Configuration

Connecting to a Wi-Fi Network .....	5-1
Manually Adding a Wi-Fi Network .....	5-2
Configuring for a Proxy Server .....	5-3
Ethernet Settings .....	5-4
Configuring Ethernet Proxy Settings .....	5-4
Configuring Ethernet Static IP Address .....	5-5
Advanced Wi-Fi Settings .....	5-6
Additional Wi-Fi Settings .....	5-6

Enable Logging .....	5-8
Additional Wi-Fi Advanced Features .....	5-9
Zebra Mobility Extensions .....	5-10
Remove a Wi-Fi Network .....	5-10

## Chapter 6: Settings

Screen Unlock Settings .....	6-1
Single User Mode .....	6-1
Set Screen Unlock Using PIN .....	6-2
Set Screen Unlock Using Password .....	6-2
Set Screen Unlock Using Pattern .....	6-3
Passwords .....	6-4
Button Remapping .....	6-5
Remapping a Button .....	6-5
Setting the Headset Key .....	6-6
Enterprise Reset .....	6-8
Accounts .....	6-9
Language Usage .....	6-9
Changing the Language Setting .....	6-9
Adding Words to the Dictionary .....	6-9
Keyboard Settings .....	6-9
Date Persistence .....	6-10
Ethernet Settings .....	6-11
Configuring Ethernet Proxy Settings .....	6-11
Configuring Ethernet Static IP Address .....	6-12
About Device .....	6-13
PTT Express Configuration .....	6-13
Importing a PTT Express Configuration File .....	6-13
Remapping the PTT Private Key .....	6-14
Low RAM Device Configuration .....	6-15

## Chapter 7: Application Deployment

Security .....	7-1
Secure Certificates .....	7-1
Installing a Secure Certificate .....	7-1
Configuring Credential Storage Settings .....	7-2
Development Tools .....	7-2
ADB USB Setup .....	7-3
Application Installation .....	7-3
Installing Applications Using the USB Connection .....	7-4
Installing Applications Using the Android Debug Bridge .....	7-5
Mobility Services Platform .....	7-5
Uninstalling an Application .....	7-5
System Update .....	7-6
Copying Applications and Configuration Files .....	7-7
Upgrading the Operating System from KitKat to Lollipop .....	7-8
Converting Non-Voice Configuration to Voice Configuration .....	7-8
Upgrading to Lollipop .....	7-9



Storage .....	7-11
Random Access Memory .....	7-11
On Device Storage .....	7-12
Internal Storage .....	7-13
Enterprise Folder .....	7-13
Application Management .....	7-14
Viewing Application Details .....	7-15
Stopping an Application .....	7-15
Changing Application Location .....	7-16
Managing Downloads .....	7-16
RxLogger .....	7-17
RxLogger Configuration .....	7-17
Main Log Plug-in .....	7-18
PushPullClient Plug-in .....	7-19
KernelLog Plug-in .....	7-19
ANR Plug-in .....	7-20
LTS Plug-in .....	7-20
Logcat Plug-in .....	7-20
Tombstone Plug-in .....	7-21
QxdmLog Plug-in .....	7-22
RamOops Plug-in .....	7-22
Snapshot Plug-in .....	7-22
TCPDump Plug-in .....	7-23
Configuration File .....	7-23
Enabling Logging .....	7-23
Disabling Logging .....	7-23
Extracting Log Files .....	7-24

## Chapter 8: Maintenance and Troubleshooting

Maintaining the MC40 .....	8-1
Battery Safety Guidelines .....	8-1
Cleaning Instructions .....	8-2
Approved Cleanser Active Ingredients .....	8-2
Harmful Ingredients .....	8-2
Cleaning Instructions .....	8-2
Special Cleaning Notes .....	8-3
Cleaning Materials Required .....	8-3
Cleaning Frequency .....	8-3
Cleaning the MC40 .....	8-3
Housing .....	8-3
Display .....	8-3
Exit and Camera Window .....	8-3
Connector Cleaning .....	8-3
Cleaning Cradle Connectors .....	8-4
Troubleshooting .....	8-4
Troubleshooting the MC40 .....	8-4
Single-Slot Charge Cradle Troubleshooting .....	8-6
Five-Slot Charge Only Cradle CRDUNIV-40-5000R Troubleshooting .....	8-7
Four-Slot Battery Charger SACMC40XX-4000R Troubleshooting .....	8-7

**Appendix A: Technical Specifications**

MC40 Technical Specifications ..... A-1

MC40 Decode Zone ..... A-5

    SE4500-DL ..... A-5

    SE4710 ..... A-6

MC40 Connector Pin-Outs ..... A-7

    Headset Connector ..... A-7

    Power Connector ..... A-7

    USB Connector ..... A-8

Single-Slot Charge Cradle CRDMC40XX-1000R Technical Specifications ..... A-9

Five-Slot Charge Only Cradle CRDUNIV-40-5000R Technical Specifications ..... A-10

Four-Slot Battery Charger SACMC40XX-4000R Technical Specifications ..... A-11

**Appendix B: Keypad Remap Strings**

# 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.

This guide covers Android™ operating system Android Open Source Project (AOSP) Version 5.1.1 (Lollipop).

---

## 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/r WPAN: Bluetooth v 4.0 Low Energy	4.3" color WVGA	1 GB RAM / 8 GB Flash	camera and imager or camera, imager and MSR, optional RS507 Hands-free Imager	Android-based, Android Open-Source Project 5.1.1 (Lollipop)

## Software Versions

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

- **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.

To determine the device serial number, touch  >  **About device** > **Status**.

- **Serial number** - Displays the serial number.

To determine the Device Patch Version, touch  >  **About device** > **SW components**.

- **Device Patch Version** - Displays the device patch version number.

Over-the-Air (OTA) update packages/incremental updates allow for patching the device with necessary software updates.

## Build Number

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

Example Build Number: XX-XX-XX-L-V0-M1

- XX - Software version number
- L - Lollipop
- V - VoIP telephony ready / F - FIPS & VoIP telephony ready
- M - Hardware version number

## Chapter Descriptions

Topics covered in this guide are as follows:

- [Getting Started](#) provides information on getting the MC40 up and running for the first time.
- [Accessories](#) describes the available accessories and how to use them with the MC40.
- [USB Communication](#) describes how to connect the MC40 to a host computer using USB.
- [DataWedge Configuration](#) describes how to use and configure the DataWedge application.
- [WLAN Configuration](#) describes the how to configure the MC40 to connect with a wireless LAN network.
- [Administrator Utilities](#) provides information for using the suite of administrative tools for configuring the MC40.
- [Settingsfor Android Devices](#) provides the settings for configuring the MC40.
- [Application Deploymentfor Android Devices](#) provides information for developing and managing applications.

- [Maintenance and Troubleshooting](#) includes instructions on cleaning and storing the MC40, and provides troubleshooting solutions for potential problems during MC40 operation.
- [Technical Specifications](#) provides the technical specifications for the MC40.
- [Keypad Remap Strings](#) 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 User Guide*, p/n MN-002851-xx
- *RS507 Hands-free Imager Product Reference Guide*, p/n 72E-120802-xx

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

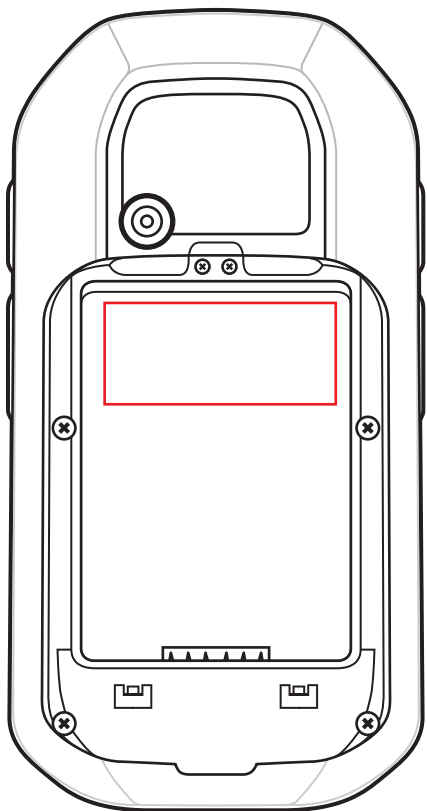
---

## Service Information

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

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

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



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

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

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





# CHAPTER 1 GETTING STARTED

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

---

## 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 Zebra Support Center immediately. See Service Information for contact information.

---

## Setup

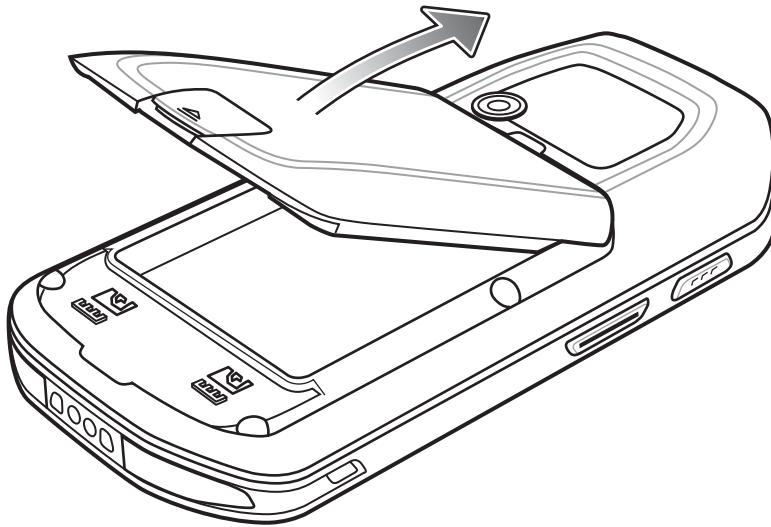
To start using the MC40 for the first time:

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

### Installing the Battery

To install the battery:

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.

## Charging the Battery



**CAUTION** Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 8-1](#).

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 on page 1-3](#) 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 [Chapter 2, Accessories](#).

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 see [Chapter 2, Accessories](#).

- 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. The battery is below 20%.
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 [Chapter 2, Accessories](#) for information on using accessories to charge spare batteries.

## Powering On the MC40

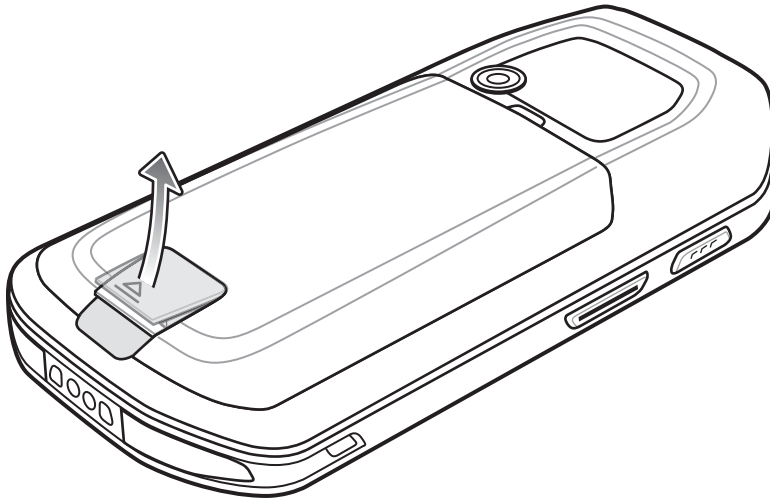
If the MC40 did not turn on when the battery was installed, press the Power button until the Right and Left LEDs flash once. The splash screen displays for about a minute as the MC40 initializes its flash file system. Note that these windows also appear upon reset.

✓ **NOTE** The MC40 Android Lollipop version contains a known limitation that for every first reboot (after flashing or an enterprise/factory reset), the device may take approximately eight minutes to boot to the home screen.

## Replacing the Battery

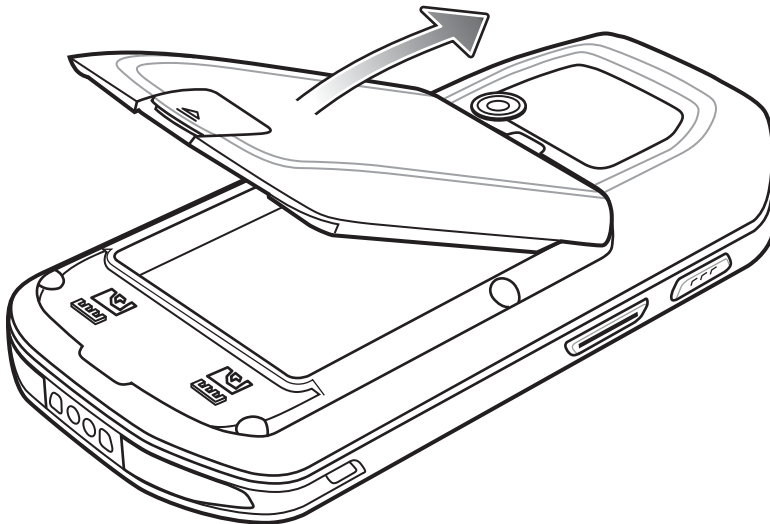
✓ **NOTE** Ensure that the Battery Swap mode procedures are followed, otherwise the backup battery will deplete quickly.

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 turn 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.

---

## Resetting the Device

There are four reset functions:

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

### Performing a Soft Reset

Perform a soft reset if applications stop responding.

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

### Performing a Hard Reset

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

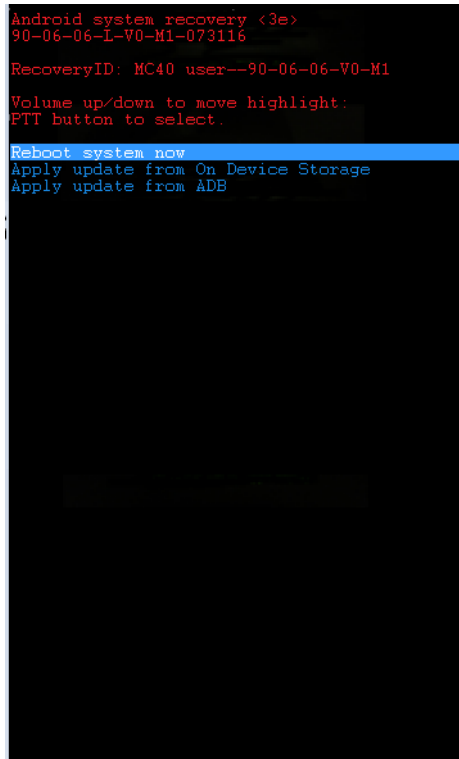
1. Simultaneously press the Power, Left Scan/Action and Up Volume buttons.
2. The device shuts down and then reboots.

### Performing an Enterprise Reset

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

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

1. Download the Enterprise Reset file from the Zebra Support & Downloads web site.
2. Copy the Enterprise Reset zip file (*M40N0LXXXRE0000002.zip*) to the root directory of the On Device Storage. See [Chapter 3, USB Communication](#).
3. Press and hold the Power button until the menu appears.
4. Touch **Reboot**. The device shuts down and then reboots.
5. Press and hold the Left Scan/Action button.
6. When the System Recovery screen appears release the button.



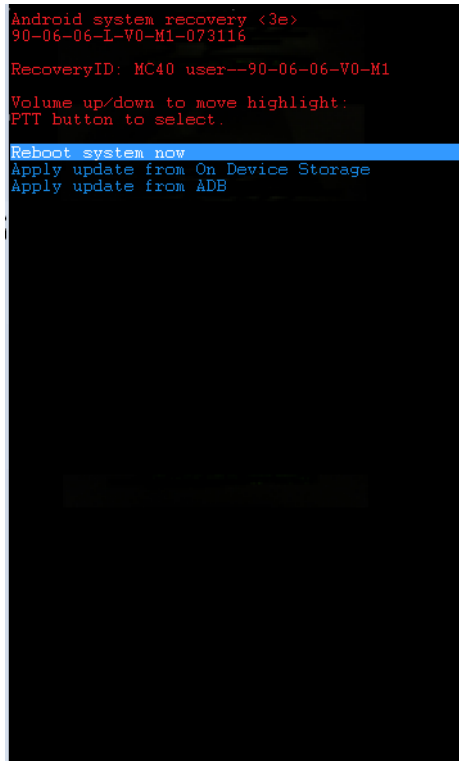
**Figure 1-4** System Recovery Screen

7. Press the Up and Down Volume buttons to navigate to the **Apply update from On Device Storage** option.
8. Press the PTT button.
9. Press the Up and Down Volume buttons to navigate to the Enterprise Reset zip file (*M40N0LXXXRE0000002.zip*).
10. Press the PTT button. The Enterprise Reset occurs and then the device resets.
11. Press the Volume Up and Volume Down buttons to navigate to the **Reboot system now** option.
12. Press the PTT button to reboot the device.

## 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 [System Update on page 7-6](#) for more information.

1. Download the Factory Reset file from the Zebra Support & Downloads web site.
2. Copy the Factory Reset zip file (*M40N0LXXXRF0000002.zip*) to the root directory of the On Device Storage. See [Chapter 3, USB Communication](#).
3. Press and hold the Power button until the menu appears.
4. Touch **Reboot**. The device shuts down and then reboots.
5. Press and hold the Left Scan/Action button.
6. When the System Recovery screen appears release the button.



**Figure 1-5** System Recovery Screen

7. Press the Up and Down volume buttons to navigate to the **Apply update from On Device Storage** option.
8. Press the PTT button.
9. Press the Up and Down volume buttons to navigate to the Factory Reset zip file (*M40N0LXXXRF0000002.zip*).
10. Press the PTT button. The Factory Reset occurs and then the device resets.
11. Press the Volume Up and Volume Down buttons to navigate to the **Reboot system now** option.
12. Press the PTT button to reboot the device.





# CHAPTER 2 ACCESSORIES

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

## MC40 Accessories

MC40 Accessories lists the accessories available for the MC40.

Table 2-1 MC40 Accessories

Accessory	Part Number	Description
<b>Cradles</b>		
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.
<b>Chargers</b>		
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.
<b>Cables</b>		
Micro USB Cable	25-MCXUSB-01R	Provides power to the MC40 and USB communication with a host computer.

**Table 2-1** MC40 Accessories (Continued)

Accessory	Part Number	Description
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.
<b>Miscellaneous</b>		
Spare 2680 mAh lithium-ion battery	BTRY-MC40EAB0E	Replacement 2680 mAh battery.
	BTRY-MC40EAB0E-10R	Replacement 2680 mAh battery (10-pack)
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).
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.
Wired Headset	HDST-25MM-PTVP-01	2.5 mm wired headset for PTT and VoIP telephony communications.

---

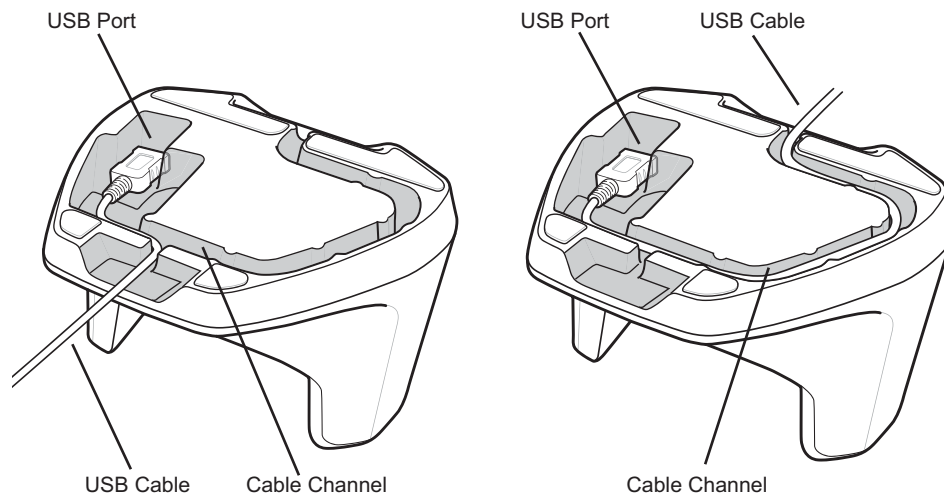
## Single Slot Charge Only Cradle

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.

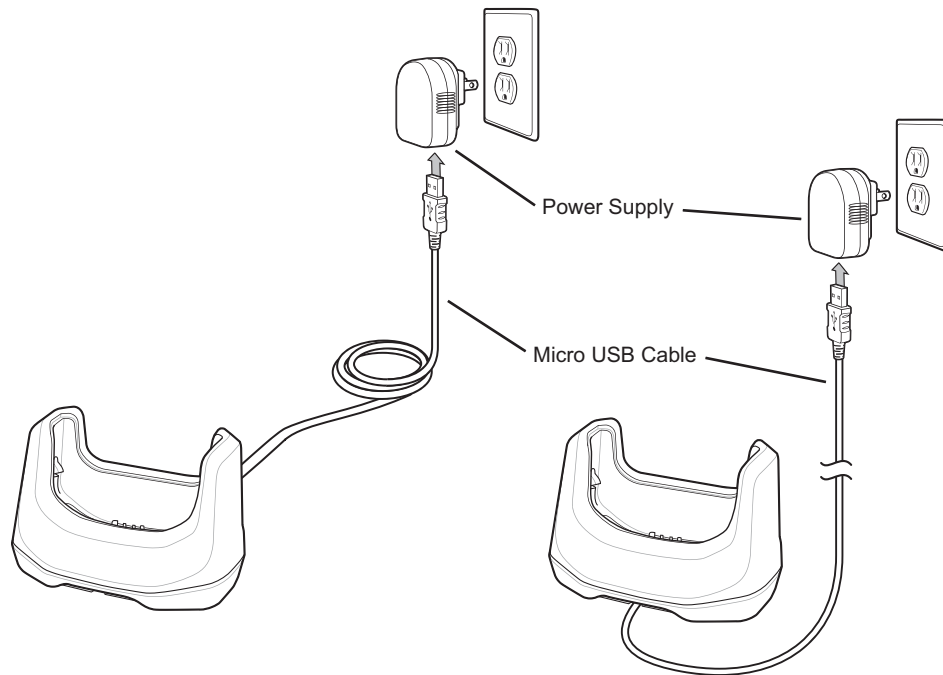
### Single Slot Charge Cradle Setup

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*

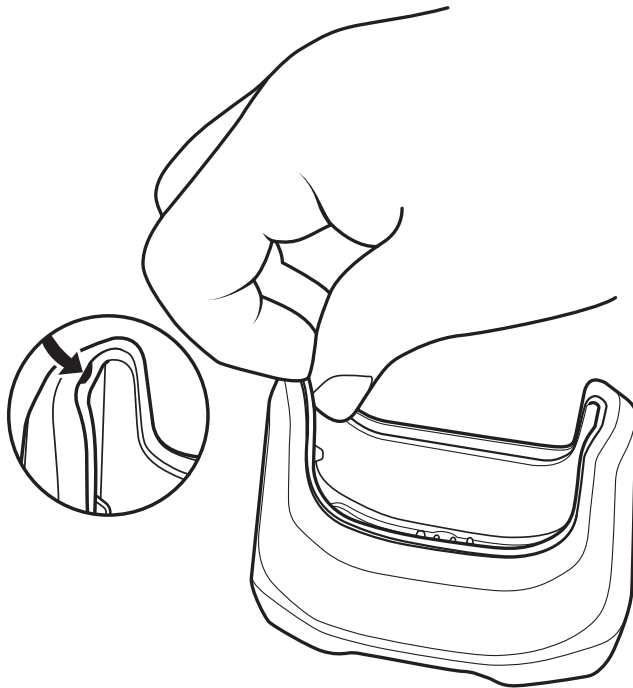
3. Plug the other end of the Micro USB Cable into the USB port on the power supply.
4. Plug the power supply into a wall outlet.



**Figure 2-2** *Single Slot Charge Only Cradle Setup*

## Removing Cradle Insert

1. With finger nail, grasp insert notch.



**Figure 2-3** *Grasp Insert Notch*

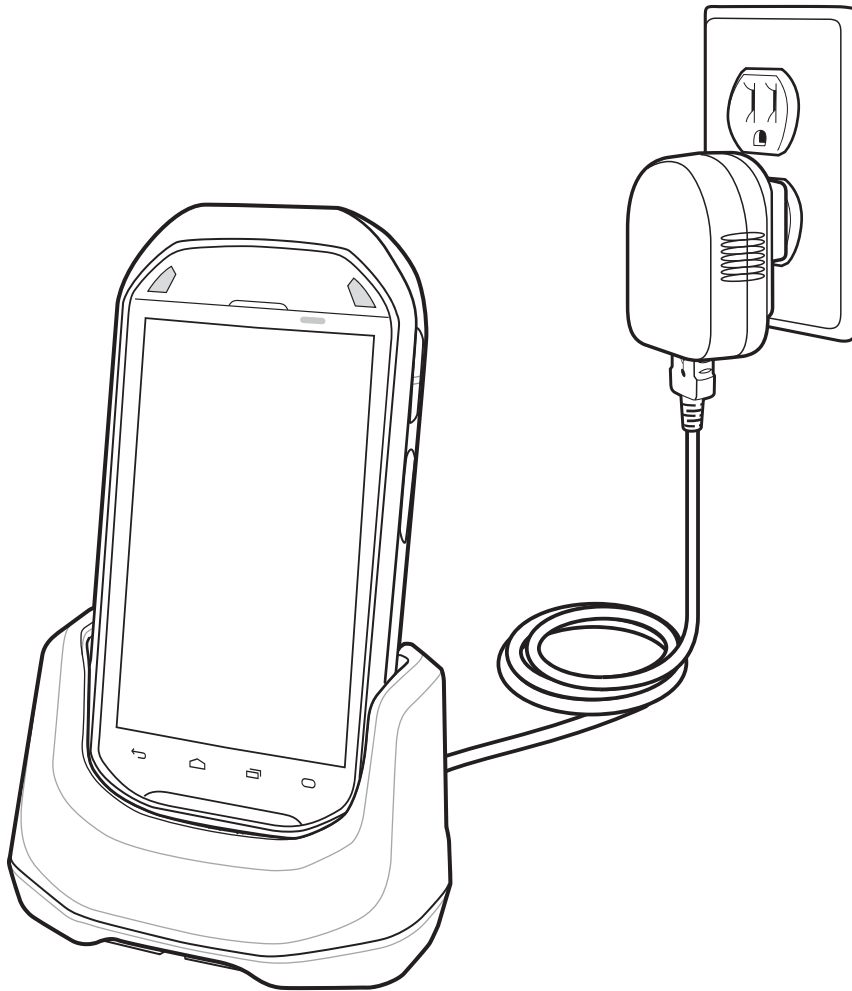
2. Pull insert out of cradle.



**Figure 2-4** *Remove Insert*



### **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 on page 1-3](#) 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.

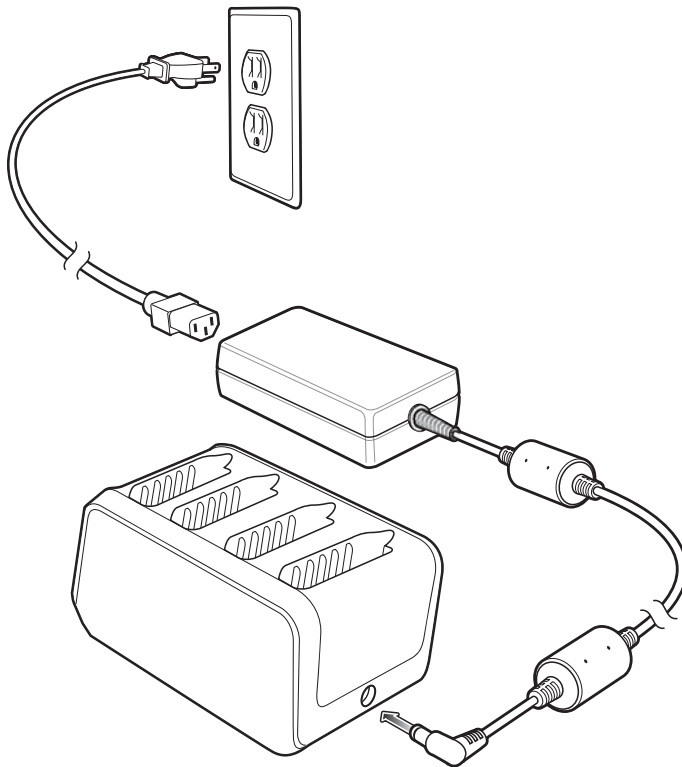
---

## Four Slot Battery Charger

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

### Single Charger Setup

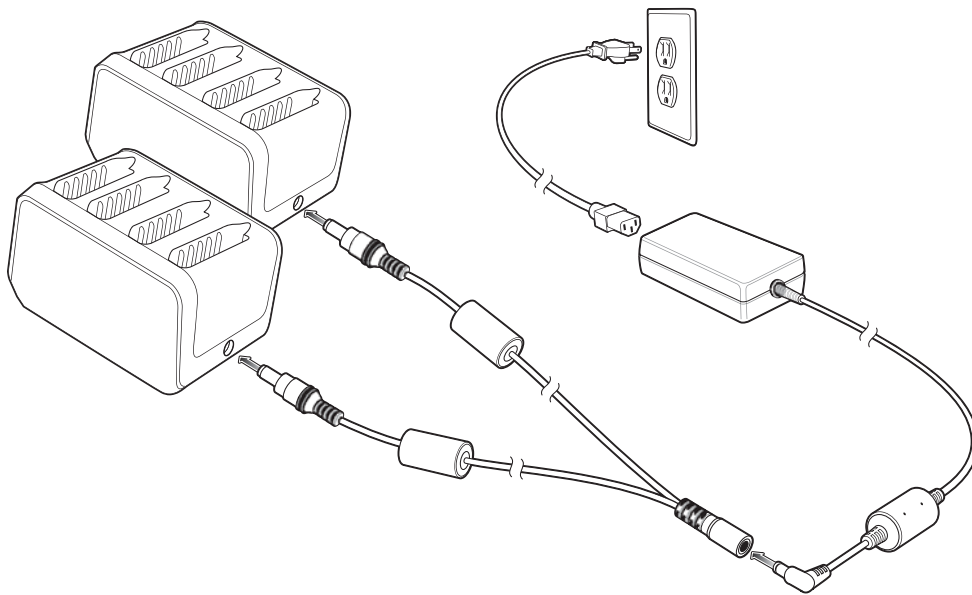
1. Plug the power supply plug into the power port on the back of the charger.
2. Plug the AC line cord into the power supply.
3. Plug the AC line cord into an AC outlet.



**Figure 2-6** *Four Slot Battery Charger*

### Two Charger Setup

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.

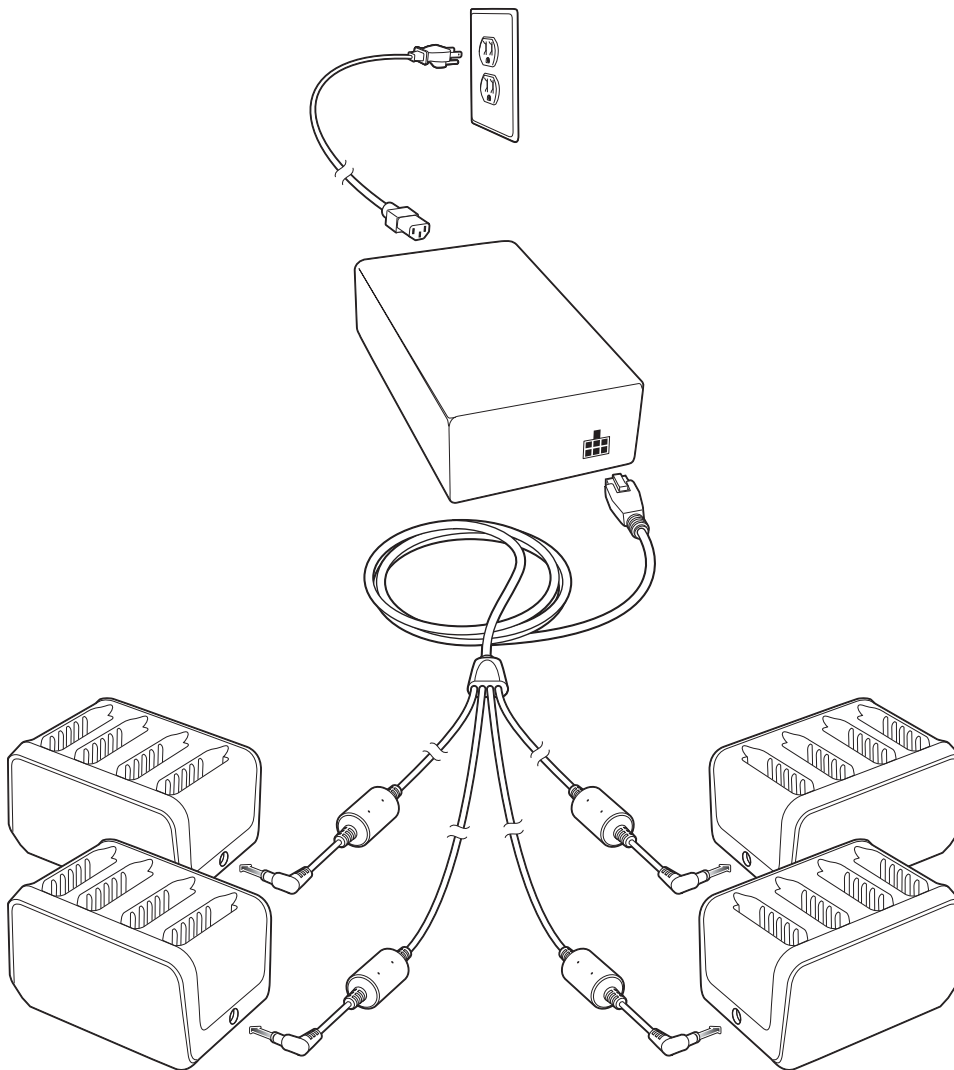


**Figure 2-7** Setup with 2-way DC Cable

## Four Charger Setup

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.



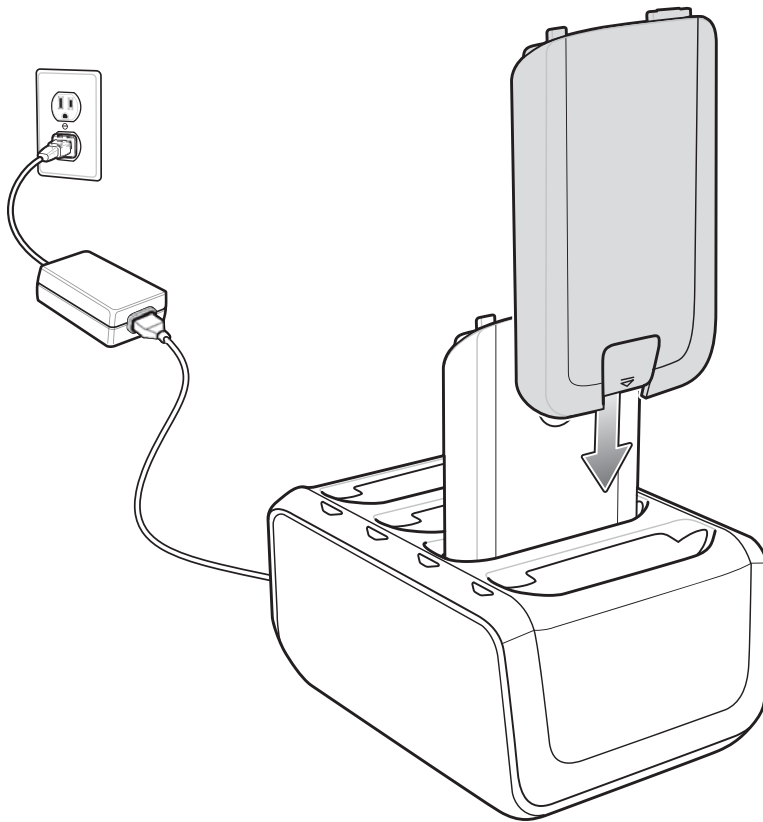


**Figure 2-8** Setup with 4-way DC Cable

## 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 on page 2-10](#) 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

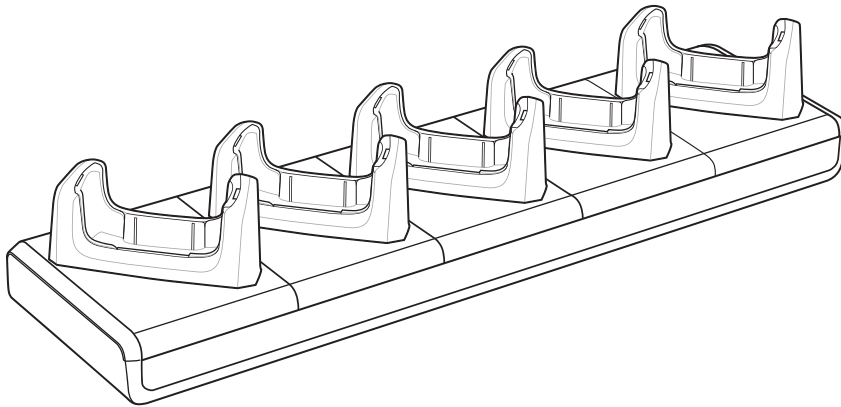
Status	Indications
Off	No battery a slot. Battery is not charging. Battery is not inserted correctly in the charger. Charger is not powered.
Slow Blinking Amber	Battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Charging error, e.g.: <ul style="list-style-type: none"> <li>• Temperature is too low or too high.</li> <li>• Charging has gone on too long without completion.</li> </ul>

---

## 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.

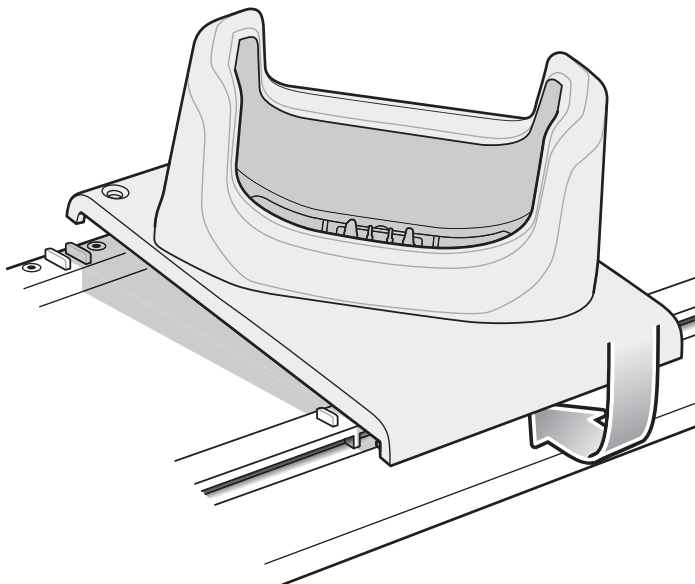


**Figure 2-10** *Five Slot Charge Only Cradle*

### Installing a Cup

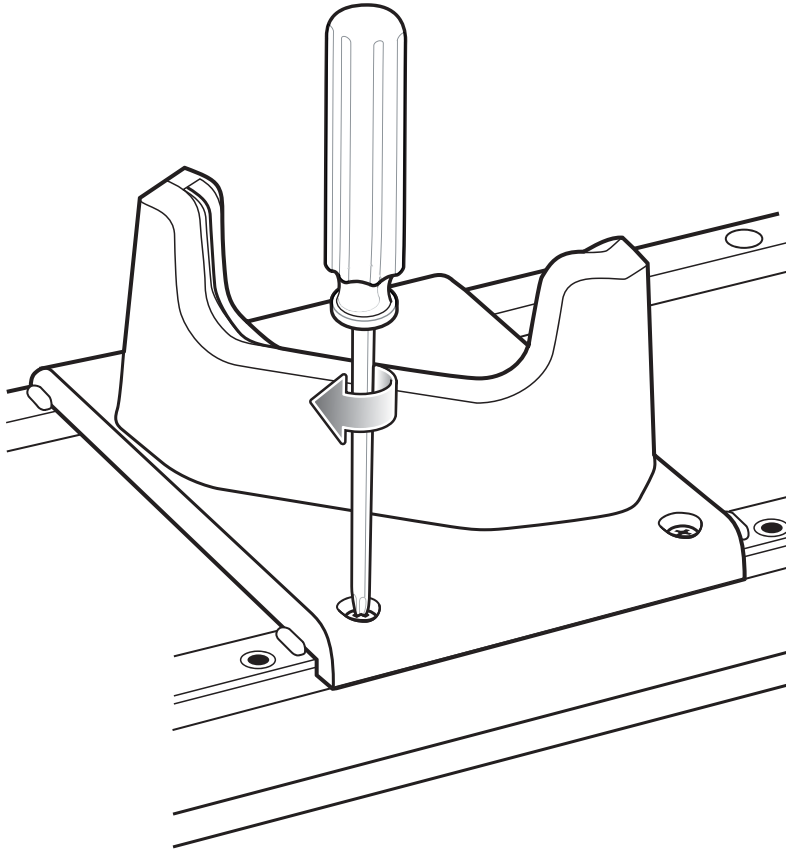
The Five Slot Charge Only Cradle ships without any cradle cups installed. To base accepts the MC40 Charging Cup, Battery Charger Cup and Blank Slot Cover. To install the cradle cups:

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.



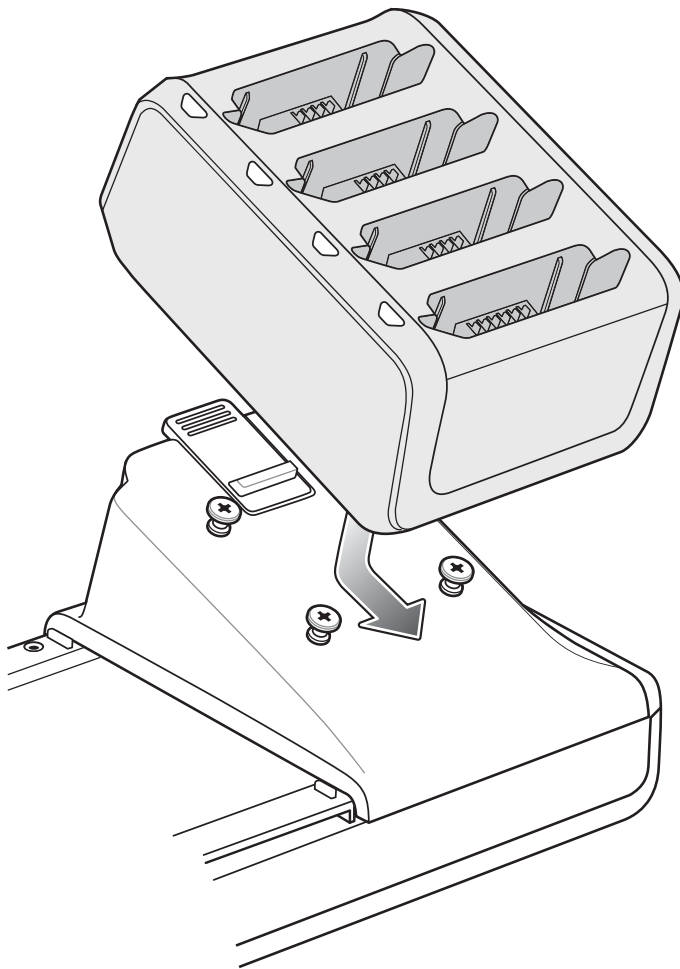
**Figure 2-12** *Securing Cup to Base*

5. Each slot on the Cradle Base must have a cup installed.
6. Repeat for each additional cup.

## Installing a Four Slot Battery Charger

To install a Four Slot Battery Charger:

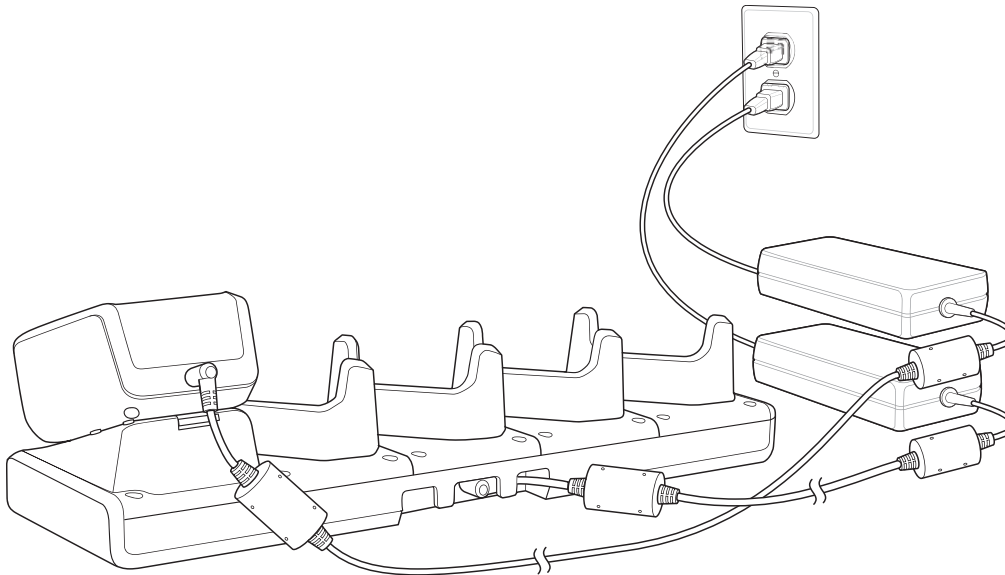
1. Install a Battery Charger Cup. See [Installing a Cup on page 2-11](#).
2. Align the mounting slots on the bottom of the Four Slot Battery Charger with the screws on the cup.
3. Slide the Four Slot Battery Charger down until it snaps into place.



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

## **Power to Five Slot Charge Only Cradle**

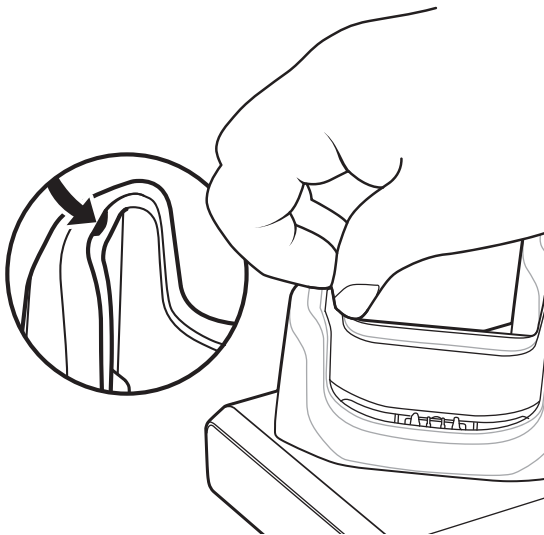
Use one power supply to provide power to the Charging Base to power the Charging Cups. A separate power supply is required for each Four Slot Battery Charger installed. The power supply is connected directly to the Four Slot Battery Charger.



**Figure 2-14** *Five Slot Charge Only Cradle Power Connections*

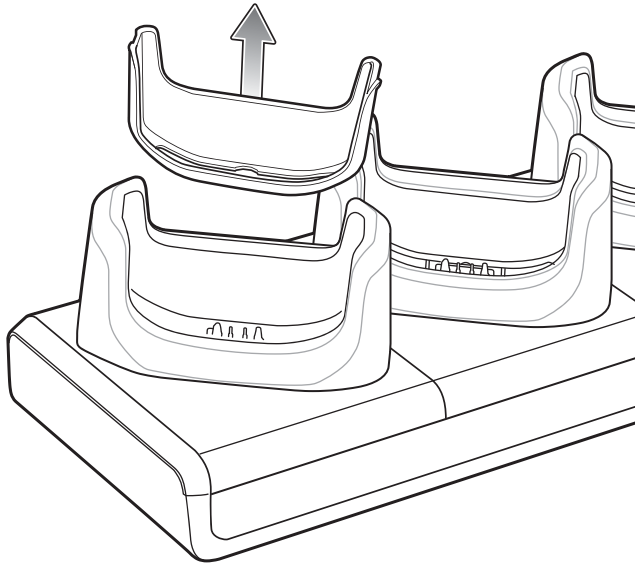
## Removing Cradle Insert

1. With finger nail, grasp insert notch.



**Figure 2-15** *Grasp Insert Notch*

2. Pull insert out of cradle.





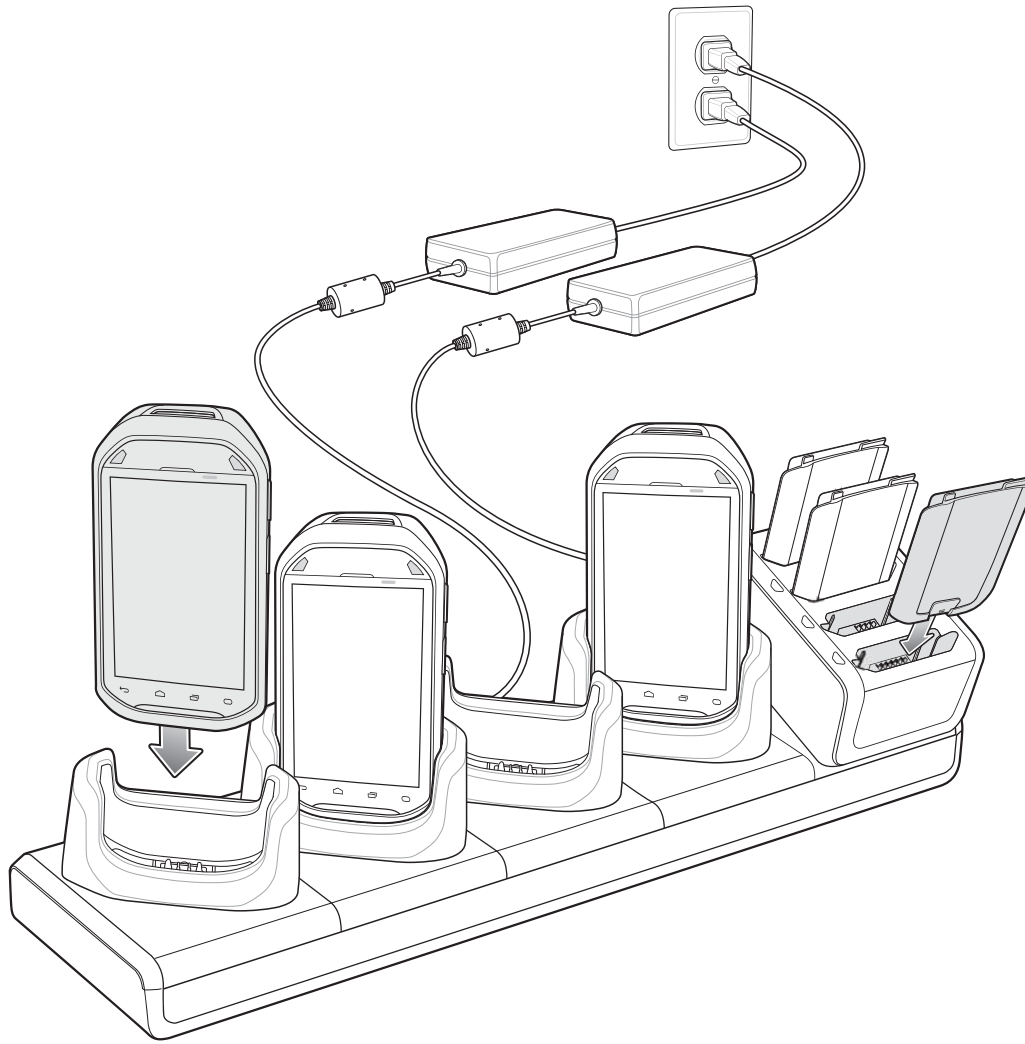
**Figure 2-16** *Remove Insert*

## 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 on page 1-3](#) 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*

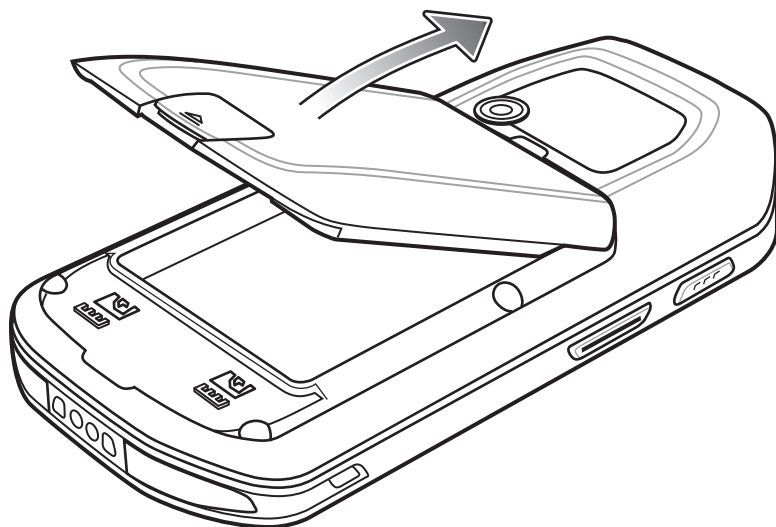
---

## Installing the Finger Strap

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

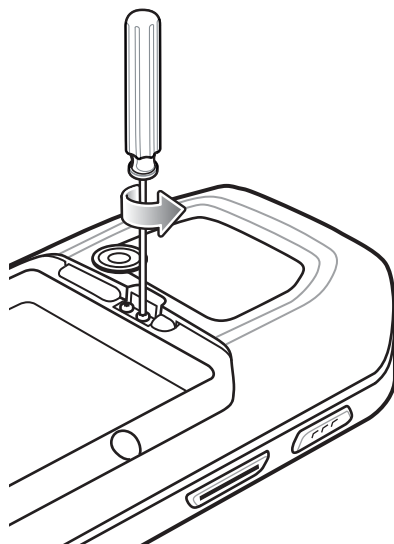
1. Press the Power button until the Device options menu appears.
2. Touch Power off.
3. Remove the battery.





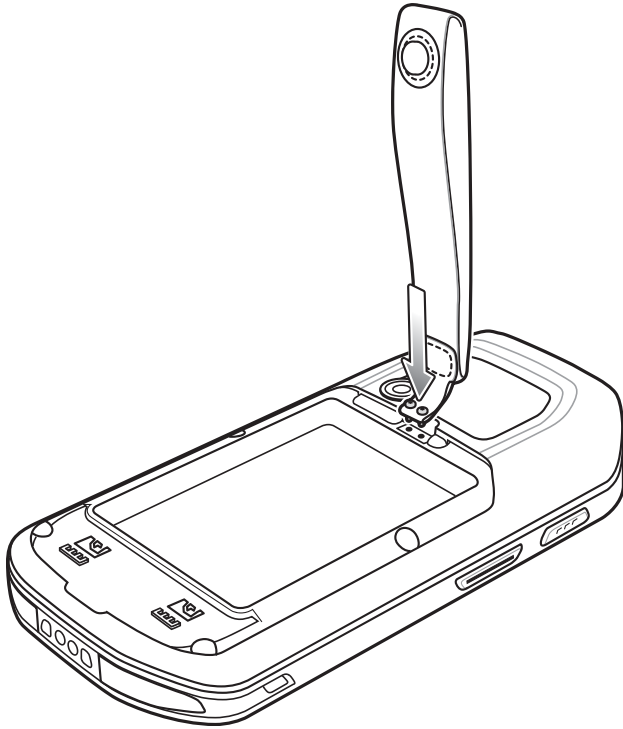
**Figure 2-18** *Remove Battery*

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



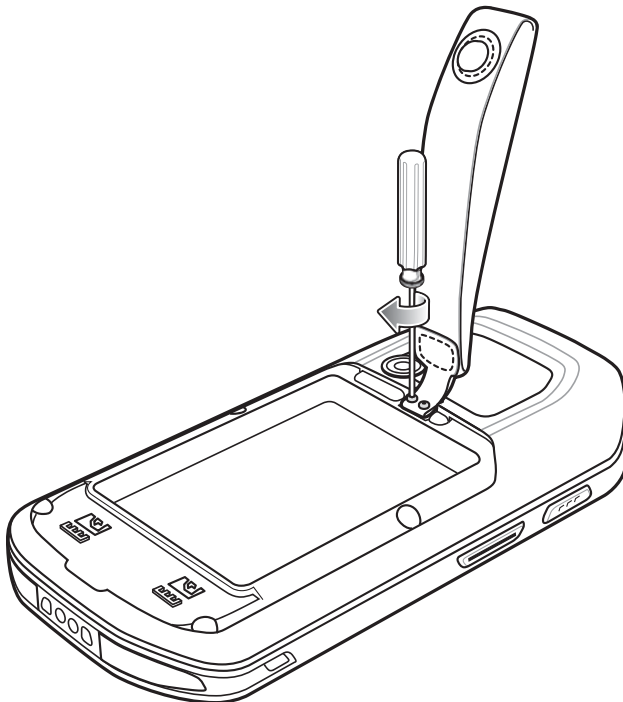
**Figure 2-19** *Remove Plug*

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



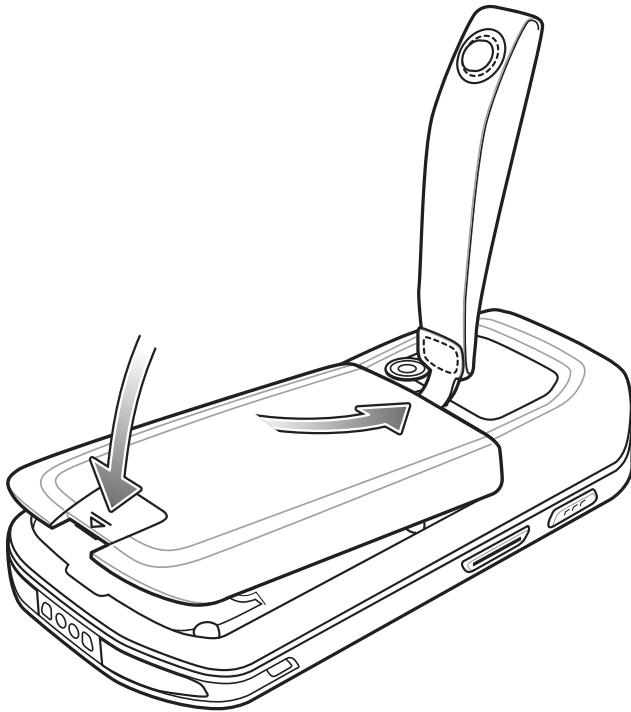
**Figure 2-20** *Align Finger Strap*

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



**Figure 2-21** *Secure Finger Strap to MC40*

7. Replace the battery.

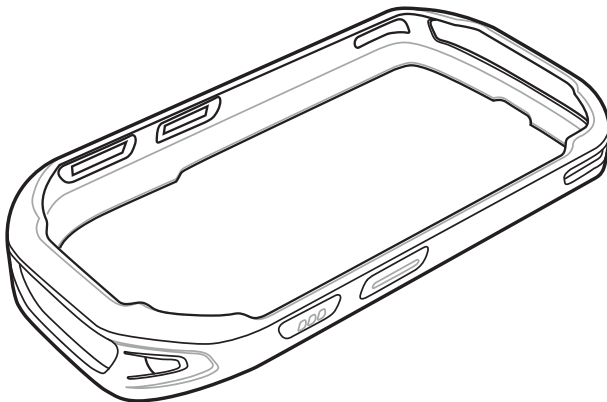


**Figure 2-22** *Install Battery*

---

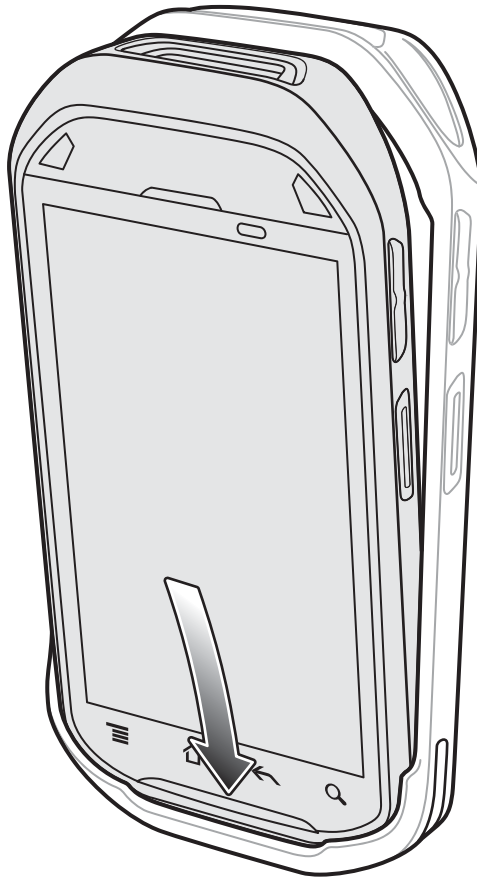
## Installing the Rubber Boot

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



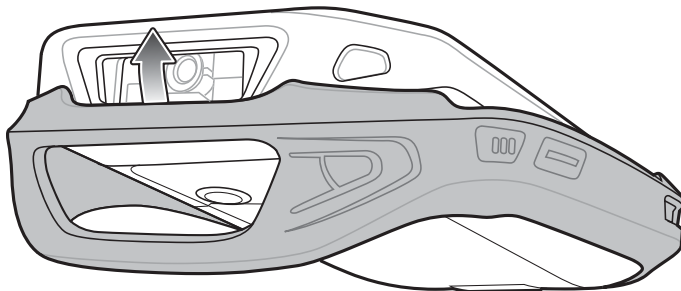
**Figure 2-23** *Rubber Boot*

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.




## Ethernet Settings

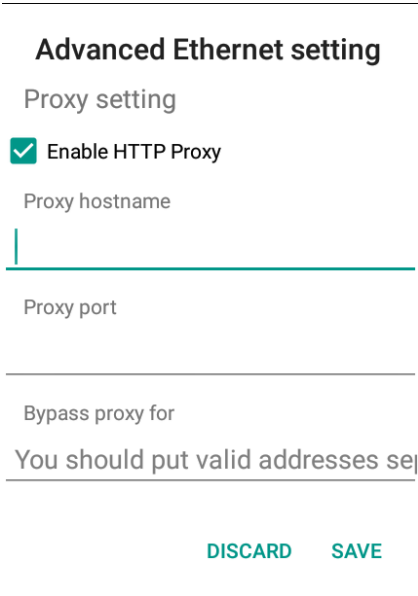
The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

### Configuring Ethernet Proxy Settings

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Advanced**.




**Figure 2-26** Ethernet Proxy Settings

5. Touch **Enable HTTP Proxy**.
6. In the **Proxy hostname** field, enter the proxy server address.
7. In the **Proxy port** field, enter the proxy server port number.






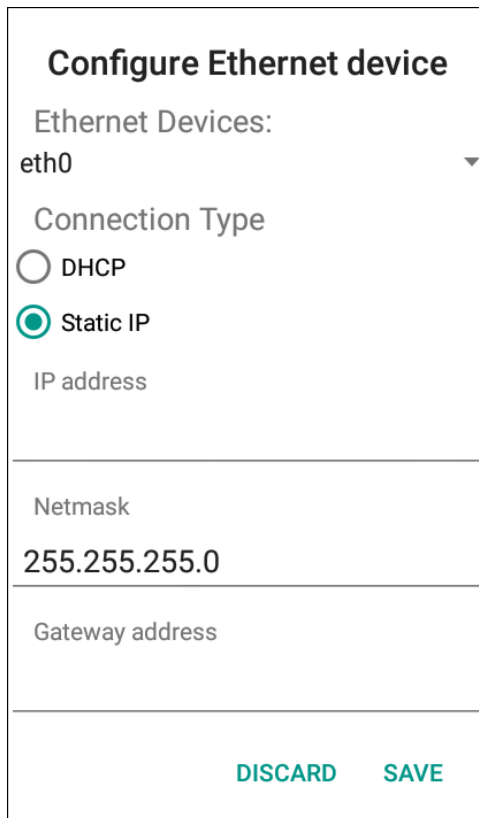
**NOTE** When entering proxy addresses in the **Bypass proxy for** field, do not use spaces or carriage returns between addresses.

8. 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.
9. Touch **Save**.
10. Touch .

## Configuring Ethernet Static IP Address

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection. By default, the device is configured to use Dynamic Host Configuration Protocol (DHCP) to assign an Internet Protocol (IP) address when connecting to an Ethernet network. To configure the device to connect to a network using a static IP address:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Config**.



**Configure Ethernet device**

Ethernet Devices:  
eth0

Connection Type

☐ DHCP

☒ Static IP

IP address

---

Netmask

255.255.255.0


---

Gateway address

---

**DISCARD** **SAVE**

**Figure 2-27** *Configure Ethernet Device Settings*

5. Under **Connection Type**, touch the **Static IP** radio button.  
**DHCP** is the default **Connection Type**.
6. In the **IP address** field, enter the proxy server address.
7. If required, in the **Netmask** text box, enter the network mask address.
8. If required, in the **Gateway address** text box, enter a gateway address for the device.
9. If required, in the **DNS 1 address** text box, enter a Domain Name System (DNS) address.
10. If required, in the **DNS 2 address** text box, enter a DNS address.
11. Touch **Save**.
12. Touch .

# CHAPTER 3 USB COMMUNICATION

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

---

## 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. ADB connectivity on Android Lollipop requires the latest ADB driver (1.0.32 or later) to be installed on the 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.

1. Connect the micro USB connector to the USB port on the device. See [Chapter 2, Accessories](#) for setup information.
2. Connect the USB A connector to the host computer USB port.  
**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)**.



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

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



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

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

---

## 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.

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



# CHAPTER 4 DATAWEDGE CONFIGURATION

---

## DataWedge Configuration

This chapter applies to DataWedge on Android devices. DataWedge is an application that reads data, processes the data and sends the data to an application.

---

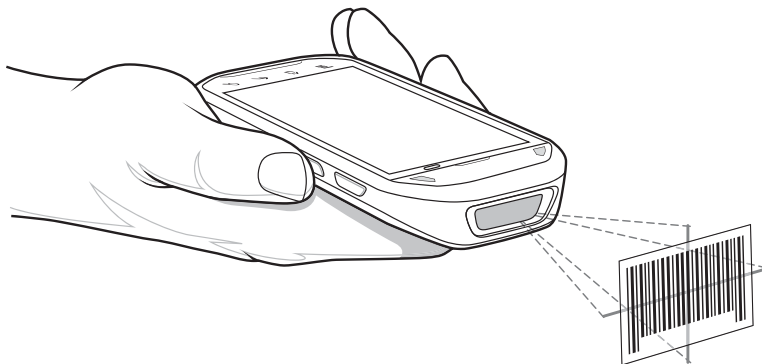
## Basic Scanning

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

### Using the Imager

To capture bar code data:

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.



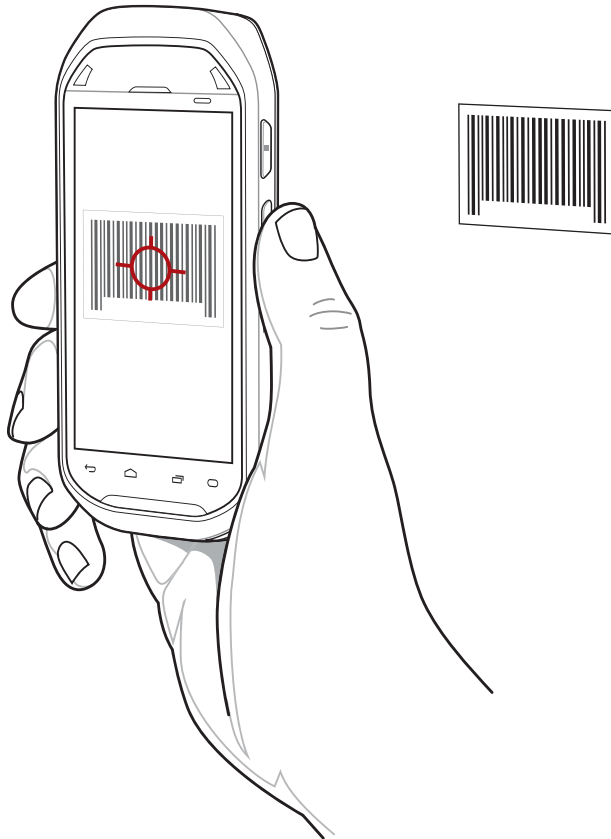
**Figure 4-1** *Data Capture*

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.

### Using the Camera

To capture bar code data:

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 4-2** *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.

---

## 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. Note: to save battery power, disable this profile when not required.
  - **DWDemo** - provides support for the DWDemo application.
- DataWedge has built-in configurations for RD Client, MSP Agent, MspUserAttributes, and RhoElements.
- DataWedge disables scanning when the default camera application is in the foreground.

## Profile0

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

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

---

## Plug-ins

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

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

### Input Plug-ins

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

- **Bar Code Scanner Input Plug-in** – The Bar Code Scanner Input Plug-in is responsible for reading data from the integrated bar code scanner and supports different types of bar code readers including laser, imager and internal camera. Raw data read from the bar code scanner can be processed or formatted using Process Plug-ins as required. **DataWedge** has built-in feedback functionality for the bar code scanner to issue user alerts. The feedback settings can be configured according to user requirement.
- **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.

### 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.

### 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.

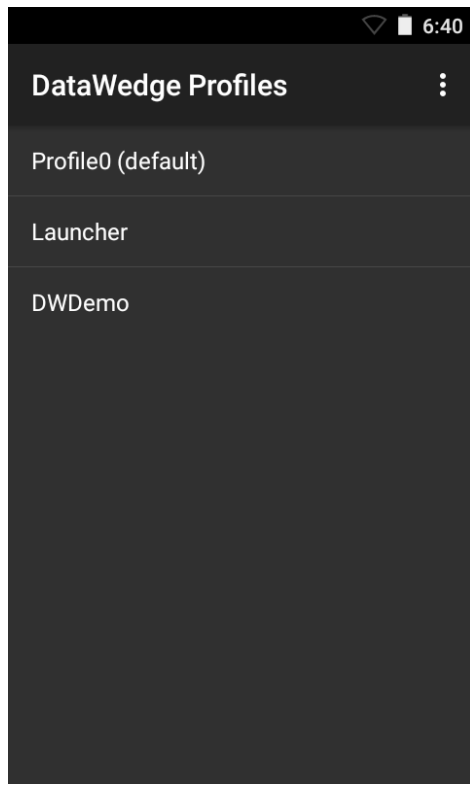
---

## 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.



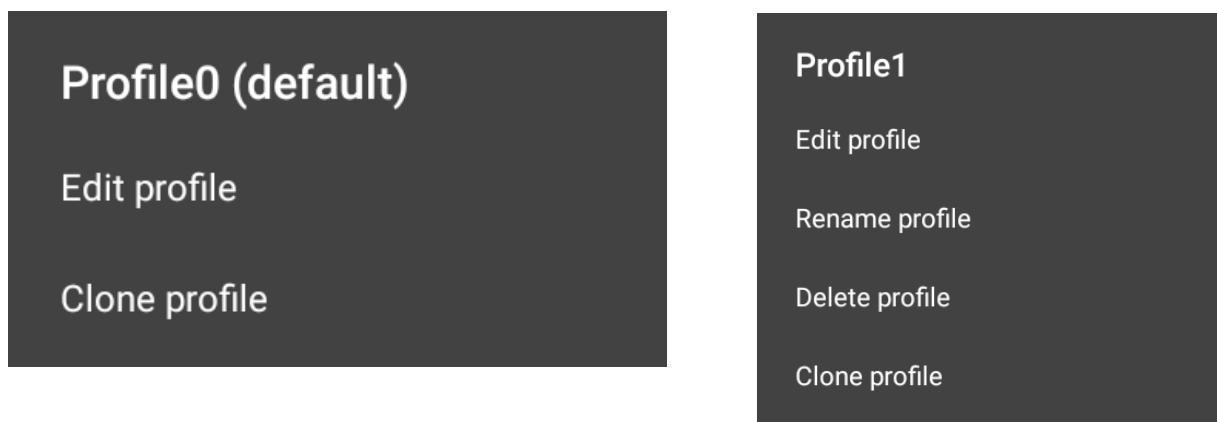
**Figure 4-3** *DataWedge Profiles Screen*

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.

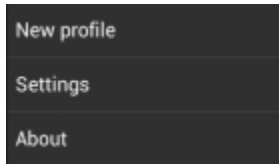


**Figure 4-4** *Profile Context Menu*

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

## Options Menu




Touch  to open the options menu.



**Figure 4-5** *DataWedge Options Menu*

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

## Disabling DataWedge




1. Touch  > .
2. Touch  > **Settings**.
3. Touch **DataWedge enabled**.

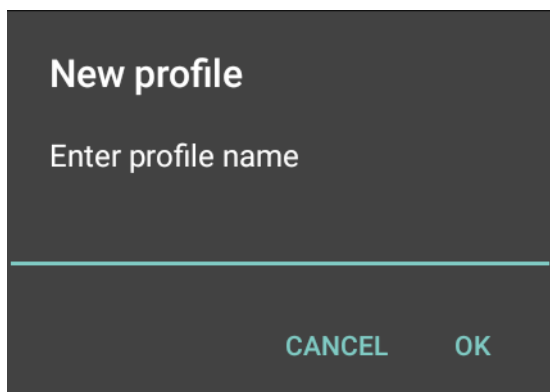
The blue check disappears from the checkbox indicating that DataWedge is disabled.

---

## Creating a New Profile

To create a profile:

1. Touch  > .
2. Touch  > **New profile**.
3. 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).

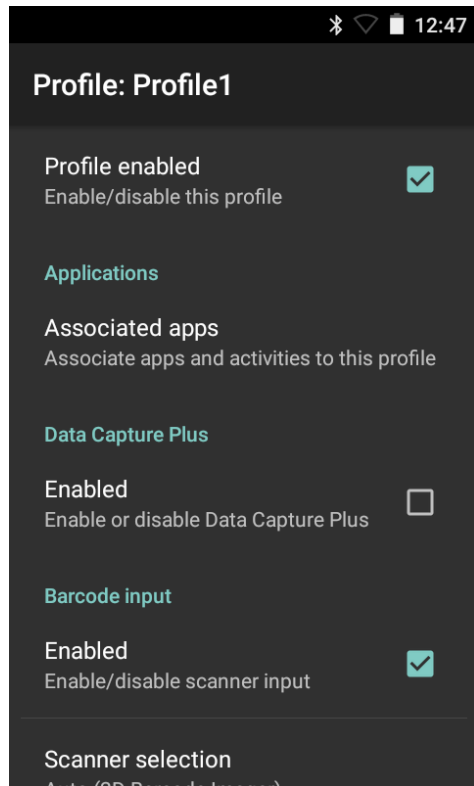


**Figure 4-6** *New Profile Name Dialog Box*

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

## Profile Configuration

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



**Figure 4-7** Profile Configuration Screen

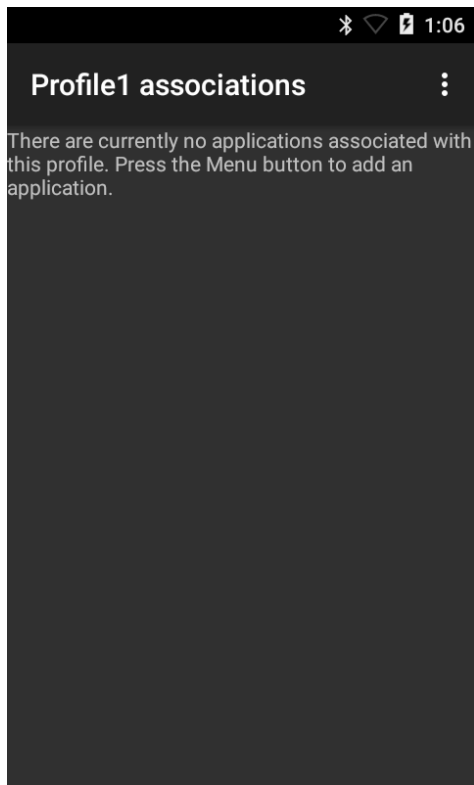
The configuration screen lists the following sections:

- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode input
- MSR input
- Keystroke output
- Intent output
- IP output.


## Associating Applications

Use Applications option to associate applications with this profile. User created profiles should be associated with one or more applications and its activities.

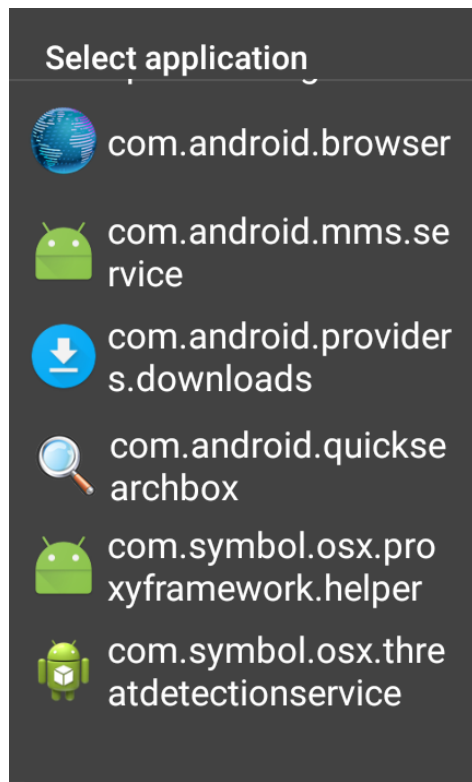
1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.



**Figure 4-8** *Associated Apps Screen*

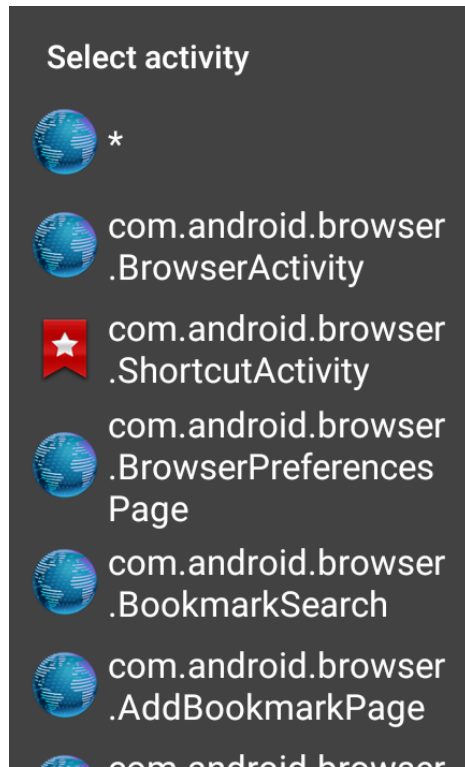
2. Touch  > **New app/activity**.
3. In the **Select application** screen, select the desired application from the list.





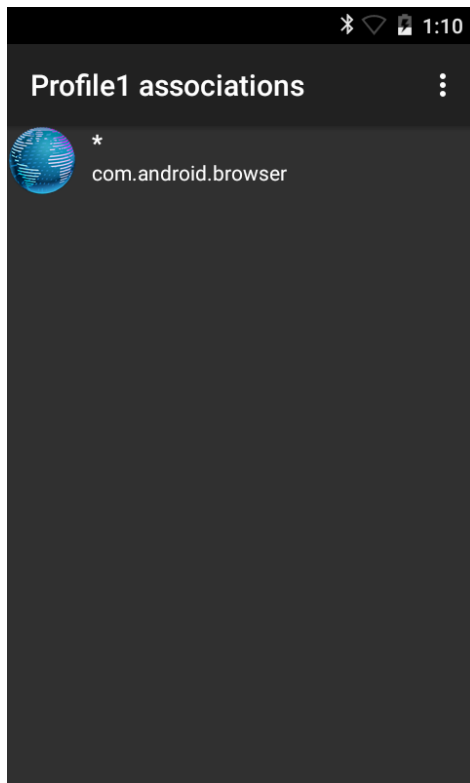
**Figure 4-9** *Select Application Menu*

4. In the **Select activity** menu, selecting the activity adds that application/activity combination to the associated application list for that profile. Selecting \* as the activity results in all activities within that application being associated to the profile. During operation, DataWedge tries to match the specific application/activity combinations with the foreground application/activity before trying to match the general application/\* combinations.




**Figure 4-10** *Select Activity Menu*

5. The selected applications/activities display for the profile.



**Figure 4-11** *Selected Application/Activity*

6. Touch .

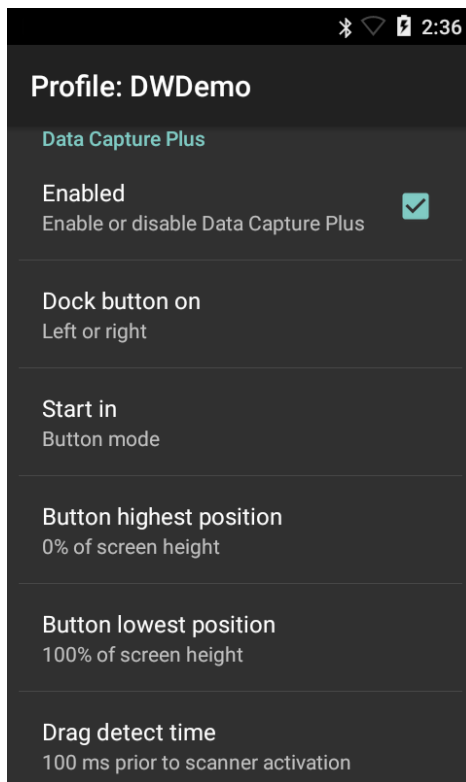
## Data Capture Plus

The Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching an area on the screen. A button or screen overlay acts like a scan button.



**Figure 4-12** *Data Capture Plus Dock Button*

The DataWedge profile configuration screen allows the user to configure how the DCP appears on the screen once the particular profile is enabled. The DCP is hidden by default. Enabling DCP option displays additional configuration parameters.



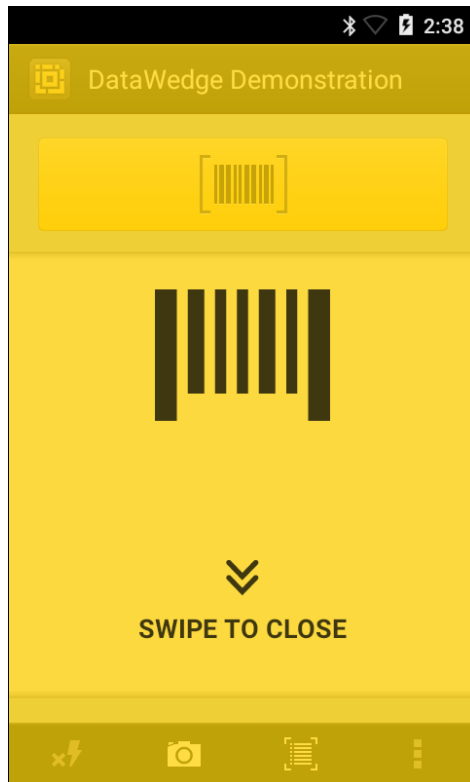
**Figure 4-13** *Data Capture Plus Settings*

- **Enable** - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
  - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
  - **Left only** - Places the button on left edge of the screen.
  - **Right only** - Places the button on the right edge of the screen.
- **Start in** - Select the initial DCP state.
  - **Fullscreen mode** - DCP covers the whole screen.
  - **Button mode** - DCP displays as a circular button on the screen and can be switched to fullscreen mode.
  - **Button only mode** - DCP displays as a circular button on the screen and cannot be switched to fullscreen mode.
- **Button highest position** - Select the top of the range the user is allowed to move the DCP, given as a percent of the screen height (default - 0).
- **Button lowest position** - Select the bottom of the range the user is allowed to move the DCP, given as a percent of the screen height (default - 100).
- **Drag detect time** - Select the time in milliseconds that the scanner waits before activating scanner. This allows the user to drag the button without initiating scanner (default - 100 ms, maximum 1000 ms).



**NOTE** The DCP does not appear if the scanner is disabled in the profile even though the **Enabled** option is set.

In Button mode, the user can place DCP in full screen mode by dragging the button over **Fullscreen mode**. The overlay covers the screen.



**Figure 4-14** *Fullscreen Mode*

Swipe down to return to button mode.

## 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 Barcode Imager.
- **Camera Scanner** - Scanning is performed with the rear-facing camera.
- **2D Barcode Imager** - Scanning is performed using the 2D Imager.
- **Bluetooth Scanner** - Scanning is performed using an optional RS507 Hands-free Bluetooth scanner.


### Decoders

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

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. The supported decoders are:

✓ **NOTE** DataWedge supports the decoders listed below but not all are validated on this device.

Touch  to return to the previous screen.

**Table 4-1** *Supported Decoders*

Symbology	Bar Code Imager	Camera	RS507
Australian Postal	Disabled	Disabled	Disabled
Aztec	Enabled	Enabled	Enabled
Canadian Postal	Disabled	Disabled	N/A
Chinese 2 of 5	Disabled	Disabled	Disabled
Codabar	Enabled	Enabled	Enabled
Code 11	Disabled	Disabled	Disabled
Code 128	Enabled	Enabled	Enabled
Code 39	Enabled	Enabled	Enabled
Code 93	Disabled	Disabled	Disabled
Composite AB	Disabled	Disabled	Disabled
Composite C	Disabled	Disabled	Disabled
Discrete 2 of 5	Disabled	Disabled	Disabled
Datamatrix	Enabled	Enabled	Enabled
Dutch Postal	Disabled	Disabled	Disabled
EAN13	Enabled	Enabled	Enabled
EAN8	Enabled	Enabled	Enabled
GS1 DataBar	Enabled	Enabled	Enabled
GS1 DataBar Expanded	Enabled	Enabled	Enabled
GS1 DataBar Limited	Disabled	Disabled	Disabled
HAN XIN	Disabled	Disabled	N/A
Interleaved 2 of 5	Disabled	Disabled	Disabled
Japanese Postal	Disabled	Disabled	Disabled
Korean 3of 5	Disabled	Disabled	Disabled
MAIL MARK	Enabled	Enabled	N/A
Matrix 2 of 5	Disabled	Disabled	Disabled

**Table 4-1** *Supported Decoders (Continued)*

Symbology	Bar Code Imager	Camera	RS507
Maxicode	Enabled	Enabled	Enabled
MicroPDF	Disabled	Disabled	Disabled
MicroQR	Disabled	Disabled	Disabled
MSI	Disabled	Disabled	Disabled
PDF417	Enabled	Enabled	Enabled
QRCode	Enabled	Enabled	Enabled
Decoder Signature	Disabled	Disabled	Disabled
TLC39	Disabled	Disabled	Disabled
Trioptic 39	Disabled	Disabled	Disabled
UK Postal	Disabled	Disabled	Disabled
UPCA	Enabled	Enabled	Enabled
UPCE0	Enabled	Enabled	Enabled
UPCE1	Disabled	Disabled	Disabled
US4state	Disabled	Disabled	Disabled
US4state FICS	Disabled	Disabled	Disabled
US Planet	Disabled	Disabled	Disabled
US Postnet	Disabled	Disabled	Disabled

## Decoder Params

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

### Codabar

- **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).
- **Length1** - Use to set decode lengths (default - 6). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-22](#) for more information.
- **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).
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

### Code 11

- **Length1** - Use to set decode lengths (default - 4). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-22](#) 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).
- **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).
- **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.

### Code128

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 bar codes. (Available on Bar Code Imager and Camera Scanner)
- **Ignore Code128 FNC4** - When enabled, and a Code 128 bar code has an embedded FNC4 character, it will be removed from the data and the following characters will not be changed. When the feature is disabled, the FNC4 character will not be transmitted but the following character will have 128 added to it. (Available on Bar Code Imager and Camera Scanner)
- **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).
- **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.
- **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-22](#) 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).
- **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

- **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 bar codes. (Available on Bar Code Imager and Camera Scanner)
- **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).
- **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),
- **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See [Decode Lengths on page 4-22](#) 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 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).
- **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).
  - **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.
- **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).

### Code93

- **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-22](#) 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).

**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).

**Discrete 2 of 5**

- **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 14). See [Decode Lengths on page 4-22](#) 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).

**GS1 DataBar Limited**

- **GS1 Limited Security Level** -
  - **GS1 Security Level 1** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” bar codes.
  - **GS1 Security Level 2** - This setting eliminates most misdecodes (default).
  - **GS1 Security Level 3** - Select this option if Security level 2 fails to eliminate misdecodes.
  - **GS1 Security Level 4** - If Security Level 3 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.

**HAN XIN** (Available on Bar Code Imager and Camera Scanner)

- **HAN XIN Inverse**
  - **Disable** - Disables decoding of HAN XIN inverse bar codes (default).
  - **Enable** - Enables decoding of HAN XIN inverse bar codes.
  - **Auto** - Decodes both HAN XIN regular and inverse bar codes.

**Interleaved 2 of 5**

- **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.
- **Length1** - Use to set decode lengths (default - 14). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 10). See [Decode Lengths on page 4-22](#) 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).
- **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).

- **I2of5 Security Level** - Options: **I2of5 Security level 0**, **I2of5 Security Level 1**, **I2of5 Security Level 2** and **I2of5 Security Level 3** (default - I2of5 Security level 1). (Available on Bar Code Imager and Camera Scanner)
- **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
- **I2of5 Reduced Quiet Zone** - Enables decoding of margin-less I2of5 bar codes. (Available on Bar Code Imager and Camera Scanner)

### Matrix 2 of 5

- **Length1** - Use to set decode lengths (default - 10). See [Decode Lengths on page 4-22](#) for more information.
- **Length2** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-22](#) 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).

### MSI

- **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.
- **Length 1** - Use to set decode lengths (default - 4). See [Decode Lengths on page 4-22](#) for more information.
- **Length 2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-22](#) 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).
- **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).

### Trioptic39

- **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). (Available on Bluetooth Scanner)

### 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).

**UPCA**

- **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.
- **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).

**UPCE0**

- **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).
- **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 None** - Transmit no preamble (default).
- **Preamble Sys Char** - Transmit System Character only.
- **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
- **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).

**UPCE1**

- **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).

- **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 None** - Transmit no preamble (default).
- **Preamble Sys Char** - Transmit System Character only.
- **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
- **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).

**US Planet**

- **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).

## 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.

- **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.
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC bar codes. (Available on Bar Code Imager and Camera Scanner)
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **Bookland Format** - If Bookland EAN is enabled, select one of the following formats for Bookland data: (Available for Bluetooth Scanner)
  - **Format ISBN-10** - The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
  - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **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.
- **Coupon Report Mode** - Traditional coupon symbols are composed of two bar code: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded bar code. The new format offers more options for purchase values (up to \$999.999) and supports complex discount offers as a second purchase requirement. An interim coupon symbol also exists that contain both types of bar codes: UPC/EAN and Databar Expanded. This format accommodates both retailers that do not recognize or use the additional information included in the new coupon symbol, as well as those who can process new coupon symbols.
  - **Old Coupon Report Mode** - Scanning an old coupon symbol reports both UPC and Code 128, scanning interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
  - **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
  - **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded. (default)
- **Ean Zero Extend** – Enable this parameter to add five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols. Disable this to transmit EAN-8 symbols as is. Default – disabled.
- **Linear Decode** - (Available for Bluetooth Scanner) - This option applies to code types containing two adjacent blocks (e.g., UPC-A, EAN-8, EAN-13). Enable this parameter to transmit a bar code only when both



the left and right blocks are successfully decoded within one laser scan. Enable this option when bar codes are in proximity to each other.

- **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).
- **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.
  - **Supplementals 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 bar code 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.

### Reader Params

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

- **1D Quiet Zone Level** - Sets the level of aggressiveness in decoding bar codes with a reduced quiet zone (the area in front of and at the end of a bar code), and applies to symbologies enabled by a Reduced Quiet Zone parameter. Because higher levels increase the decoding time and risk of misdecodes, Zebra strongly recommends enabling only the symbologies which require higher quiet zone levels, and leaving Reduced Quiet Zone disabled for all other symbologies. (Available on Bar Code Imager and Camera Scanner). Options are:
  - **0** - The scanner performs normally in terms of quiet zone.
  - **1** - The scanner performs more aggressively in terms of quiet zone (default).
  - **2** - The scanner only requires one side EB (end of bar code) for decoding.
  - **3** - The scanner decodes anything in terms of quiet zone or end of bar code.
- **Aim mode** - Turns the scanner cross-hairs on or off. (available on Bar code Imager and Bluetooth Scanner)
  - **On** - Cross-hair is on (default).
  - **Off** - Cross-hair is off.
- **Character Set Selection** -
  - ISO-88959-1 - part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
  - Shift\_JIS - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
  - UTF-8 - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
- **Time Delay to Low Power** - Sets the time the decoder remains active after decoding. After a scan session, the decoder waits this amount of time before entering Low Power Mode. Options: **1 Second** (default), **30 Seconds**, **1 Minute** or **5 Minutes**. (Available on Bluetooth Scanner)
- **Illumination Brightness** - Sets the brightness of the illumination by altering LED power. The default is 10, which is maximum LED brightness. For values from 1 to 10, LED brightness varies from lowest to highest level of brightness (Available on Bluetooth Scanner).
- **Illumination mode** - Turns imager illumination on and off. (Available on Bar Code Imager)
  - **Off** - Illumination is off.
  - **On** - Illumination is on (default).
- **Image Capture Mode** - Sets the bar code scanner to image capture mode. (Available on Bar Code Imager)
  - **None** - (default). No image capturing.
  - **Single Image Capture on Decode** - Captures an image with decoded data.
  - **Image Capture only** - Only captures an image and no bar code data is dispatched. Note that Zebra does not recommend changing this parameter when bar code scanning is used with DataWedge. No image data is processed by DataWedge.



- **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.
- **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. (Available on Bar Code Imager)
  - **Disabled** - Disables the LCD mode (default).
  - **Enabled** - Enables LCD mode.
- **Linear Security Level** - Sets the number of times a bar code is read to confirm an accurate decode. (Available on Bar Code Imager)
  - **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.
- **HW Engine Low Power Timeout** - Time (in ms) of inactivity before scanner enters low-power mode. (0 - 1000 in increments of 50; default 250). (Available on Bar Code Imager).
  - **Inverse 1D Mode** - Permits option selection for inverse 1D bar code decoding.
    - **Disabled** - Disables decoding of inverse 1D symbologies.
    - **Enabled** - Enables decoding of inverse 1D symbologies only.
    - **Auto** - Automatically detects and decodes positive and inverse 1D symbologies.
- **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.
  - **Disabled** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Enabled** - Enables Picklist mode so that only the bar code under the projected reticle can be decoded. (Available on Bluetooth Scanner).
  - **Hardware Picklist** – Enables Picklist mode so that only the bar code under the projected reticle can be decoded. (Available on Bar Code Imager).
  - **Software Picklist** – Enables Picklist mode so that only the bar code in the center of the image is decoded. (Available on Bar Code Imager and Camera Scanner)
- **Poor Quality Decode Effort** - Permits selection of enhancement modes for decoding bar codes of poor or degraded quality. (Available on Bar Code Imager and Camera Scanner)
  - **Effort Level 0** - (default). Decoding performance on regular 1D and 2D bar codes is not affected.
  - **Effort Level 1** - The scanner performance on regular 2D bar codes is impacted while decoding performance on Tesco Thailand bar code and Suppository bar code is improved.
  - **Effort Level 2** - Same as Level 1.
  - **Effort Level 3** - Same as Level 1.

Note the same performance from Effort Level 1 to Effort Level 3.
- **Viewfinder Mode** - Configures the Viewfinder modes supported for camera scanning. (Available on Camera Scanner).
  - **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).

- **Viewfinder X Offset** - (Available on Camera Scanner). Offset the viewfinder along the X axis from 0 (default) to 100.
- **Viewfinder Y Offset** - (Available on Camera Scanner). Offset the viewfinder along the Y axis from 0 (default) to 100.
- **Viewfinder Size** - (Available on Camera Scanner). Set the size of the viewfinder from 0 to 100 (default).
- **Aim Timer** - Sets the maximum amount of time that aiming remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the aim to stay on indefinitely (default - 500).
- **Aim Type** - Set the aiming usage.
  - **Trigger** - A trigger event activates decode processing, which continues until the trigger event ends or a valid decode occurs (default).
  - **Timed Hold (Available on Bar Code Imager)** - A trigger pull and hold activates the laser for aiming, which continues until the trigger is released, a valid decode, or the decode session time-out is expired.
  - **Timed Release (Available on Bar Code Imager)** - A trigger pull activates the laser for aiming, which continues until a valid decode or the remaining decode session time has expired.
  - **Press and Release (Available on Bar Code Imager)** - A trigger pull and release activates the laser for aiming, which continues until a trigger is pressed again, a valid decode, or the decode session time-out is expired.
  - **Continuous Read** - When the imager detects an object in its field of view, it triggers an attempt to decode.
- **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).
- **Different Symbol Timeout** - Controls the time the scanner is inactive between decoding different symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.

Use to prevent the device from decoding another bar code within a specific interval (applicable only when aim type is set to **Continuous Read**). The user may want to prevent decoding too quickly and set an interval that the user can aim before scanning the next bar code. A value of 0 indicates no interval is required between two successful reads.
- **Same Symbol Timeout** - Controls the time the scanner is inactive between decoding same symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.

Use to prevent the device from decoding the same bar code within a specific time interval (applicable only when Aim Type is set to **Continuous Read**). The user can perform rapid scanning and prevents the user from decoding the same bar code twice. A value of 0 indicates no interval is required between two successive reads.

### 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.
  - **Code ID Type AIM** - Insert AIM Character prefix.
  - **Code ID Type Symbol** - Insert Symbol character prefix.
  - **Code ID Type None (Auto)** - No prefix. (default).
  - **Code ID Type Symbol (Auto)** - Insert Symbol character prefix.
- **Engine Decode LED** - Use to turn on scanner red LED when the scan beam is emitting either by scanner trigger or using soft scan button (Available on Bluetooth Scanner).

- **BT Disconnect On Exit** - Bluetooth connection is disconnected when data capture application is closed. (Available on Bluetooth Scanner).
- **Connection Idle Time** - Set connection idle time. The Bluetooth connection disconnects after being idle for set time (Available on Bluetooth Scanner).
- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).
- **Display BT Address Barcode** - Enable or disable displaying Bluetooth Address bar code if there is no Bluetooth scanner being paired when application tries to enable the Bluetooth scanner (Available on Bluetooth Scanner).
- **Establish Connection Time** - The timeout which the MC40 will try to enable or reconnect to the Bluetooth scanner when the Bluetooth scanner is not in the vicinity or not paired (Available on Bluetooth Scanner).
- **Audio Feedback Mode** - Select good decode audio indication. (Available on Bluetooth Scanner)
  - **Local Audio Feedback** - Good decode audio indication on MC40 only.
  - **Remote Audio Feedback** - Good decode audio indication on scanner only.
  - **Both** - Good decode audio indication on MC40 and scanner.
  - **Disable** - No good decode audio indication on either MC40 or scanner (default).
- **LED Feedback Mode** - Select good decode LED indication. (Available on Bluetooth Scanner)
  - **Local LED Feedback** - Good decode LED indication on MC40 only.
  - **Remote LED Feedback** - Good decode LED indication on scanner only.
  - **Both** - Good decode LED indication on MC40 and scanner (default).
  - **Disable** - No good decode LED indication on either MC40 or scanner.
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).
- **Decode Feedback LED Timer** - Set the amount of time (in milliseconds) that the green Data Capture LED stays lit after a good decode. (default - 75 msec.)
- **Beep Volume Channel** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.



**NOTE** Not all ringtones are fully supported as decode tones and those of longer length may be truncated when used as a decode tone. The recommendation is to test the selected tone for operation before deployment to a customer site.

- **Media** - Set the good decode beep to the media sound.
- **Ringer** - Set the good decode beep to the ringer sound.
- **Notifications** - Set the good decode beep to the notification sound (default).
- **Alarms** - Set the good decode beep to the alarm sound.

### Keep enabled on suspend

When this setting is enabled, suspending the device does not disable the scanner. Therefore, pressing the trigger on the RS507 will resume the device from suspend mode. (Available only on Bluetooth Scanner).

### MSR Input

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

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

## Keystroke Output

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

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code 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.
- **Multi byte character delay** - Set the inter-character delay for multi-byte characters (in milliseconds). (Available on Bar Code Imager and Camera Scanner)
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 4-35](#) for more information.
- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

## Intent Output

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).
- **Intent delivery** - Select the method by which the intent is delivered:
  - Send via StartActivity
  - Send via startService (default)
  - Broadcast intent
- **Receiver foreground flag** - Set flag in broadcast event.
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 4-35](#) for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

## Intent Overview

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

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

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

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

```
android.intent.category.DEFAULT
```

and the Intent category would be:

```
android.intent.category.MAIN.
```

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

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

- String LABEL\_TYPE\_TAG = "com.symbol.emdk.datawedge.label\_type";
  - String contains the label type of the bar code.
- String DATA\_STRING\_TAG = "com.symbol.emdk.datawedge.data\_string";
  - String contains the output data as a String. In the case of concatenated bar codes, the decode data is concatenated and sent out as a single string.
- String DECODE\_DATA\_TAG = "com.symbol.emdk.datawedge.decode\_data";
  - Decode data is returned as a list of byte arrays. In most cases there will be one byte array per decode. For bar code symbologies that support concatenation e.g. Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per bar code). Clients can get data in each byte array by passing an index.

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

- String MSR\_DATA\_TAG = "com.symbol.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.symbol.emdk.datawedge.msr\_track1";
  - MSR track 1 data is returned as a byte array.
- String MSR\_TRACK2\_TAG = "com.symbol.emdk.datawedge.msr\_track2";
  - MSR track 2 data is returned as a byte array.
- String MSR\_TRACK3\_TAG = "com.symbol.emdk.datawedge.msr\_track3";
  - MSR track 3 data is returned as a byte array.
- String MSR\_TRACK1\_STATUS\_TAG = "com.symbol.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.symbol.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.symbol.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.

## IP Output



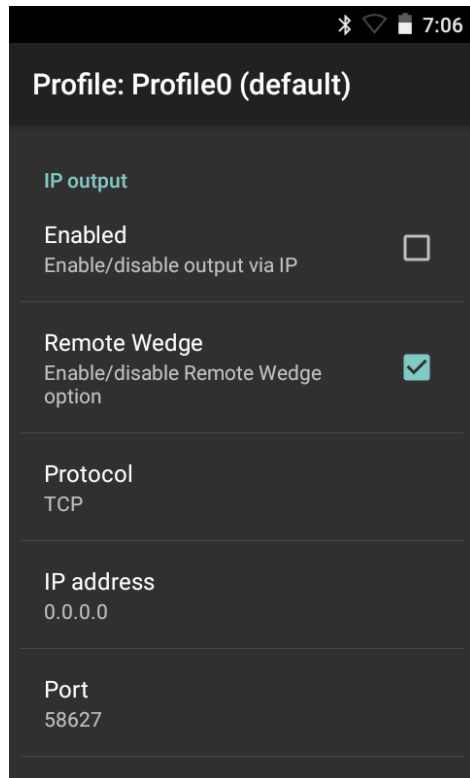
**NOTE** IPWedge application is required on a host computer. Download the IPWedge application from the Support Central web site: <http://www.zebra.com/support>.

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.
- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 4-35](#) 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**.



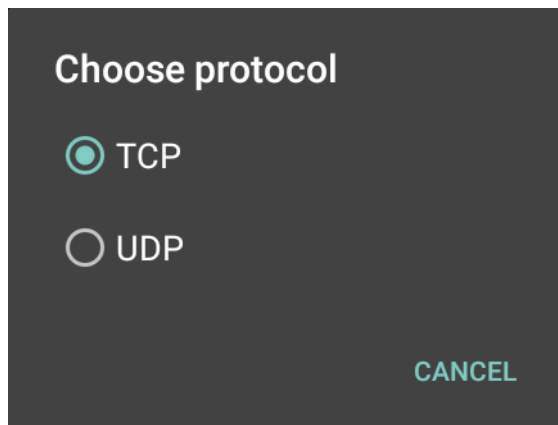
**Figure 4-15** *IP Output Screen*

### Using IP Output with IPWedge

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

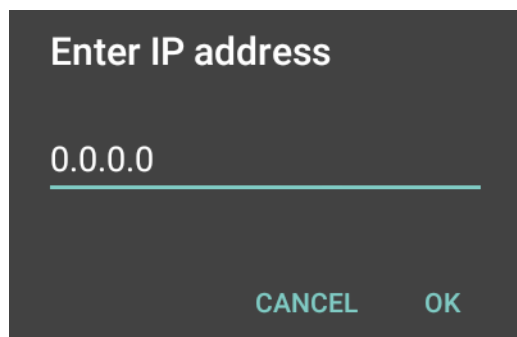
1. In **IP Output**, touch **Enabled**.  
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is enabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).





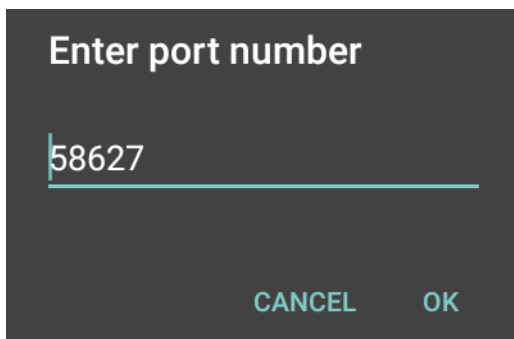
**Figure 4-16** *Protocol Selection*

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



**Figure 4-17** *IP Address Entry*

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



**Figure 4-18** *Port Number Entry*

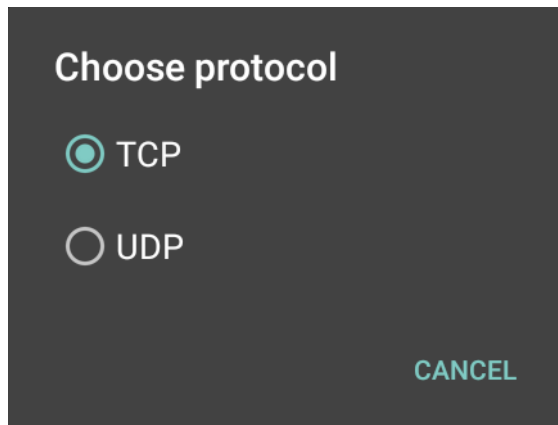
9. Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

### Using IP Output without IPWedge

IP Output Plug-in can be used to send captured data from DataWedge to a remote device or host computer without using IPWedge. At the data receiving end, the host computer or mobile device should have an application, that

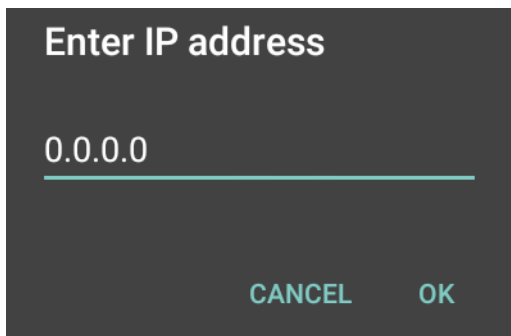
listens to TCP or UDP data coming from a configured port and IP address in the IP Output plug-in. To enable IP Output to send captured data to a remote computer:

1. In **IP Output**, touch **Enabled**.  
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is disabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).



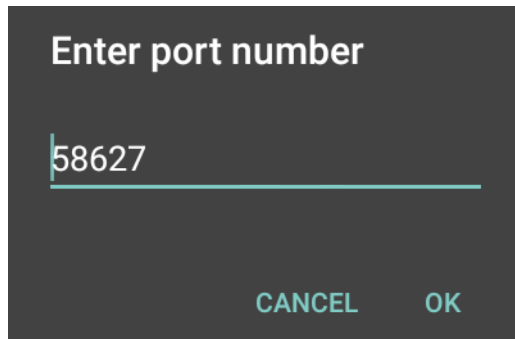
**Figure 4-19** *Protocol Selection*

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



**Figure 4-20** *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 4-21** *Port Number Entry*

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



## Generating Advanced Data Formatting Rules

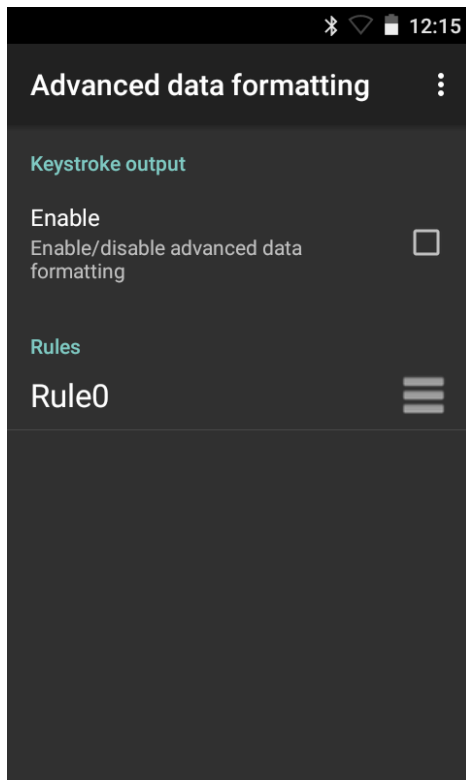
The ADF plug-in applies rules (actions to be performed based on defined criteria) to the data received via an input plug-in before sending it to the output plug-in.

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

## Configuring ADF Plug-in

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

1. Touch  >  **DataWedge**.
2. Touch a DataWedge profile.
3. In **Keystroke Output**, touch **Advanced data formatting**.




**Figure 4-22** *Advanced Data Formatting Screen*

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

### Creating a Rule

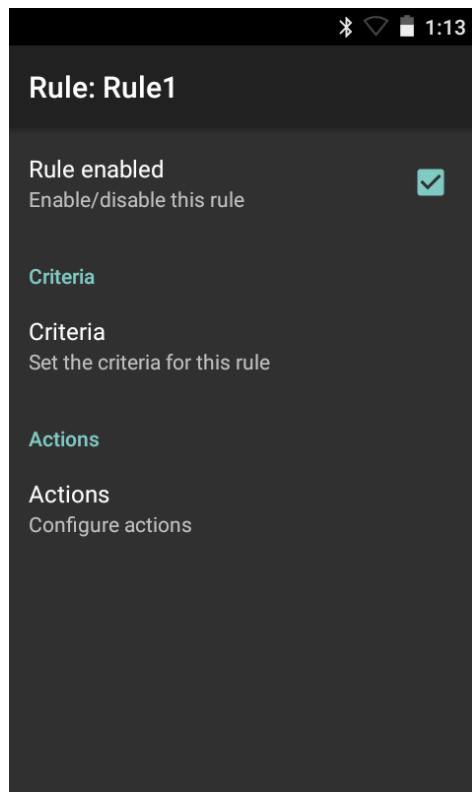


**NOTE** By default, Rule0, is the only rule in the Rules list.

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

### Defining a Rule

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

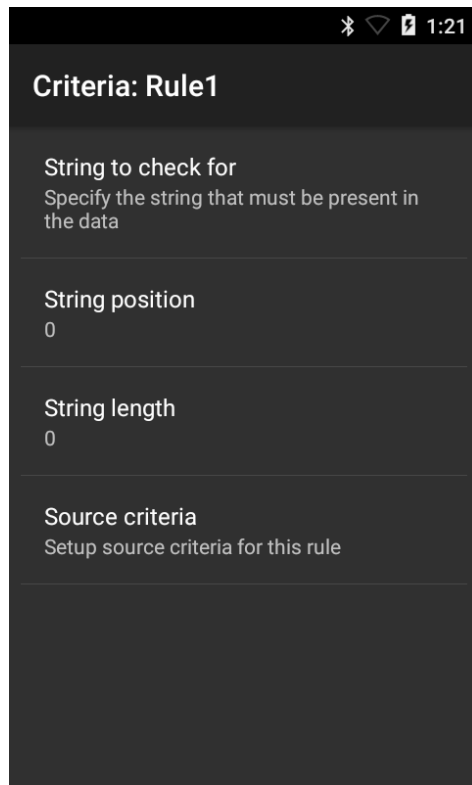


**Figure 4-23** *Rule List Screen*

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

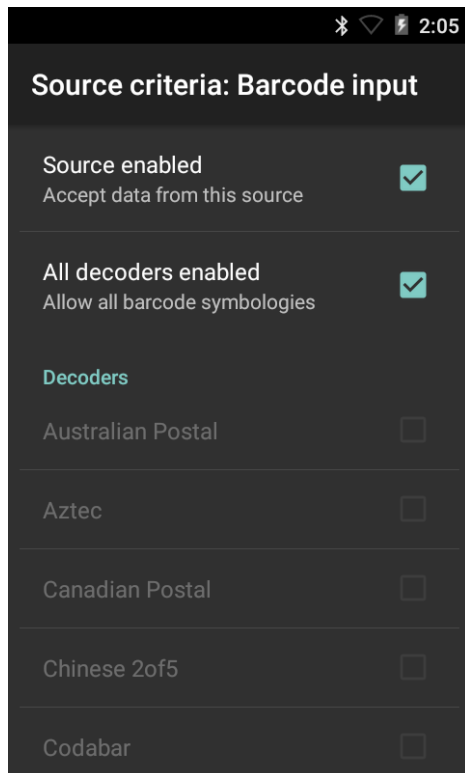
### Defining Criteria

1. Touch **Criteria**.





**Figure 4-24** 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 **OK**.
5. 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).
6. Touch the **+** or **-** to change the value.
7. Touch **OK**.
8. 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.
9. Touch the **+** or **-** to change the value.
10. Touch **OK**.
11. 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.
12. Touch **Barcode input** or **MSR input**. Options vary depending upon the device configuration.
13. Touch the **Source enabled** checkbox to accept data from this source.






**Figure 4-25** Barcode Input Screen

14. 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.
15. Touch  until the **Rule** screen appears.
16. If required, repeat steps to create another rule.
17. Touch  until the **Rule** screen appears.

## Defining an Action

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

1. Touch  > **New action**.
2. In the **New action** menu, select an action to add to the **Actions** list. See [Table 4-2 on page 4-40](#) for a list of supported ADF actions.
3. Some Actions require additional information. Touch the Action to display additional information fields.
4. Repeat steps to create more actions.
5. Touch .
6. Touch .

## Deleting a Rule

1. Touch and hold on a rule until the context menu appears.
2. Touch **Delete rule** to delete the rule from the **Rules** list.



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

### Order Rules List



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

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

**Table 4-2** 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.



**Table 4-2** ADF Supported Actions (Continued)

Type	Actions	Description
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 <b>Crunch spaces</b> action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last <b>Remove all spaces</b> 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 <b>Remove leading zeros</b> 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 <b>Pad with zeros</b> 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 <b>Pad with spaces</b> 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 <b>Replace string</b> actions.
Data Sending	Send next	Sends the specified number of characters from the current cursor position. Enter the number of characters to send.
	Send remaining	Sends all data that remains from the current cursor position.
	Send up to	Sends all data up to a specified string. Enter the string.
	Send pause	Pauses the specified number of milliseconds before continuing the next action. Enter the amount of time in milliseconds.
	Send string	Sends a specified string. Enter the string to send.
	Send char	Sends a specified ASCII/ Unicode character. Enter a character value. The maximum Unicode character value can be entered is U-10FFFF (= 1114111 in decimal).

**Deleting an Action**

1. Touch and hold the action name.
2. Select **Delete action** from the context menu.

**ADF Example**

The following illustrates an example of creating Advanced Data Formatting:







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




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

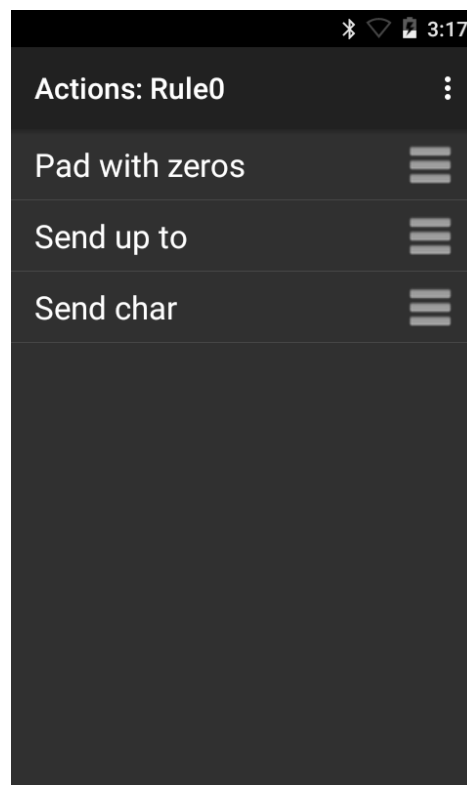
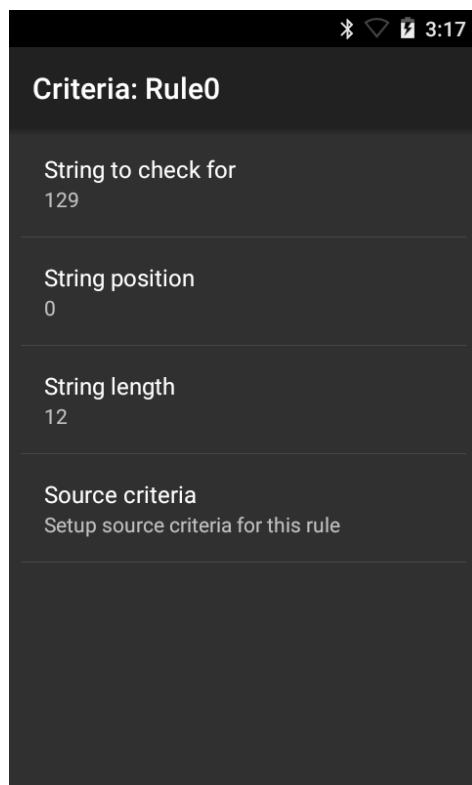
Modify the data as follows:

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

To create an ADF rule for the above example:

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

29. Select **Send up to**.
30. Touch **Send up to** rule.
31. Touch **String**.
32. In the **Enter a string** text box, enter x.
33. Touch **OK**.
34. Touch .
35. Touch  > **New action**.
36. Select **Send char**.
37. Touch **Send char** rule.
38. Touch **Character code**.
39. In the **Enter character code** text box, enter 32.
40. Touch **OK**.
41. Touch .



**Figure 4-26** ADF Sample Screens

42. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
43. Aim the exit window at the bar code.



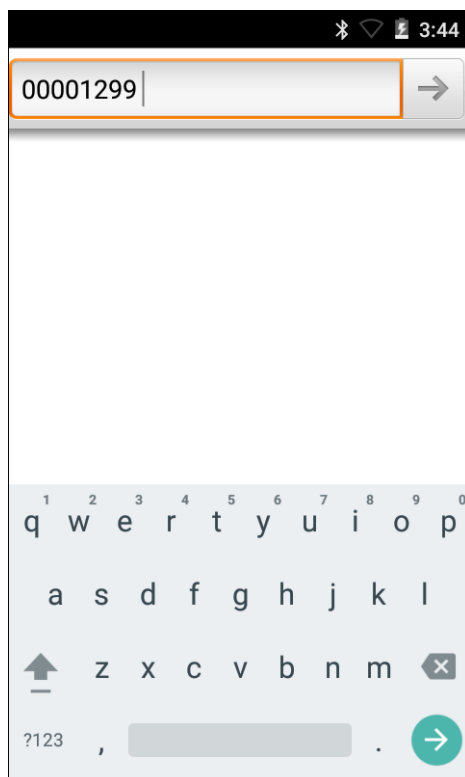
**Figure 4-27** Sample Bar Code

44. 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.

45. The LED lights green and a beep sounds, by default, to indicate the bar code was decoded successfully. Haptic Feedback is not enabled by default, so vibration will not work by default. The formatted data 000129X<space>appears in the text field.

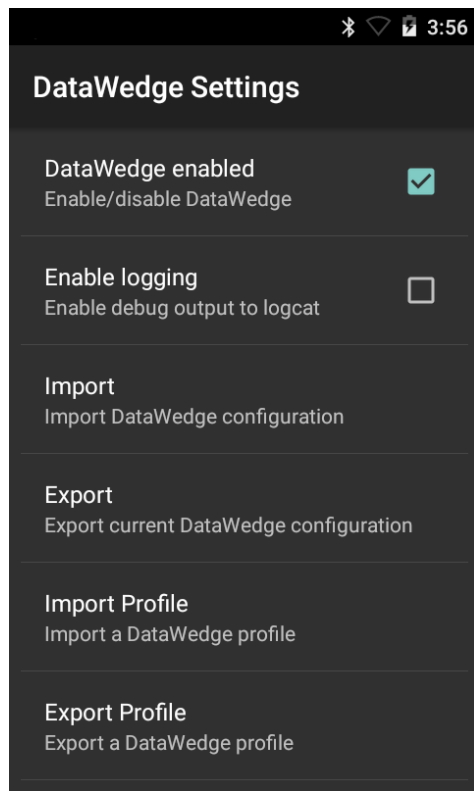
Scanning a Code 39 bar code of 1299X15598 does not transmit data (rule is ignored) because the bar code data did not meet the length criteria.



**Figure 4-28** Formatted Data

## DataWedge Settings




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






**Figure 4-29** *DataWedge Settings Window*

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

## Importing a Configuration File




1. Copy the configuration file to a location on the device (Internal Storage or microSD card `/Android/data/com.symbol.datawedge/files` folder).
2. Touch  >  **DataWedge**.
3. Touch  > **Settings**.
4. Touch **Import**.
5. In the **Import datawedge.db from** dialog box, select the location to import the configuration file from. Use `.` and `..` and folder entries to browse to the configuration file. The configuration file (`datawedge.db`) is imported and replaces the current configuration.

## Exporting a Configuration File




1. Touch  >  **DataWedge**.
2. Touch  > **Settings**.
3. Touch **Export**.
4. In the **Export to** dialog box, select the location to store the file.
5. Touch **Export**. The configuration file (*datawedge.db*) is saved to the selected location.

## 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.




1. Copy the profile file to the root of the On Device Storage.
2. Touch  >  **DataWedge**.
3. Touch  > **Settings**.
4. Touch **Import Profile**.
5. In the **Import profile from** dialog box, select the location to import the profile file from. Use .,and .., and folder entries to locate the profile file. The profile file (*dwprofile\_x.db*, where x = the name of the profile) is imported and appears in the profile list.

## Exporting a Profile

1. Touch  >  **DataWedge**.
2. Touch  > **Change** to change the location to save the file.
3. Select **Internal Storage** or **External Storage**.
4. Touch **OK**.
5. Select a profile from the profile list.
6. Touch **Export**. The profile file (*dwprofile\_x.db*, where x = name of the profile) is saved to the selected location.

## Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Touch  >  **DataWedge**.
2. Touch  > **Settings**.
3. Touch **Restore**.
4. Touch **Yes**.

---

## Configuration and Profile File Management

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

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

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 be copied to the On—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.



**NOTE** A Factory Reset deletes all files in the Enterprise folder.

### Auto Import

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

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



**NOTE** A Factory Reset deletes all files in the Enterprise folder.

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

---

## Programming Notes

The following paragraphs provide specific programming information when using DataWedge.




## 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.
- DataWedge has an intent to enable or disable the bar code scanner if the user needs to control this programmatically. More details can be found at: <http://techdocs.zebra.com/datawedge/5-0/guide/api/>.

## Disable DataWedge on MC40 and Mass Deploy

To disable DataWedge and deploy onto multiple MC40 devices:

1. Touch  >  **DataWedge**.
2. Touch  > **Settings**.
3. Unselect the **DataWedge enabled** check box.
4. Export the DataWedge configuration. See [Exporting a Configuration File on page 4-46](#) for instructions. See [Configuration and Profile File Management on page 4-47](#) for instructions for using the auto import feature.

## Soft Scan Feature

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

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

**action:** "com.symbol.emdk.datawedge.api.ACTION\_SOFTSCANTRIGGER"

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

**name:** "com.symbol.emdk.datawedge.api.EXTRA\_PARAMETER"

**value:** "START\_SCANNING" or "STOP\_SCANNING" or "TOGGLE\_SCANNING"

### Sample

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



# CHAPTER 5 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.

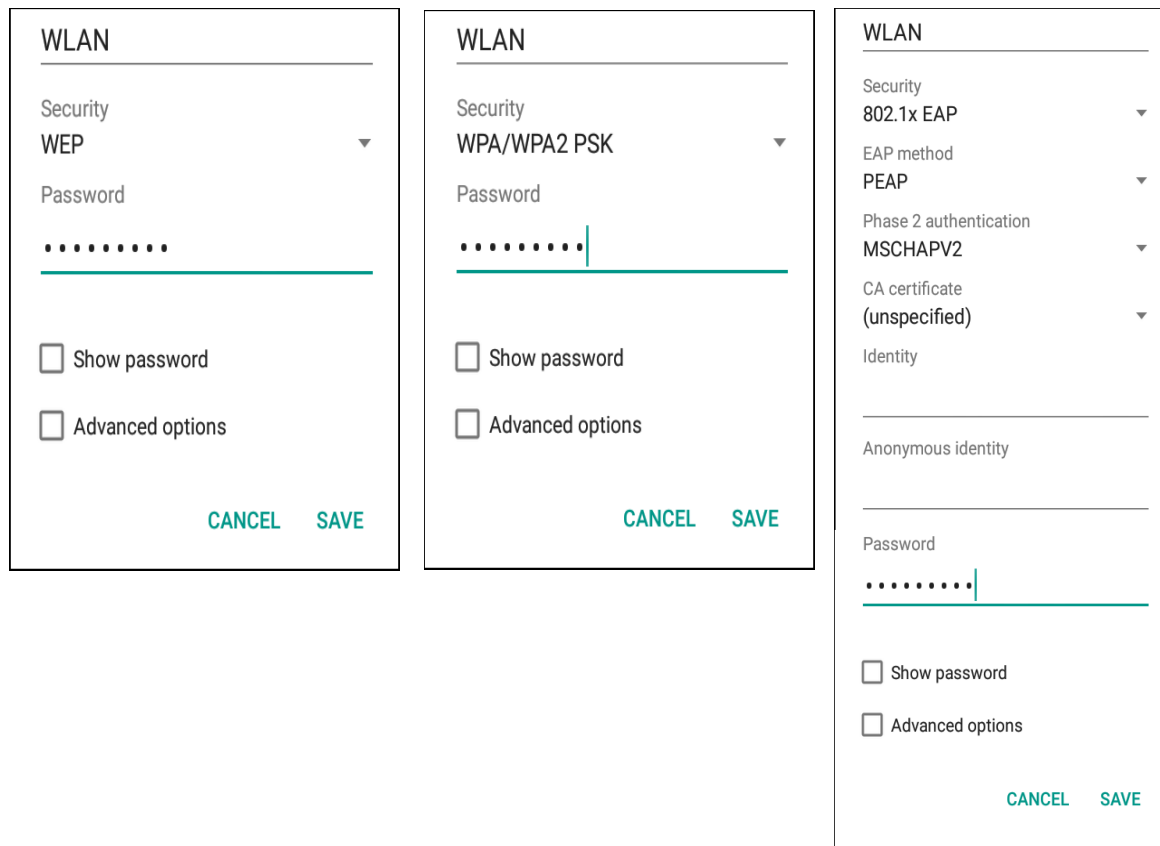
---

## 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 Configuring for a Proxy Server for setting connection to a proxy server and see Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

1. Touch  >  **Wi-Fi**.
2. 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 a lock .
3. Scroll through the list and touch the desired WLAN network.



**Figure 5-1** WLAN Network Security Dialog Boxes






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

4. For open networks, touch **Connect** or for secure networks enter the required password or other credentials then touch **Connect**. See the system administrator for more information.
5. 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 [Configuring Ethernet Static IP Address on page 5-5](#).
6. When the device connects to the network, the network name appears at the top of the list and **Connected** appears below the network name.

## 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.

1. Touch  >  **Wi-Fi**.
2. Slide the Wi-Fi switch to the **On** position.
3. Touch  > **Add network**.

4. In the **Network SSID** text box, enter the name of the Wi-Fi network.
  5. In the **Security** drop-down list, select the type of security. Options:
    - **None**
    - **WEP**
    - **WPA/WPA2 PSK**
    - **802.1x EAP**.
  6. If the network security is **None**, touch **Save**.
  7. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password and then touch **Save**.
  8. If the network security is **802.1x EAP**:
    - Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **TTLS**, **LEAP** or **FAST**.
    - 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.
- ✓ **NOTE** By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See [Configuring for a Proxy Server on page 5-3](#) for setting connection to a proxy server and see [Configuring Ethernet Static IP Address on page 5-5](#) for setting the device to use a static IP address.
9. Touch **Save**. To connect to the saved network, touch and hold on the saved network and select **Connect to network**.
  10. Touch .

---

## 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.




## Ethernet Settings

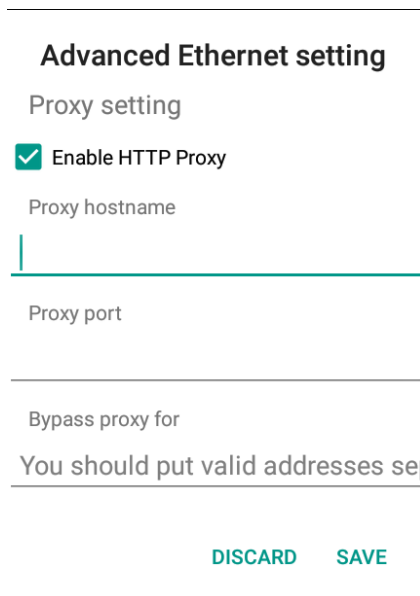
The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

### Configuring Ethernet Proxy Settings

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Advanced**.



**Advanced Ethernet setting**

Proxy setting

☒ Enable HTTP Proxy

Proxy hostname

Proxy port

Bypass proxy for

You should put valid addresses separated by |


DISCARD SAVE

**Figure 5-2** Ethernet Proxy Settings

5. Touch **Enable HTTP Proxy**.
6. In the **Proxy hostname** field, enter the proxy server address.
7. In the **Proxy port** field, enter the proxy server port number.






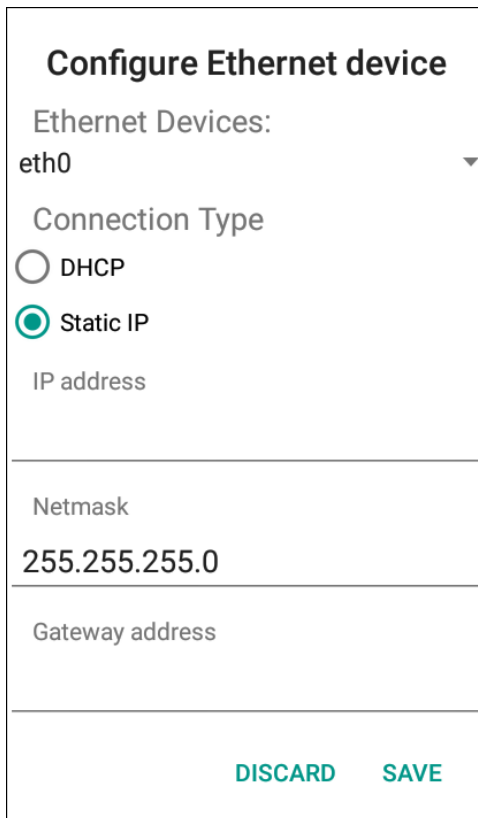
**NOTE** When entering proxy addresses in the **Bypass proxy for** field, do not use spaces or carriage returns between addresses.

8. 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.
9. Touch **Save**.
10. Touch .

## Configuring Ethernet Static IP Address

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection. By default, the device is configured to use Dynamic Host Configuration Protocol (DHCP) to assign an Internet Protocol (IP) address when connecting to an Ethernet network. To configure the device to connect to a network using a static IP address:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Config**.



**Configure Ethernet device**

Ethernet Devices:  
eth0 ▼

Connection Type

☐ DHCP

☒ **Static IP**

IP address

---

Netmask

255.255.255.0


---

Gateway address

---

**DISCARD** **SAVE**

**Figure 5-3** *Configure Ethernet Device Settings*


5. Under **Connection Type**, touch the **Static IP** radio button.  
**DHCP** is the default **Connection Type**.
6. In the **IP address** field, enter the proxy server address.
7. If required, in the **Netmask** text box, enter the network mask address.
8. If required, in the **Gateway address** text box, enter a gateway address for the device.
9. If required, in the **DNS 1 address** text box, enter a Domain Name System (DNS) address.
10. If required, in the **DNS 2 address** text box, enter a DNS address.
11. Touch **Save**.
12. Touch .

---

## Advanced Wi-Fi Settings



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

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


- **Network notification** - When enabled, notifies the user when an open network is available.
- **Scanning always available** - Let Google's location service and other apps scan for networks, even when Wi-Fi is off.
- **Keep Wi-Fi on during sleep** - Opens a menu to set whether and when the Wi-Fi radio turns off.
  - **Always** - 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** - The radio turns off when the device enters suspend mode (default).
- **Wi-Fi frequency band** - Use to select the frequency band. Options: **Automatic** (default), **5 GHz only** or **2.4 GHz only**.
- **Install Certificates** – Touch to install certificates.
- **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **IP address** - Displays the Internet Protocol (IP) address of the device when connecting to Wi-Fi networks.

---

## Additional Wi-Fi Settings



**NOTE** Additional Wi-Fi settings are for the device not for a specific wireless network.

Use the **Additional Settings** option to configure additional Wi-Fi settings. Touch  > **Additional Settings** to view the additional settings.

- **Regulatory**
  - **Country selection** - Allows user to select the country of operation. If **Auto** is selected, the MC40 will acquire the country information from the Access Points and displays the acquired country name.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Use to select the frequency band. Options: **Automatic** (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**.
- **Logging**
  - **Advanced Logging** - Provides support for continuous capture of system logs to a file to help in debugging and resolution of Wi-Fi related issues. Disabled by default. In the **Advanced Logging** dialog

box, select **Enable logging**. If desired, change the log directory location. When enabled, the following logs are captured:

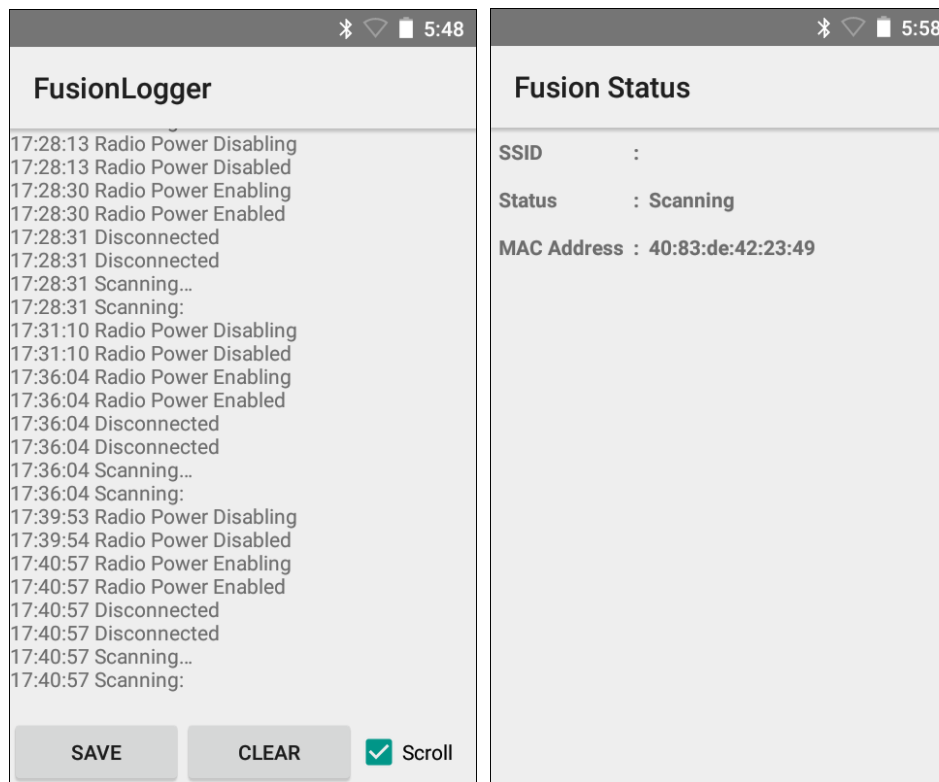


**NOTE** All log files are saved in /storage/sdcard/fusionlogs on the MC40.

Fusion will ask the user whether to clear out previous logs before starting logging.

tcpdump capture file and fusion-sysinfo.log will only be generated when advanced logging is stopped.

- Android logcat output with time stamps and the kernel messages in the file: *fusion-wlan.log*.
- tcpdump intermediate capture of packets between network stack and driver in the file: *fusion-pktcap.pcap*
- Fusion versions, Wi-Fi state machine logs and other framework information in the file: *fusion-sysinfo.log*.
- **Wireless logs** - Use to capture Wi-Fi log files.
- **Fusion Logger** - Touch to open the **Fusion Logger** application. This application maintains a history of high level WLAN events which helps to understand the status of connectivity.
- **Fusion Status** - Touch to display live status of WLAN state. Also provides information of device and connected profile.








**Figure 5-4** Fusion Logger Screen and Fusion Logger Status Screen

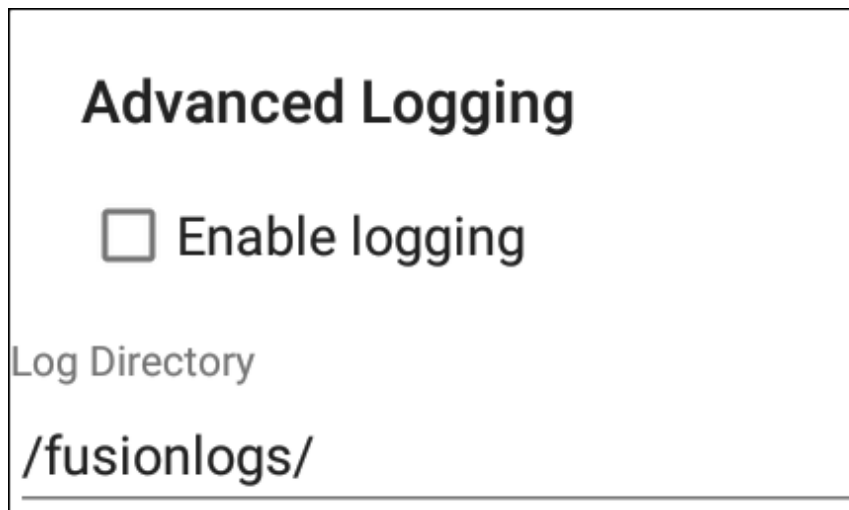
- **About**
- **Version** - Displays the current Fusion information.

## Enable Logging



**NOTE** Make sure that no other ADB command or any application that captures **KMSG** is running.

1. Touch  >  **Developer options**.
2. Slide the **USB debugging** switch to the **ON** position.
3. Touch .
4. Touch  **Wi-Fi**.
5. Touch  > **Additional settings** > **Advanced logging**.



**Figure 5-5** *Advanced Logging Dialog Box*

6. Touch **Enable Logging**.
7. After logging is complete:, unckeck **Advanced Logging**.
  - Touch **Enable Logging**  
The MC40 saves the log file `fusion-wlan.log` to On Device Storage `fusionlogs` directory.
8. Connect MC40 to host computer.
9. Copy the log file from the location listed above.
10. Disconnect the MC40 from the host computer.



## Additional Wi-Fi Advanced Features

Some additional Wi-Fi settings cannot be accessed from the User Interface. They can be configured by using Wi-Fi (CSP). Refer to EMDK documentation for the details on the Wi-Fi settings configuration using the Wi-Fi CSP.

- **Auto Time Config** - Using this feature, the device can sync up its time with Zebra WLAN infrastructure. This feature works only when the device is connected to Zebra WLAN infrastructure and the feature is enabled on the WLAN infrastructure side. Default: disabled.
- **PMKID Caching** - Allows the device to skip 802.1x authentication during roaming if it had previously connected to that AP with a full 802.1x authentication. Default: disabled. Note: disable OKC when enabling PMKID Caching.
- **Opportunistic Key Caching** - Use this feature to skip 802.1x authentication during roaming. The device will go for full 802.1x authentication for the first time it connects to the network. For subsequent roaming, the device skips 802.1x authentication. Default: enabled.
- **Cisco Centralized Key Management** - Allows the device to skip 802.1x and key-handshake phases during roaming. This feature is available only when the device is connected to a Cisco infrastructure that supports Cisco Centralized Key Management (CCKM). Default: enabled.
- **Fast Transition** - Fast Transition (FT) is the fast roaming standard, 802.11r. With this feature, the device can skip 802.1x and key-handshake phases during roam. Default: enabled.
- **Fast Transition Resource Information Container** - Allows the device to request TSPEC as part of re-association frame exchange. This helps to avoid sending a separate resource request after roaming is completed. Default: disabled.
- **Power Save** - The device can be configured to work in different power save modes:
  - **Active** - Keeps the WLAN radio always in active mode (i.e. power save mode disabled).
  - **Power save using WMM-PS** - This is the default power save mode. Device uses WMM-PS power save method if the AP is configured to use this. If the AP is not supporting WMM-PS, the device will use PS-Poll power save method.
  - **Power save using PS-Poll** - In this method, the device will use PS-Poll frames to retrieve buffered frames from the AP.
  - **Null Data Power Save** - In Null Data Power Save (NDP), the device will stay awake for 100 ms after the last frame is sent or received. The device will send a Null Data packet with power management bit cleared to retrieve buffered frames from the AP.
- **FIPS** - The device supports FIPS 140-2 Level 1. In this mode, the device will not support TKIP and WEP encryption modes. When Wi-Fi is enabled, the stack will run predefined tests to make sure that the encryption engine is working correctly and the firmware and firmware loader modules are correct.
- **802.11k** - Using 802.11k, the device can discover neighbor APs and adds support for different types of radio resource measurements. Default: enabled.
- **Band Preference** - The device can be configured to prefer one band over another. By default, device prefers 5 GHz frequency band over 2.4 GHz.
- **Subnet Roaming** - When the device roams between different sub networks, if it detects that it is roaming to a different subnet, the device will request a fresh IP address. Default: disabled.

---

## Zebra Mobility Extensions




Zebra Mobility Extensions make use of 802.11 specifications and Zebra proprietary extensions to achieve the highest level of performance, efficiency and reliability. The MC40 adds support for the following Zebra Mobility Extensions.

- **Coverage Hole Detection** - The MC40 includes enhancements to the IEEE 802.11k standard. These improvements will report gaps in signal coverage to the Zebra wireless LAN infrastructure. Network administrators can detect and mitigate coverage gaps present in the network for greater reliability. Default: enabled.
- **Aggregated Fast Transition** - Aggregated FT improves on IEEE 802.11r, Over-the-DS fast roaming. In conjunction with Zebra wireless LAN infrastructure, the MC40 will achieve more reliable and consistent fast roaming. Default: enabled.
- **Scan Assist** - The MC40 monitors neighbor access points and retrieves roaming related information from the Zebra wireless LAN infrastructure without doing scans. Using this Scan Assist feature, the MC40 improves roaming. Default: enabled.

---

## Remove a Wi-Fi Network

To remove a remembered or connected network:



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

# CHAPTER 6 SETTINGS

This chapter describes settings available for configuring the device.

---

## 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.
  - **Swipe** - Slide the lock icon to unlock the screen.
  - **Pattern** - Draw a pattern to unlock screen. See [Set Screen Unlock Using Pattern on page 6-3](#) for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See [Set Screen Unlock Using PIN on page 6-2](#) for more information.
  - **Password** - Enter a password to unlock screen. See [Set Screen Unlock Using Password on page 6-2](#) for more information.

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

### Single User Mode




When locked, a slide, 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.

## Set Screen Unlock Using PIN

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

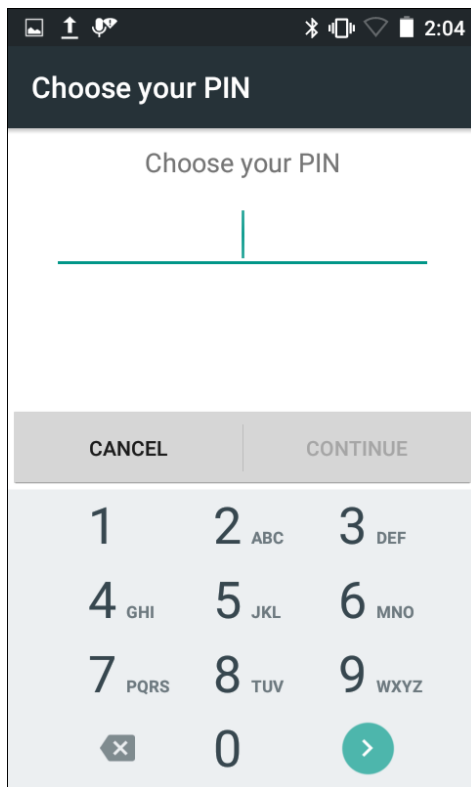



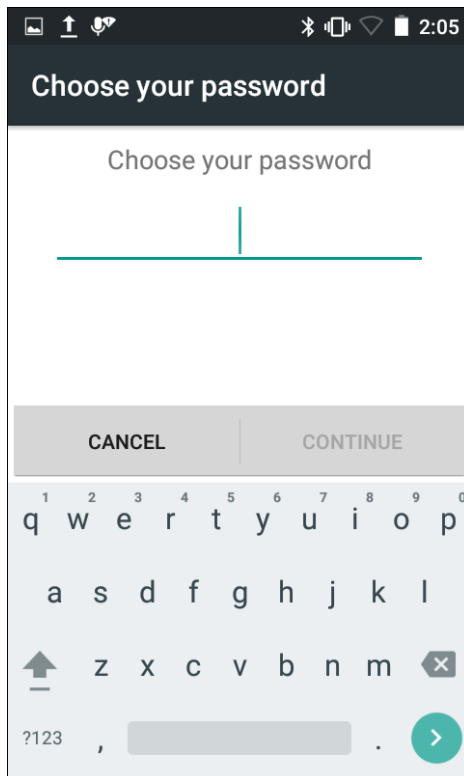


Figure 6-1 Choose Your PIN Screen




## Set Screen Unlock Using Password

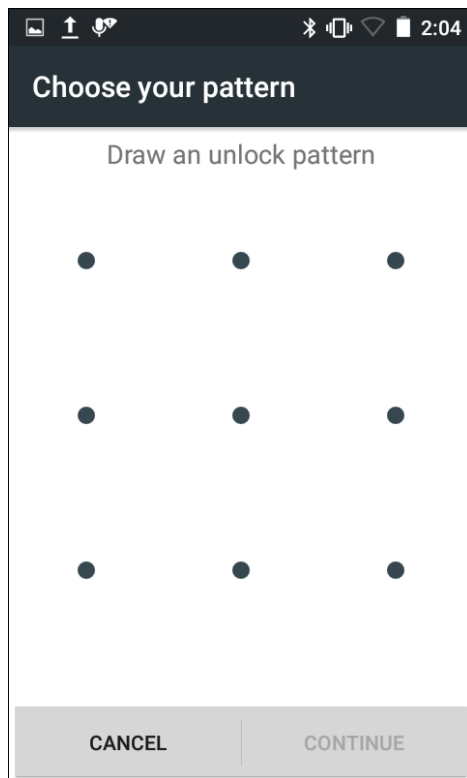
1. Touch  >  **Security** > **Screen lock**.
2. Touch **Password**.
3. Touch in the text field.
4. Enter a password (between 4 and 16 characters) then touch **Continue**.
5. Re-enter the password and then touch **OK**.
6. Touch . The next time the device goes into suspend mode a password is required upon waking.



**Figure 6-2** *Choose Your Password Screen*

## Set Screen Unlock Using Pattern



1. Touch  >  **Security** > **Screen lock**.
2. Touch **Pattern**.
3. Draw a pattern connecting at least four dots.
4. Touch **Continue**.
5. Re-draw the pattern.
6. Touch **Confirm**.
7. Touch an option for **When your device is locked, how do you want notifications to show?**
  - a. **Show all notification content** - Notifications and their details display on the lock screen.
  - b. **Hide sensitive notification content** - Notifications display on the lock screen, but any details that could reveal private information is automatically hidden.
  - c. **Don't show notifications at all** - Notifications do not display on the lock screen. Notifications display once the device is unlocked.
8. Touch **Done**.
9. On the **Security** screen, slide the **Make pattern visible** switch to the **ON** position to show pattern when you draw the pattern.
10. Touch . The next time the device goes into suspend mode a Pattern is required upon waking.



**Figure 6-3** *Choose Your Pattern Screen*





---

## Passwords

To set the device to briefly show password characters as the user types, set this option. Touch  >  **Security**. Slide the **Make password visible** switch to the **ON** position.

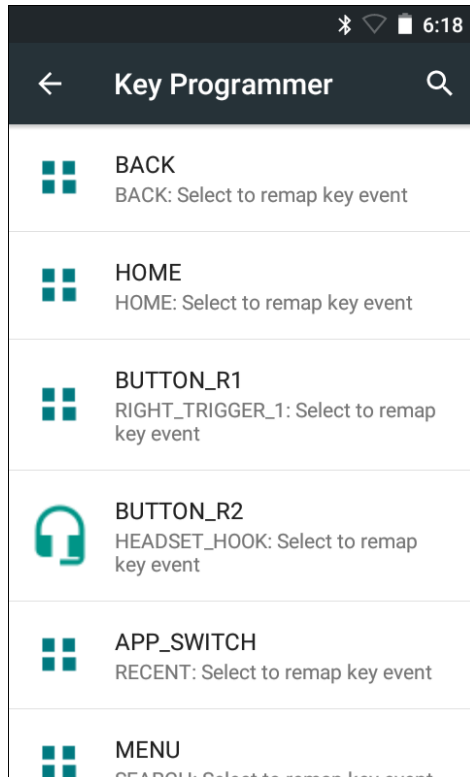
## Button Remapping

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

- BACK -  button below display
- HOME -  button below display
- RIGHT\_TRIGGER\_1- Right Scan button
- HEADSET\_HOOK - Button on Headset.
- RECENT -  button below display
- SEARCH -  button below display
- VOLUMEDOWN - Volume down button
- VOLUMEUP -Volume up button
- LEFT\_TRIGGER\_1 - Left Scan/Action button
- LEFT\_TRIGGER\_2 - PTT button.

### Remapping a Button

1. Touch  >  **Key Programmer**.

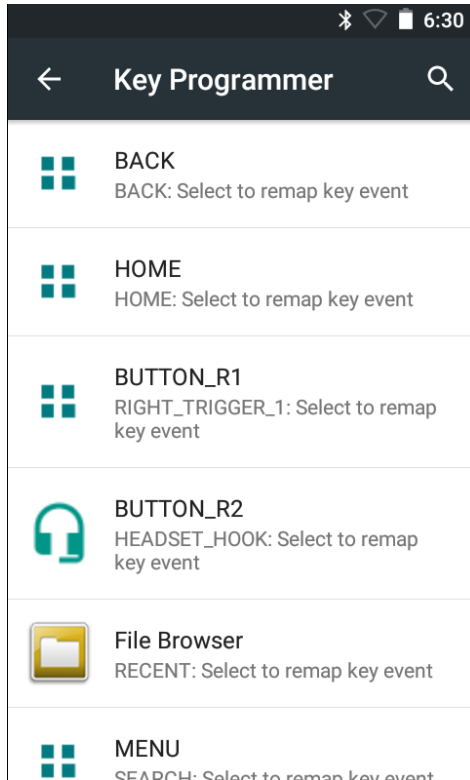


**Figure 6-4** Key Programmer Screen


2. Select the button to remap.
3. Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.

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

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



**Figure 6-5** *Remapped Button*

5. Touch .

## 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 an 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**.

1. Touch  >  **Key Programmer**.
2. Select the Headset button.
3. On the **BUTTON REMAPPING** tab, select **HEADSETHOOK**, **BUTTON\_R2** or **DONOTHING**
4. Touch .



## 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*.



**NOTE** Using the MC40 Android Lollipop version, a user cannot import/export the XML file from the application UI. This can only be done using CSP.

```
<?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_UP</REMAP_CODE>
    <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 [Appendix B, Keypad Remap Strings](#) for a list of available button functions.

## Enterprise Reset

To ensure that the configuration persists after an Enterprise Reset:

- 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:

- 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.

---

## Accounts

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



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

---




## Language Usage

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

### Changing the Language Setting

1. Touch  >  **Language & input**.
2. Touch **Language**.
3. In the **Language** screen, select a language from the list of available languages.  
The operating system text changes to the selected language.

### Adding Words to the Dictionary

1. Touch  >  **Language & input**.
2. Touch **Language**.
3. In the **Language** screen, select a language from the list of available languages.
4. In the **Language & input** screen, touch **Personal dictionary**.
5. Touch **+** to add a new word or phrase to the dictionary.
6. In the **Phrase** text box, enter the word or phrase.
7. In the **Shortcut** text box, enter a shortcut for the word or phrase.
8. **Touch** the check mark in the bottom right corner of the screen to add the new word.
9. **Touch** .

---

## Keyboard Settings

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

- Android Keyboard (AOSP)
- Japanese IME
- Chinese Keyboard

---

## Date Persistence

After a Real-time clock (RTC) reset, the system date returns to the default system date. To prevent the system date from returning to the default date:

The default system date is defined in the file *date.txt* located in the */enterprise/usr* folder.

On each MC40 reboot, the date saved in the *date.txt* file is compared to the system date.

If the system date is less than the date in *date.txt* file then the system date is updated with the one in *date.txt* file

If the system date is greater than the date in *date.txt* file, then the file is updated with the system date.

Currently the default date in the *date.txt* file is set to 2013-09-01 00:00:00. It can be modified by the system administrator as required.




## Ethernet Settings

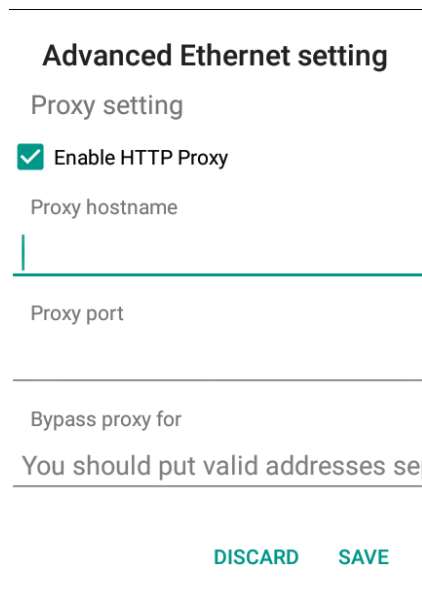
The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

### Configuring Ethernet Proxy Settings

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Advanced**.



**Advanced Ethernet setting**

Proxy setting

☒ Enable HTTP Proxy

Proxy hostname

Proxy port

Bypass proxy for

You should put valid addresses se


DISCARD SAVE

**Figure 6-6** Ethernet Proxy Settings

5. Touch **Enable HTTP Proxy**.
6. In the **Proxy hostname** field, enter the proxy server address.
7. In the **Proxy port** field, enter the proxy server port number.






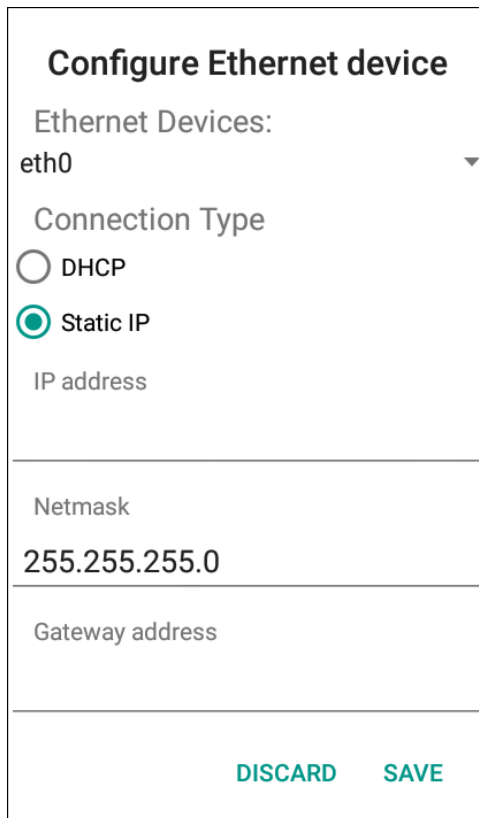
**NOTE** When entering proxy addresses in the **Bypass proxy for** field, do not use spaces or carriage returns between addresses.

8. 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.
9. Touch **Save**.
10. Touch .

## Configuring Ethernet Static IP Address

The MC40 includes Ethernet cradle drivers. The MC40 can connect to an Ethernet network using a third-party Ethernet dongle. After connecting the MC40, configure the Ethernet connection. By default, the device is configured to use Dynamic Host Configuration Protocol (DHCP) to assign an Internet Protocol (IP) address when connecting to an Ethernet network. To configure the device to connect to a network using a static IP address:

1. Place the MC40 into the Ethernet cradle slot.
2. Touch  >  **Ethernet**.
3. Slide the switch to the **ON** position.
4. Touch  > **Config**.



**Configure Ethernet device**

Ethernet Devices:  
eth0 ▼

Connection Type

☐ DHCP

☒ **Static IP**

IP address

---

Netmask

255.255.255.0


---

Gateway address

---



**DISCARD** **SAVE**

**Figure 6-7** *Configure Ethernet Device Settings*

5. Under **Connection Type**, touch the **Static IP** radio button.  
**DHCP** is the default **Connection Type**.
6. In the **IP address** field, enter the proxy server address.
7. If required, in the **Netmask** text box, enter the network mask address.
8. If required, in the **Gateway address** text box, enter a gateway address for the device.
9. If required, in the **DNS 1 address** text box, enter a Domain Name System (DNS) address.
10. If required, in the **DNS 2 address** text box, enter a DNS address.
11. Touch **Save**.
12. Touch .

---

## 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.
  - **Ethernet MAC address** - Displays the Ethernet 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.
- **SW components** - Lists filenames and versions for various software on the MC40.
- **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.
- **Build tags** - Displays the key used to sign the build.
- **Android version** - Displays the operating system version.
- **Android security patch level** - Displays the security patch level date.
- **Kernel version** - Displays the kernel version.
- **Build fingerprint** - Displays unique build information.
- **Build number** - Displays the software build number.

---

## PTT Express Configuration

The system administrator can manually configure PTT Express by creating an xml file and loading it onto the MC40. Refer to the *PTT Express User Guide* at <http://www.zebra.com/support> for information on configuring the PTT Express Client application.

### Importing a PTT Express Configuration File

1. Copy the configuration file *ptt\_settings.xml* from a host computer to the root of the On Device Storage. See [Chapter 3, USB Communication](#).
2. On the MC40, use File Browser to move the *ptt\_settings.xml* file from the root of the On Device Storage to the folder: `/enterprise/device/settings/ptt`.



**NOTE** The configuration file can also be loaded on the MC40 using ADB. See [Installing Applications Using the Android Debug Bridge on page 7-4](#)

## Remapping the PTT Private Key

The PTT Private Key and the Left Scan Trigger work differently in Android KitKat and Android Lollipop. In Android Lollipop, by default, the MC40 device does not support PTT Private Key functionality. In order to get the PTT Private Key functionality to work, it is necessary to remap the PTT Private Key as described in the procedure below. Performing the procedure enables PTT Private Key functionality but it disables scanning functionality from the left scan trigger and only allows the right scan trigger to be used scanning. This is not different from Android KitKat functionality when PTT is enabled. The only difference is that even when PTT is disabled, the left scan trigger cannot be used for scanning unless you reverse the procedure and remap the key back.

To avoid conflict with the left scan trigger, the PTT Private Call key code has been changed from KEYCODE\_BUTTON\_L1 to KEYCODE\_PTT and the corresponding physical key is mapped to act as the PTT Private Call key by default. This can be remapped to any other desired keys using the existing key remapping UI or the StageNow application.

To remap the key using StageNow:

1. Launch StageNow from a host computer.
2. Click **Create new profile**.
3. On the **Select a Wizard** screen:
  - a. In the **Please select the MX version on your device** drop-down, select **MX 5.3**.
  - b. Click **Xpert Mode**.
  - c. Click **Create**.
4. On the **Xpert Mode** screen:
  - a. In the **Enter Profile name** field, enter the profile name.
  - b. Click **Start**.
5. On the **ADD/EDIT** screen:
  - a. Add **KeyMappingMgr**.
  - b. Click **Add**.
6. On the **StageNow Config** tab for KeyMappingMgr:
  - a. Enable **Re-use Saved Setting**.
  - b. Under **Action**, select **Remap a key**.
  - c. In the **Choose a key to modify** drop-down, select **Button L1**.
  - d. In the **Key-code** drop-down, select **Push-to-talk**.
  - e. Click **Continue**.
7. On the **Review** tab for Staging Profile, click **Complete Profile**.
8. On the **Publish** tab:
  - a. Select **Barcode**.
  - b. Click **Test**.

The bar code is generated in a PDF.

9. Scan the bar code using the StageNow application on the device.



---

## Low RAM Device Configuration

By default, the MC40 with Android V5.1.1 is configured as a low RAM device. This restricts some features available on the device, such as Data Separation and Multiuser functionality. To change the configuration to enable those features, the system property “persist.lowram\_override” must be set to true. This system property overrides the default “low-ram” setting (configured via ro.config.low\_ram flag) that the device is shipped with.

To set the system property programmatically:

```
{  
    Class clazz;  
    clazz = Class.forName("android.os.SystemProperties");  
    Method method = clazz.getDeclaredMethod("set", String.class, String.class);  
    method.invoke(null, "persist.lowram_override", "true");  
        } catch (Exception e) {  
        //Add proper error handling here  
}
```



# CHAPTER 7 APPLICATION DEPLOYMENT

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

---

## Security

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



**NOTE** Ensure the date is set correctly before installing certificates or when accessing secure web sites.

### Secure Certificates



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

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

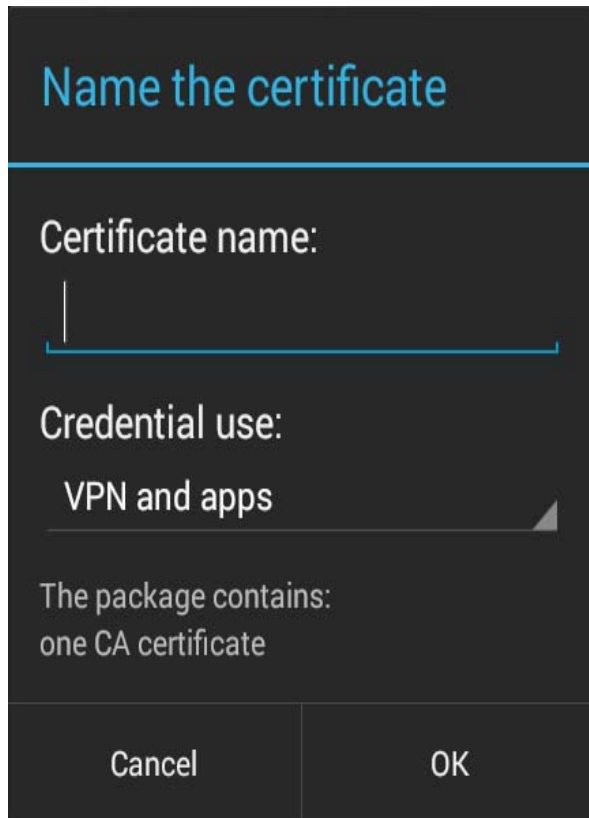
The device also installs any accompanying private key or certificate authority certificates contained in the key store.

### Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the On Device Storage. See [Chapter 3, USB Communication](#) for information about connecting the device to a host computer and copying files.
2. Touch  >  **Security**.
3. Touch **Install from On Device Storage**.
4. Navigate to the location of the certificate file.



5. Touch the filename of the certificate to install. Only the names of certificates not already installed display.
6. If prompted, enter the certificate's password and touch **OK**.
7. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.



**Figure 7-1** *Name the Certificate Dialog Box*

8. 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.

## Configuring Credential Storage Settings

1. 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.

---

## Development Tools

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



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

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

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

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

Open the Developer options screen to set development related settings.

By default, the Developer Options are hidden. To un-hide the developer options, touch  >  **About device**. Scroll down to **Build number**. Tap **Build number** seven times until **You are now a developer** appears.

Touch  >  **Developer options**. Slide the switch to the **ON** position to enable developer options.

---

## ADB USB Setup

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

ADB driver for Windows and Linux are available on the Zebra Support Central web site at <http://www.zebra.com/support>. Download the ADB and USB Driver Setup package. Follow the instructions with the package to install the ADB and USB drivers for Windows and Linux.

---

## Application Installation



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

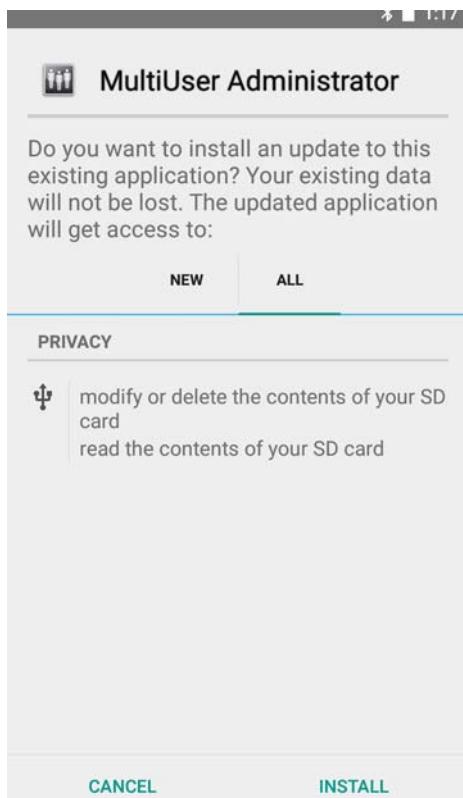
- USB connection, see [Installing Applications Using the USB Connection on page 7-4](#).
- Android Debug Bridge, see [Installing Applications Using the Android Debug Bridge on page 7-5](#).
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

## Installing Applications Using the USB Connection



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

1. Connect the device to a host computer using USB. See [Chapter 3, USB Communication](#).
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 [Chapter 3, USB Communication](#).
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 7-2** *Accept Installation Screen*

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



## Installing Applications Using the Android Debug Bridge

Use ADB commands to install applications 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.

Ensure that the ADB drivers are installed on the host computer. See [ADB USB Setup on page 7-3](#).

1. Connect the device to a host computer using USB. See [Chapter 3, USB Communication](#).
2. Touch  >  **Developer options**.
3. Slide the switch to the **ON** position.
4. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
5. Touch **OK**.
6. 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.
7. Disconnect the device from the host computer. See [Chapter 3, USB Communication](#).

## 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:

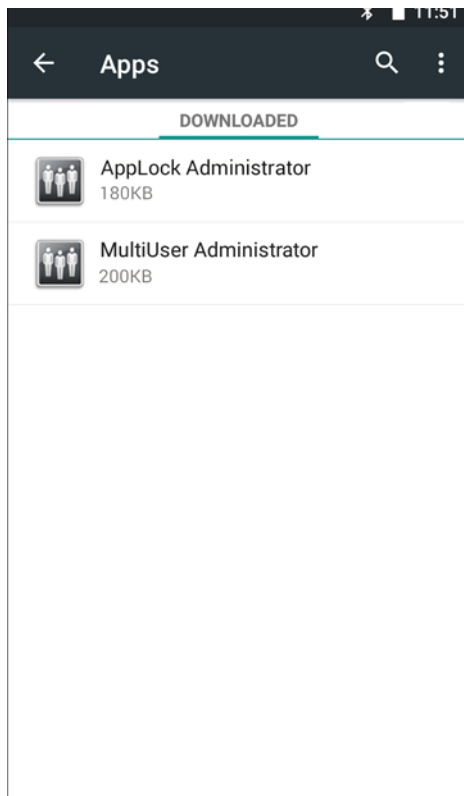
- The **Rapid Deployment** application provides support for MSP Staging functionality, provides support for the MSP Legacy Staging process, and provides support for backward-compatible legacy MSP 2.x Legacy Staging functionality.
- The **MSP Agent** application provides MSP Provisioning functionality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

## Uninstalling an Application

To uninstall an application:

1. Touch  >  **Apps**.
2. Swipe left or right until the **Downloaded** screen displays.



**Figure 7-3** Downloaded Screen

3. Touch the application to uninstall.
4. Touch **Uninstall**.
5. Touch **OK** to confirm.

---

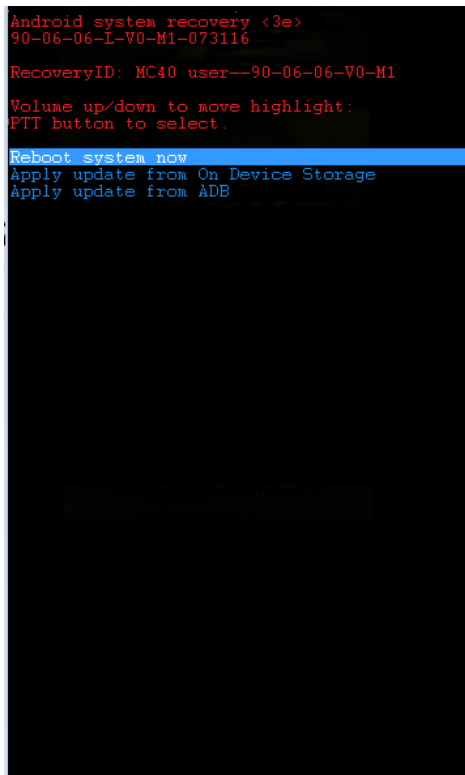
## System Update

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

Before performing a system update, copy all installed applications that you want to persist after the update into the `/enterprise/usr/persist` folder. After the update is complete, the MC40 installs the applications.

1. Download the system update package:
  - a. Go to the Zebra Support & Downloads web site, <http://www.zebra.com/support>.
  - b. Download the appropriate System Update package to a host computer.
2. Copy the System Update Package zip file (*M40N0LXXVRBxx21104.zip*) to the root directory of the On Device Storage. See [Chapter 3, USB Communication](#) for more information.
3. Press and hold the Power button until the menu appears.
4. Touch **Reboot**.
5. Press and hold the Left Scan button.
6. When the Zebra logo splash screen appears, release the scan button.  
The **System Recovery** screen appears.









**Figure 7-4** System Recovery Screen

7. Press the Volume Up and Volume Down buttons to navigate to the **Apply update from On Device Storage** option.
8. Press the PTT button.
9. For Lollipop device updates, press the Volume Up and Volume Down buttons to navigate to the System Update Package zip file (*M40N0LXXVRBxx21104.zip*).
10. Press the PTT button. The System Update installs and then the MC40 resets.

## Copying Applications and Configuration Files

Before performing an upgrade, 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.

1. Touch  > .
2. Navigate to the */enterprise/user* folder.
3. Touch  > **New Folder**.
4. In the **Create a New Folder** dialog box, enter *persist*.
5. Touch **OK**.
6. Locate application .APK files and configuration .xml files and copy into the */enterprise/user/persist* folder.
7. Touch .

---

## Upgrading the Operating System from KitKat to Lollipop

The MC40 KitKat (AOSP V4.4.4) operating system can be upgraded to Lollipop (AOSP V5.1.1) operating system. MC40 non-voice KitKat configurations must be first converted to voice configuration prior to upgrading to Lollipop.

Customers who purchased a Service Agreement option for the MC40 KitKat version, are entitled to a one-time, operating system upgrade via the Zebra Customer Support web site: <http://www.zebra.com/support>. Customers must enter the serial number for each device to be upgraded. Zebra 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 Lollipop, an Operating System Upgrade must be purchased separately. The software will be delivered after the customer places an order. 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.

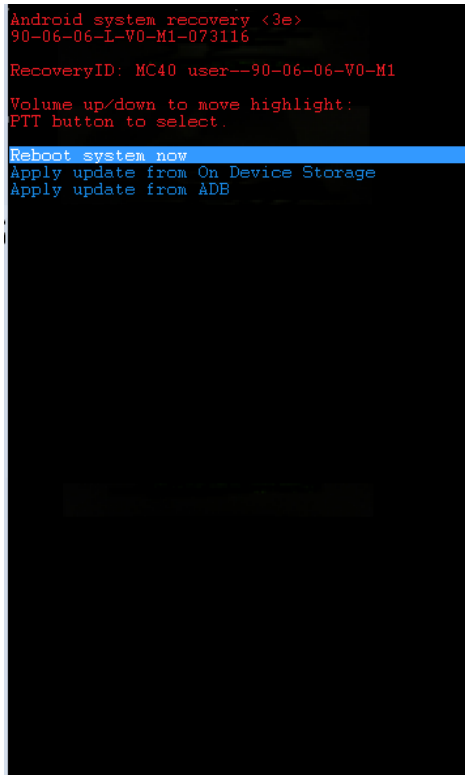
Refer to the MDM Client documentation for information on how to upgrade the MC40 using an MDM. The upgrade can also be performed on an individual device using the procedure below.

### Converting Non-Voice Configuration to Voice Configuration



**NOTE** MC40 non-Voice configuration must be converted into a Voice configuration prior to upgrading to Lollipop.

1. Download the MC40 KitKat Non-Voice to Voice Recovery Package:
  - a. Go to the Zebra Support & Downloads web site, <http://www.zebra.com/support>.
  - b. Locate the MC40 KitKat Non-Voice to Voice Recovery Package.
  - c. Download the package into a separate folder.
    - MC40 KitKat Non-Voice to Voice Recovery Package - *recovery-update-voice-l.zip*
2. Copy the *recovery-update-voice-l.zip* file to the root directory of the On Device Storage. See [Chapter 3, USB Communication](#) for more information.
3. Disconnect the MC40 from the host computer.
4. Press and hold the Power button until the menu appears.
5. Touch **Reboot**.
6. Press and hold the Left Scan button.
7. When the Zebra logo splash screen appears, release the scan button.  
The **System Recovery** screen appears.



**Figure 7-5** System Recovery Screen

8. Press the Volume Up and Volume Down buttons to navigate to the **Apply update from On Device Storage** option.
9. Press the PTT button.
10. For Lollipop device updates, press the Volume Up and Volume Down buttons to navigate to the *recovery-update-voice-l.zip* file.
11. Press the PTT button. The System Update installs and then the device resets.
12. Press the Volume Up and Volume Down buttons to navigate to the **Reboot system now** option.
13. Press the PTT button to reboot the device.

## Upgrading to Lollipop

1. Download the Recovery OS Update Image for MC40N0 Lollipop package:
  - a. Go to the Zebra Support & Downloads web site, <http://www.zebra.com/support>.
  - b. Locate the **Recovery OS Update Image for MC40N0 Lollipop** and **Factory Reset** and **Enterprise Reset files for MC40N0** packages.
  - c. Download the packages to a host computer.
    - MC40 Voice Lollipop Recovery OS Update Package - M40N0LXXVRBxx21104.zip
    - KitKat to Lollipop Recovery OS upgrade Package for Voice Device - M40N0LXXVRBxx21104.zip

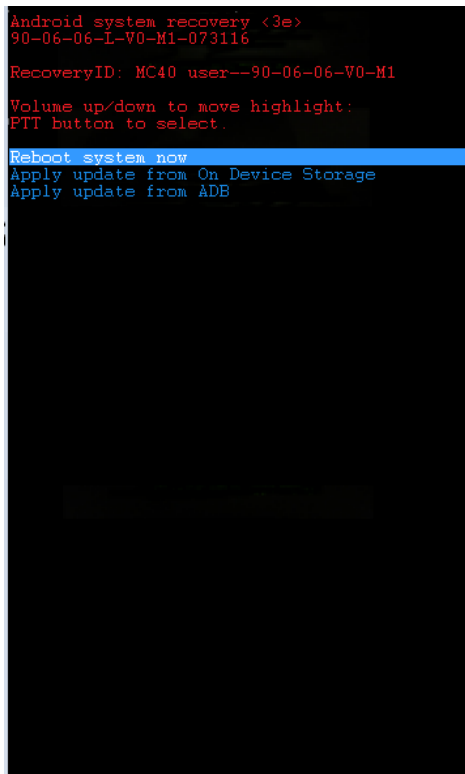
There is no special upgrade package for updating from KitKat to Lollipop. The same package is used for KitKat to Lollipop and Lollipop to Lollipop update.

    - MC40 Lollipop Enterprise Reset Package - M40N0LXXXRE0000002.zip

This step is needed only if the user wants the user data to be wiped out along with updating from KitKat to Lollipop.

- MC40 Lollipop Factory Reset Package - M40N0LXXXRF0000002.zip
2. Copy the zip files (M40N0LXXVRBxx21104.zip and M40N0LXXXRE0000002.zip) into the root directory of the On Device Storage. See [Chapter 3, USB Communication](#) for more information.
  3. Press and hold the Power button until the menu appears.
  4. Touch **Reboot**.
  5. Press and hold the Left Scan button.
  6. When the Zebra logo splash screen appears, release the scan button.

The **System Recovery** screen appears.



**Figure 7-6** System Recovery Screen

7. Press the Volume Up and Volume Down buttons to navigate to the **Apply update from On Device Storage** option.
8. Press the PTT button.
9. For Lollipop device updates, press the Volume Up and Volume Down buttons to navigate to the M40N0LXXVRBxx21104.zip file.
10. Press the PTT button. The System Update installs and then the device resets.
11. Press the Volume Up and Volume Down buttons to navigate to the M40N0LXXXRE0000002.zip file.  
This step is needed only if the user wants the user data to be wiped out along with updating from KitKat to Lollipop.
12. Press the PTT button. The System Update installs and then the device resets.
13. Press the Volume Up and Volume Down buttons to navigate to the **Reboot system now** option.
14. Press the PTT button to reboot the device.

# Storage


The device contains four types of file storage:

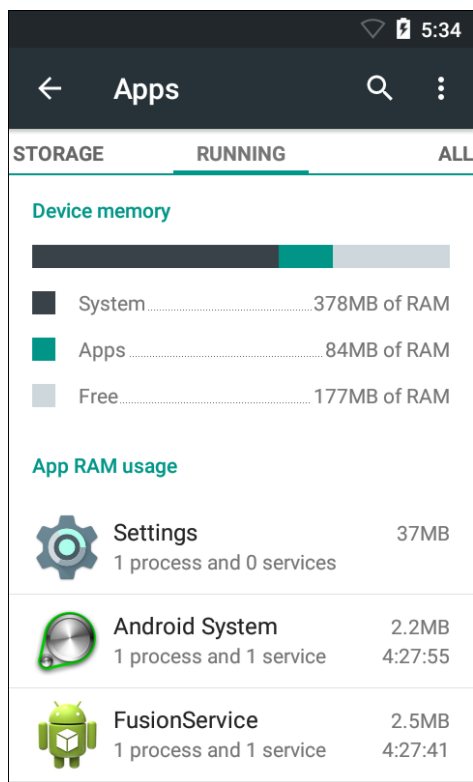
- Random Access Memory (RAM)
- On Device Storage
- Internal storage
- Enterprise folder.

## Random Access Memory

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

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

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





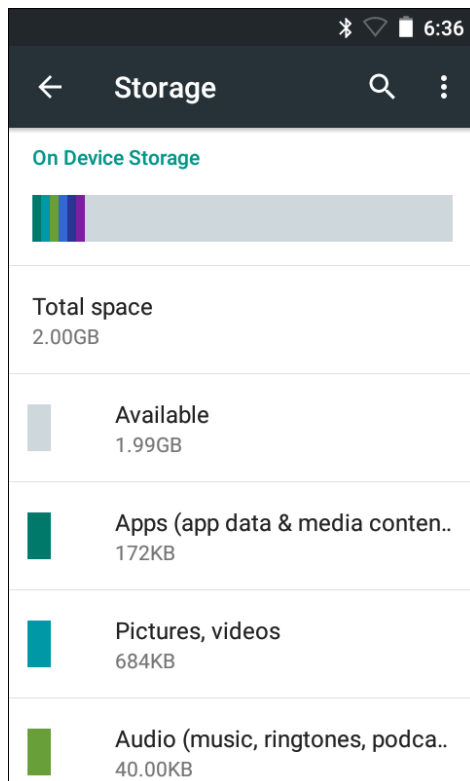
**Figure 7-7** *Running Screen*

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

## 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**.





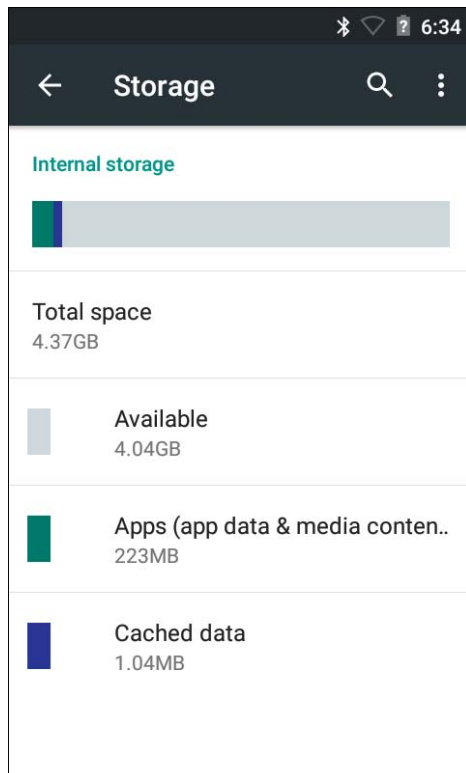
**Figure 7-8** On Device Storage Screen

- **On Device Storage**
  - **Total space** - Displays the total amount of space on On Device Storage.
  - **Available** - Displays the available 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.
  - **Audio** - Displays the available space used for music, ringtones, and podcasts on On Device Storage.
  - **Downloads** - Displays the available space used for downloaded files on On Device Storage.
  - **Cached data** - Displays the amount of cached data on On Device Storage.
  - **Misc** - Displays the available space used for miscellaneous files on On Device Storage.
- **Erase On Device Storage** - Permanently erases everything on the installed On Device Storage.

## Internal Storage

The MC40 has internal storage. The internal 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 internal storage rather than in internal memory.

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



**Figure 7-9** Internal Storage Screen



- **Internal Storage**
  - **Total space** - Displays the total amount of space on internal storage.
  - **Available** - Displays the available space on internal storage.
  - **Apps** - Displays the available space used for applications and media content on internal storage.
  - **Cached data** - Displays the amount of cached data on On Device Storage.

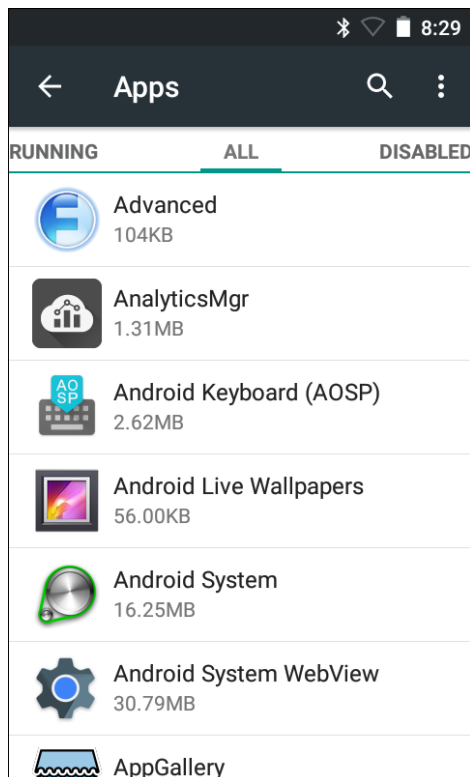
## Enterprise Folder

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

## Application Management

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

From the Home screen touch  >  **Apps**.



**Figure 7-10** Apps Screen

The **Apps** screen has five 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 **On Device Storage** 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.
- Slide the screen to the **Running** tab to view the applications and their processes and services that are running or cached.
- 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 **Disabled** tab to view the applications that are disabled.

When on the **Downloaded**, **All**, **On Device Storage**, or **Disabled** tab, touch  > **Sort by size** to switch the order of the list.






# Viewing Application Details

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

- Touch **Force stop** to stop an application.
- Touch **Uninstall** to remove the application and all of its data and settings from the device. See [Uninstalling an Application on page 7-5](#) 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** - 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.

# Stopping an Application

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

1. Touch  >  **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.

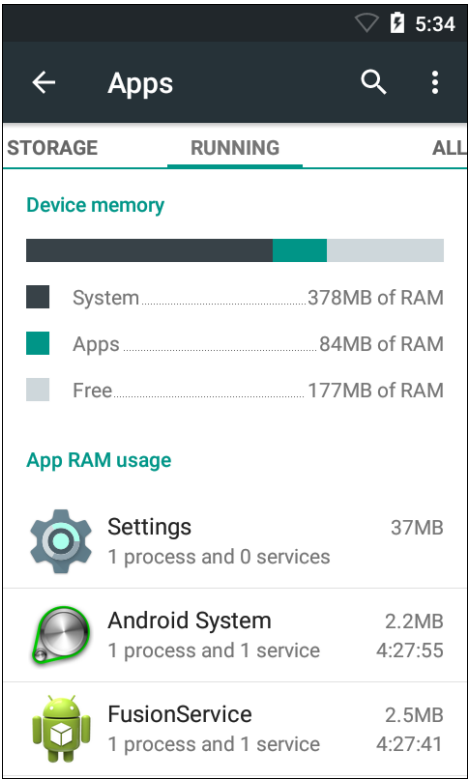


Figure 7-11 *Running Applications*

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





**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.

5. Touch **Stop**.

### 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.

1. Touch  >  **Apps**.
2. Swipe the screen to display the **On Device Storage** 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 Storage 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 device** to move the application back to the device's internal storage.

### Managing Downloads

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

1. Touch  >  **Downloads**.
2. Touch an item to open it.
3. Touch and hold an item to delete; then touch . The item is deleted from storage.
4. Touch  > **By name**, **By date modified**, or **By size** 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.

---

## RxLogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics. It allows for custom plug-ins to be created and work seamlessly with this tool. RxLogger is used to diagnose device and application issues. Its information tracking includes the following: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging, cellular logging, TCP dumps, Bluetooth logging, GPS logging, logcat, FTP push/pull, ANR dumps, etc. All logs and files generated are saved onto flash storage on the device (internal or external).

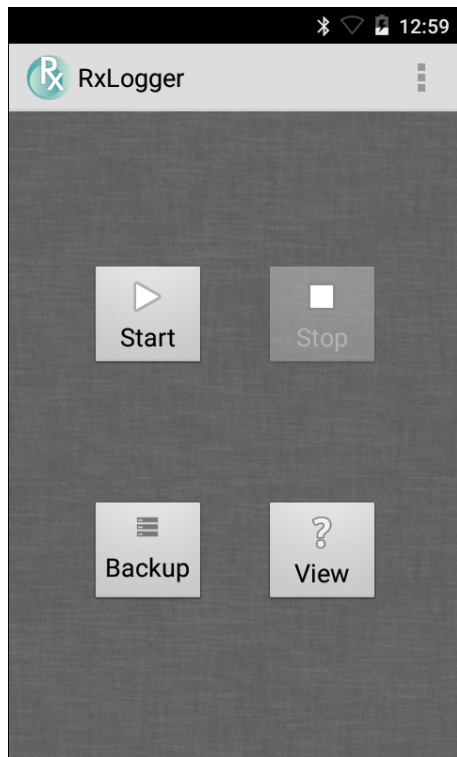



Figure 7-12 RxLogger

### RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plug-ins already built-in. The included plug-ins are described below. Touch  > **UI Settings** to open the configuration screen.



**Figure 7-13** RxLogger Configuration

### Main Log Plug-in

The Main log presents a high level time line view of the device health in an easy to read comma-separated values (CSV) format. The log contains many of the key parameters of various subsystems and is meant to be used as a first level triage that can potentially point to a range of specific detailed logs to look at. The two rightmost columns in the CSV file allow the log modules and plug-ins to insert asynchronous event based messages into the log. This is useful so that by looking at the CSV log you can see when snapshots have been created or when the tool has detected an application to be unresponsive. It is also used to show power events such as AC/DC power transitions.

- **Enable notifications** - Enables logging for this plug-in.
- **Log Interval** - Specifies the interval, in milliseconds, to poll the collected parameters and write the data to the CSV log file.
- **Log path** - Specifies the base log path to store the CSV log file. The default is to use the default external storage directory which is queried from the Android system.
- **Log file count** - Specifies the number of files to rotate through. Each file is constrained by the Log max size option.
- **Log max size** - Specifies the maximum size, in kilobytes, of each log file for the main CSV log.
- **Power** - Enables logging of power related parameters and events. These include battery stats (capacity, current, voltage, etc) and AC/DC power notification events.
- **System resources** - Enables logging of CPU and memory related items (Avg/current CPU load, program memory, storage memory, process count, etc).
- **Wifi** - Enables logging of wireless LAN items (WLAN power, signal strength, essid, connected AP, etc).
- **Cellular** - Enables logging of wireless WAN items (WAN power, network type, signal strength, connected cell tower, etc).
- **Network** - Enables logging of network items (IP address, default gateway, etc).

- **Bluetooth** - Enables logging of Bluetooth items (Bluetooth power, discoverable, connected, etc).
- **GPS** - Enables logging of GPS data (position, speed, etc).
- **GPS update frequency** - Specifies the frequency of GPS updates requested from the system. This setting can greatly affect battery life when using the tool. Frequent GPS updates will use a lot of power and the effects are greater if the device is indoors where a position cannot be obtained.
- **Light** - Enables logging of ambient light.

### PushPullClient Plug-in

The PushPullClient plug-in is designed to automatically push log files to a remote FTP server on a regular basis. It also has the capability to pull a remote file from the FTP server to a local directory on the device to automatically pull down a new configuration file so that the configuration of the tool can be set and updated remotely. The tool uses a flag file on the FTP site (based on device serial number) to ensure the file is only pulled once. By removing the flag file for a particular device you can force it to download the file again.

- **Enable Plugin** - Enables logging for this plug-in.
- **Hostname** - Specifies the FTP server to connect to.
- **Username** - Specifies the username to use to log onto the FTP server.
- **Password** - Specifies the password to use to log onto the FTP server.
- **Enable push** - Enables pushing of file to the specified FTP server.
- **Push interval** - Specifies the amount of time, in milliseconds, in between pushes to the FTP server.
- **Local directory to push** - Specifies the local directory to push files from.
- **Temp files directory** - Specifies the local directory where temporary files are located.
- **Remote push directory** - Specifies the remote directory to push files to. A separate folder will be created for each device using the device serial number.
- **Wakeup for push time** - If the pull interval is set to 0, this will specify a specific time to initiate an FTP push.
- **Do push on start** - Enable an FTP push upon startup of the plug-in.
- **Enable pull** - Enable FTP pull functionality.
- **Pull interval** - Specifies the amount of time, in milliseconds, in between pulls from the FTP server.
- **Remote pull directory** - Specifies the directory on the FTP server where the file to be pulled will be located.
- **Remote pull filename** - Specifies the file to be pulled from the FTP server.
- **Local pull directory** - Specifies the local directory to store the file pulled from the FTP server.

### KernelLog Plug-in

The kernel plug-in facilitates the capturing of Kernel traces.

- **Enable Plugin** - Enables logging for this kernel buffer.
- **Log Path** - Specifies the high level log path for storage of all kernel logs. This setting applies globally to all kernel buffers.
- **Kernel Log Filename** - Specifies the base log filename for this kernel buffer. The current file count is appended to this name.
- **Max Kernel Log size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Kernel Log Interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
- **Kernel Log File Count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.

### ANR Plug-in

Application Not Responsive (ANR) indicates that a running application's UI thread is not responding for a specified time period. RxLogger is able to detect this condition and trigger a copy of the call stack trace of the unresponsive application into the log directory. The event will also be indicated in the high level CSV log.

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the default log path to store the ANR log files.
- **Max file size** - Specifies the maximum file size, in kilobytes, of the ANR trace to be copied. If the file is too large, the copy will be skipped. On older devices that append each ANR event to the same trace file the size can get very large. In this case we will avoid expending resources to copy the large file every time.

### LTS Plug-in

The LTS plug-in is used for keeping a complete set of log files on a device for a longer period of time without any redundancy in the data. It will also zip all files as it saves them, in order to save space.

- **Enable Plugin** - Enables logging for this plug-in.
- **RXlogger Storage Directory** - Specifies the folder that RxLogger is writing to so that LTS can start to observe the directory.
- **LTSP Storage Directory** - Specifies the folder in which LTS plug-in should write its log files.

### Logcat Plug-in

Logcat is an essential debugging tool on Android devices. RxLogger provides the ability to record data from all four of the available logcat buffers. The Logcat plug-in has the ability to collect data from multiple logcat buffers provided by the system. Currently these are the main, event, radio, and system buffers. Each of the settings are available for each buffer independently unless otherwise noted.

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.
- **Main Logcat Buffer**
  - **Enable main logcat** - Enables logging for this logcat buffer.
  - **Main log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
  - **Main log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Main log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Max main log size** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Main log filter** - Custom filter to reduce log output.

- Event Logcat Buffer
  - **Enable event logcat** - Enables logging for this logcat buffer.
  - **Event log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
  - **Event log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Event log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Max Event log size** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Event log filter** - Custom filter to reduce log output.
- Radio Logcat Buffer
  - **Enable radio logcat** - Enables logging for this logcat buffer.
  - **Radio log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
  - **Radio log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Radio log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Max radio log size** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Radio log filter** - Custom filter to reduce log output.
- System Logcat Buffer
  - **Enable system logcat** - Enables logging for this logcat buffer.
  - **System log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
  - **System log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **System log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Max system log size** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **System log filter** - Custom filter to reduce log output.
- Combined Logcat
  - **Enable combined logcat** - Enables logging for this logcat buffer.
  - **Enable main buffer** - If checked, main buffer will be included in combined log file.
  - **Enable event buffer** - If checked, event buffer will be included in combined log file.
  - **Enable radio buffer** - If checked, radio buffer will be included in combined log file.
  - **Enable system buffer** - If checked, system buffer will be included in combined log file.
  - **Combined log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
  - **Combined log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Combined log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Max combined log size** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Combined log filter** - Custom filter to reduce log output.

## Tombstone Plug-in

The Tombstone plug-in facilitates the capturing of Tombstone traces.

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specified the location to store the Tombstone log files.
- **Max file size** - Specifies the maximum file size of the Tombstone trace to be copied. If the file is too large, the copy will be skipped. On older devices that append each Tombstone event to the same trace file, the size can get very large. In this case, expending resources to copy the large file every time is avoided.

### QxdmLog Plug-in

The Qxdm plug-in is used to capture data from the Qualcomm modem.

- **Enable Plugin** - Enables logging for this plug-in.
- **Use default path** - If enabled, will store files in the RxLogger path and ignore user input for storage location.
- **Log path** - Specifies the base path to store the QXDM files.
- **Qxdm Log Filename** - Specifies the base log filename for QXDM files. The current file count will be appended to this name.
- **Choose Log Filter** - Select only one filter and this filter will be used to produce QXDM logs.

### RamOops Plug-in

The RamOops plug-in is used to capture RamOops files which are generated after a kernel panic.

- **Enable Plugin** - Enables logging for this plug-in.
- **RamOops Directory** - Specifies the base path to store the RamOops files.
- **Base filename** - Specifies the base log filename for RamOops files. The current file count will be appended to this name.
- **Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.

### Snapshot Plug-in

The Snapshot plug-in collects data from the system in periodic intervals to capture system critical information.

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the base path to use to store the snapshot files
- **Log filename** - Specifies the base filename for all the snapshot files. This file number will be appended to this base filename when saving the snapshot.
- **Log interval** - Specifies the interval, in milliseconds, on which to invoke a detailed snapshot.
- **Time to keep** - Specifies the interval, in milliseconds, to keep snapshot files on the filesystem.
- **Snapshot Section Tag** - Used to separate sections in the snapshot file.
- **Top** - Enables logging most CPU intensive processes in the system.
- **CPU Info** - Enables detailed per process CPU logging in the snapshot.
- **Memory Info** - Enables logging of detailed per process memory usage in the snapshot.
- **Battery Info** - Enables logging of detailed power information including battery life, on time, charging, and wake locks.
- **Wake Locks** - Enables logging of system wake locks.
- **Time in State** - Lists CPU frequencies supported by CPU and time spent in each.



- **Processes** - Enables dumping the complete process list in the snapshot.
- **Threads** - Enables dumping all processes and their threads in the snapshot.
- **Properties** - Enables dumping of all system properties on the device. This includes build/version information as well as state information.
- **Interfaces** - Enables logging status of available network interfaces.
- **IP Routing Table** - Enables logging of kernel routing table entries.
- **Connectivity** - Enables logging of wireless connectivity information.
- **Wifi** - Enables logging of wifi information.
- **Network Usage** - Enables dumping of all available network interfaces and the routing table.
- **Filesystems** - Enables dumping of the available volumes on the file system and the free storage space for each.
- **Disk Usage** - Installed packages' disk usage (package name, code size, data size, and cache size).
- **Usage Stats** - Enables dumping of detailed usage information for each package on the device. This includes the number of starts and duration of each run.

## TCPDump Plug-in




The TCPDump plug-in facilitates the capturing of network traces to be viewed in Wireshark or a similar tool that can decode .cap files.

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the location to store the TCPDump output log files.
- **Base filename** - Specifies the base filename to use when storing the TCPDump files. The index number of the current log file will be appended to this filename.
- **Log file count** - Specifies the number of log files to cycle through when storing the network traces.
- **Max file size** - Specifies the maximum file size, in megabytes, for each log file created.




## Configuration File

RxLogger configuration can be set using an XML file. The config.xml configuration file is located on the microSD card in the RxLogger\config folder. Copy the file from the device to a host computer using a USB connection. Edit the configuration file and then replace the .XML file on the device. There is no need to stop and restart the RxLogger service since the file change is automatically detected.

## Enabling Logging

1. Touch  > .
2. Touch **Start**.
3. Touch .

## Disabling Logging

1. Touch  > .
2. Touch **Stop**.
3. Touch .

## **Extracting Log Files**

1. Connect the device to a host computer using an USB connection.
2. Using a file explorer, navigate to the RxLogger folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

# CHAPTER 8 MAINTENANCE AND TROUBLESHOOTING

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

---

## 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 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.

---

## 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 °F and +104 °F (0 °C and +40 °C)
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact Zebra Customer Support Center.
- 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.
- 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 Zebra Customer Support Center to arrange for inspection.

---

## Cleaning Instructions



**CAUTION** Always wear eye protection.

Read warning label on compressed air and alcohol product before using.

If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.



**WARNING!** Avoid exposing this product to contact with hot oil or other flammable liquids. If such exposure occurs, unplug the device and clean the product immediately in accordance with these guidelines.

## Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite<sup>1</sup>(see Important note below), hydrogen peroxide or mild dish soap.



**IMPORTANT** Use pre-moistened wipes and do not allow liquid to pool.

1 When using sodium hypochlorite (bleach) based products always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.

Due to the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidation (corrosion) when exposed to this chemical in the liquid form (including wipes). Avoid allowing any bleach based product to come in contact with the metal electrical contacts on the device, the battery, or the cradle. In the event that these types of disinfectants come in contact with metal on the device, prompt removal with alcohol-dampened cloth or cotton swab after the cleaning step is critical.

## Harmful Ingredients

The following chemicals are known to damage the plastics on the device and should not come in contact with the device: ammonia solutions, compounds of amines or ammonia; acetone; ketones; ethers; aromatic and chlorinated hydrocarbons; aqueous or alcoholic alkaline solutions; ethanolamine; toluene; trichloroethylene; benzene; carbonic acid and TB-lysoform.

## Cleaning Instructions

Do not apply liquid directly to the device. Dampen a soft cloth or use pre-moistened wipes. Do not wrap the device in the cloth or wipe, but gently wipe the unit. Be careful not to let liquid pool around the display window or other places. Allow the unit to air dry before use.

## Special Cleaning Notes

Many vinyl gloves contain phthalate additives, which are often not recommended for medical use and are known to be harmful to the housing of the device. The device should not be handled while wearing vinyl gloves containing phthalates, or before hands are washed to remove contaminant residue after gloves are removed. If products containing any of the harmful ingredients listed above are used prior to handling the device, such as hand sanitizer that contain ethanolamine, hands must be completely dry before handling the device to prevent damage to the plastics.

## Cleaning Materials Required

- Alcohol wipes
- Lens tissue
- Cotton-tipped applicators
- Isopropyl alcohol
- Can of compressed air with a tube.

## Cleaning Frequency

The cleaning frequency is up to the customer's discretion due to the varied environments in which the mobile devices are used. They may be cleaned as frequently as required, but it is advisable to clean the camera window periodically when used in dirty environments to ensure optimum performance.

## Cleaning the 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.

### Connector Cleaning

To clean the connectors:

1. Remove the main battery from mobile computer.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator back-and-forth across the connector. Do not leave any cotton residue on the connector.
4. Repeat at least three times.
5. Use the cotton-tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
6. Use a dry cotton-tipped applicator and repeat steps 4 through 6.



**CAUTION** Do not point nozzle at yourself and others, ensure the nozzle or tube is away from your face.

7. Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.
8. Inspect the area for any grease or dirt, repeat if required.

### Cleaning Cradle Connectors

To clean the connectors on a cradle:

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 away from your face.

5. Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.
6. Remove any lint left by the cotton-tipped applicator.
7. If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.
8. Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

If the temperature is low and humidity is high, longer drying time is required. Warm temperature and dry humidity requires less drying time.



---

## Troubleshooting



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

## Troubleshooting the MC40

**Table 8-1** *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 Installing the Battery.
	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 Resetting the AndroidDevice.
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 Resetting the AndroidDevice.
	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.
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  >  <b>Apps</b> > <b>Downloaded</b> . Select the unused programs and touch <b>Uninstall</b> .

**Table 8-1** Troubleshooting the MC40

Problem	Cause	Solution
The MC40 does not decode when reading bar code.	DataWedge is not enabled.	Ensure that DataWedge is enabled and configured properly. Refer to the <i>MC40 Integrator Guide</i> 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 <i>MC40 Integrator Guide</i> 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  > <b>Wi-Fi</b> >  > <b>Advanced</b> . Deselect the <b>Enable 802.11d</b> 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.







## Single-Slot Charge Cradle Troubleshooting

**Table 8-2** *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).

## Five-Slot Charge Only Cradle CRDUNIV-40-5000R Troubleshooting

**Table 8-3** *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  >  <b>About device &gt; Status</b> 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  >  <b>About device &gt; Status</b> 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.

## Four-Slot Battery Charger SACMC40XX-4000R Troubleshooting

**Table 8-4** *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.

# APPENDIX A TECHNICAL SPECIFICATIONS

The following sections provide technical specification for the device.

## MC40 Technical Specifications

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

**Table A-1**    *MC40 Technical Specifications*

Item	Description
<b>Physical Characteristics</b>	
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.

**Table A-1** MC40 Technical Specifications (Continued)

Item	Description
Audio	Speakers, microphone and headset connector (mono, 2.5 mm jack with microphone). Stereo audio through Bluetooth stereo headsets.
Disinfectant Ready	Yes (Healthcare version)
Colors	Silver, Healthcare Blue and White
Communications	All models: Push-to-Talk. PTT Express Client pre-loaded. VoIP Telephony Ready models: Optimized for VoIP telephony. VoIP client not included.
<b>Performance Characteristics</b>	
CPU	Texas Instruments OMAP 4430 @ 1 GHz, dual-core.
Operating System	Android-based AOSP 5.1.1 (Lollipop).
Memory	1 GB RAM, 8 GB Flash.
Output Power (USB)	Docking Connector: 5 VDC @ 500 mA max.
<b>User Environment</b>	
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
<b>Wireless LAN Data Communications</b>	
Wireless Local Area Network (WLAN) radio	IEEE® 802.11a/b/g/n/d/h/i/k/r with internal antenna
Data Rates	5GHz: 802.11a/n – up to 72.2 Mbps; 2.4GHz: 802.11b/g/n – up to 72.2 Mbps
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.

**Table A-1** MC40 Technical Specifications (Continued)

Item	Description
Security and Encryption	<p>WEP (40 or 104 bit);  WPA/WPA2 Personal (TKIP, and AES);  WPA/WPA2 Enterprise (TKIP, and AES) — EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0- MSCHAPv2, PE APv1-EAP-GTC, EAP-FAST (MSCHAPv2 and EAP-GTC) and LEAP  FIPS 140-2 Level 1 DIM (Data In Motion supported by FIPS Fusion - WLAN)</p> <p><b>Note:</b> Use the FIPS advanced option to enable or disable FIPS data in motion supported in WLAN FIPS 140-2, level 1 compliance.</p> <p>FIPS 140-2 DAR (Data at Rest supported by device) &amp; FIPS DIM (Data in Motion - WLAN)</p> <p><b>Notes:</b>  The FIPS DAR feature is enabled when device encryption is enabled through Settings &gt; Security &gt; Encrypt device.</p> <p>The FIPS DIM/DAR features are only available on the FIPS configuration of the device and are not available on the standard configuration.</p>
Multimedia	Wi-Fi Multimedia™ (WMM)
Certifications	WFA (802.11n, WMM, WMM-PS), Cisco CCXv4
Fast Roam	PMKID Caching, Opportunistic Key Caching (OKC), Cisco CCKM, 802.11r, Zebra Aggregated FT
<b>Wireless PAN Data and Voice Communications</b>	
Bluetooth	Class II, v 2.1 with EDR, v 4.0 with Low Energy; integrated antenna.
<b>Data Capture</b>	
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.
RS507 Hands-free Imager	Captures 1D and 2D bar codes.
<b>Sensors</b>	
Motion Sensor	3-axis accelerometer that enables motion sensing applications for dynamic screen orientation and power management.
Ambient Light/Proximity Sensor	Automatically adjusts display brightness and turns off the display during VoIP calls.
<b>Imager (SE4500-DL) Specifications</b>	
Field of View	Horizontal - 39.2° Vertical - 25.4°

**Table A-1** MC40 Technical Specifications (Continued)

Item	Description
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
<b>Imager (SE4710) Specifications</b>	
Field of View	Horizontal - 42.0° Vertical - 28.0°
Optical Resolution	1280 H X 800 V pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles
Focal Distance	From center of exit window: 19.4 cm (7.64 in.)
Aiming Element (VLD)	610 nm
Illumination Element (LED)	Hyper Red 660 nm
<b>Supported Symbolologies</b>	
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.

## MC40 Decode Zone

### SE4500-DL

The table below lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

**Table A-2** SE4500-DL Decode Distances

Symbol Density/ Bar Code Type	Bar Code Content/ Note 2 Contrast	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
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.

**SE4710**

The table below lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

**Table A-3** SE4710 Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
4.0 mil Code 39	3.3 in 8.4 cm	8.8 in 22.4 cm
5.0 mil Code 128	2.8 in 7.1 cm	8.2 in 20.8 cm
5.0 mil Code 39	2.0 in 5.08 cm	13.5 in 34.3 cm
5 mil PDF417	3.1 in 7.9 cm	8.4 in 21.3 cm
10 mil Data Matrix	2.9 in 7.4 cm	10.1 in 25.7 cm
100% UPC-A	1.8 in 4.6 cm*	26.0 in 66.0 cm
20 mil Code 39	2.0 in 5.08 cm*	30.0 in 76.2 cm

Note: \* Limited by width of bar code in field of view.

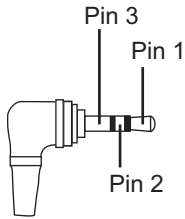
Distances measured from front edge of scan engine chassis.

**Note:** Photographic quality bar code at 15° tilt pitch angle under 30 fcd ambient illumination.



## MC40 Connector Pin-Outs

### Headset Connector

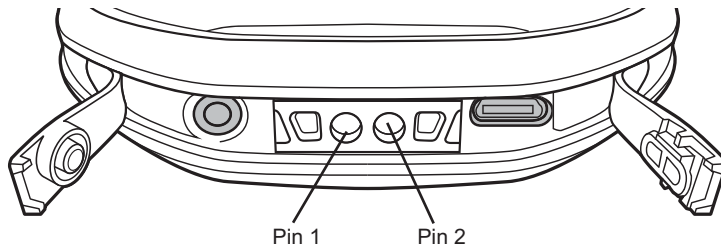


**Figure A-1** Headset Connector

**Table A-4** 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 A-2** Power Connector

**Table A-5** Power Connector Pin-Outs

Pin	Description
1	+5 VDC input power.
2	Ground

USB Connector

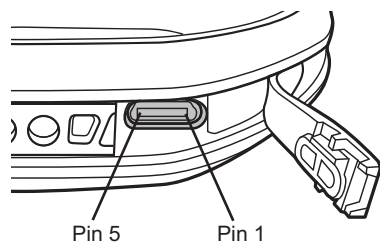


Figure A-3 *micro-B USB Connector*

Table A-6 *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	

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

**Table A-7** *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

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

**Table A-8** *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.)
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

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

**Table A-9** *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
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact



# APPENDIX B KEYPAD REMAP STRINGS

**Table B-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

**Table B-1** *Remap Key Event/Scancodes (Continued)*

Key Event	Scancode
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
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



**Table B-1** *Remap Key Event/Scancodes (Continued)*

Key Event	Scancode
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
DEL	111
GRAVE	41
MINUS	12
EQUALS	13
LEFT_BRACKET	26
RIGHT_BRACKET	27
BACKSLASH	86
SEMICOLON	39
APOSTROPHE	40
SLASH	53
AT	229
PLUS	78
MENU	139
SEARCH	217
PAGE_UP	177
PAGE_DOWN	178
PICTSYMBOLS	61

**Table B-1** *Remap Key Event/Scancodes (Continued)*

Key Event	Scancode
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





Zebra Technologies Corporation, Inc.

3 Overlook Point  
Lincolnshire, IL 60069, U.S.A.  
<http://www.zebra.com>

© 2018 ZIH Corp. and/or its affiliates. All rights reserved. ZEBRA and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. Android and Google are trademarks of Google Inc. All other trademarks are the property of their respective owners.