MC67 WITH ANDROID™ OS INTEGRATOR GUIDE

January 2014

MN000116A01

Copyrights

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

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 of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola, 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 Motorola contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

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

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

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

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

Revision History

Changes to the original guide are listed below:

Change	Date	Description
Rev. A	1/2014	Initial release.

Contents

List of Tables

List of Figures

About This Guide

Introduction

This guide provides information about using the MC67 mobile computer and accessories.

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

Documentation Set

The documentation set for the MC67 provides information for specific user needs, and includes:

- *MC67 Quick Start Guide* - describes how to get the MC67 up and running.
- *MC67 User Guide* - describes how to use the MC67.
- *MC67 Integrator Guide* - describes how to set up the MC67 and accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System	Keypads
MC67NA	WLAN: 802.11 a/b/g/n WPAN: Bluetooth v2.1 EDR WWAN:GSM/ UMTS GPS: Standalone GPS or A-GPS	3.5” VGA Color	1 GB RAM / 8 GB Flash	2D imager and camera	Android-based, Android Open-Source Project 4.1.1.	Numeric, QWERTY or DSD

Software Versions

To determine the current software versions touch ☰ > ⓘ**About phone**.

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

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

- *MC67 Quick Start Guide*, p/n MN000114Axx.
- *MC67 Regulatory Guide*, p/n MN000149Axx.
- *MC67 User Guide*, p/n MN000115Axx.
- *Mobility Services Platform User Guide*, p/n 72E-100158-xx.

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

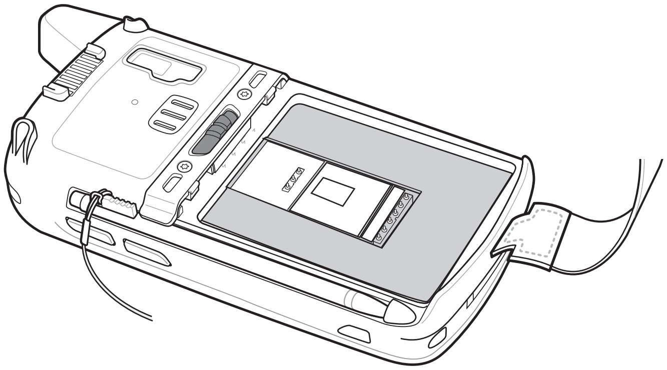
Service Information

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

When contacting support, 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
- IMEI number

Figure 1: Manufacturing Label



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

If the problem cannot be solved by Motorola Solutions Global Customer Support, the user may need to return the equipment for servicing and will be given specific directions. Motorola Solutions 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. Remove the SIM card and/or microSD card from the MC67 before shipping for service.

If the device was purchased from a Motorola Solutions business partner, contact that business partner for support.

Chapter 1

Getting Started

Setup

When and where to use: Perform this procedure to start using the MC67 for the first time.

Procedure:

1 Install a micro secure digital (SD) card (optional, required for saving photos, videos and sound recordings).
2 Install the subscriber identification module (SIM) card.
3 Install the battery.
4 Charge the MC67.
5 Power on the MC67.

Installing a microSD Card

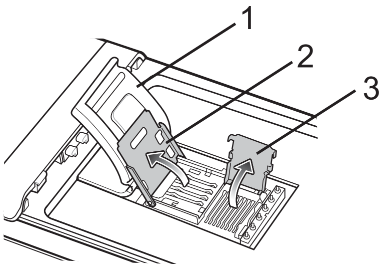
The microSD card slot provides secondary non-volatile storage. The slot is located under the battery pack. Refer to the documentation provided with the card for more information, and follow the manufacturer's recommendations for use.

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

Procedure:

1 To install the microSD card, remove the handstrap.
2 Lift the rubber access door.
3 Slide the SIM card holder door up to unlock.
4 Lift the SIM card holder door.

Figure 2: Lift SIM Slot Holder Door

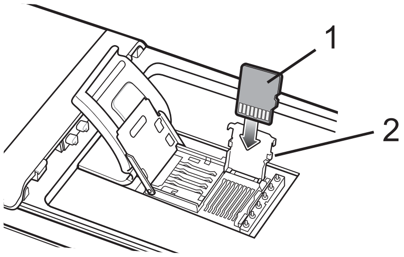


1	Rubber Access Door
2	SIM Card Holder Door
3	microSD Card Holder Door

5 Lift the microSD card holder door.

6 Insert the microSD card into the card holder door ensuring that the card slides into the holding tabs on each side of the door.

Figure 3: Insert microSD Card in Holder



1	microSD Card
2	Holding Tab

7 Close the card holder door and push down until it is securely in place.

8 Close the SIM card holder door and slide down until it locks into place.

9 Close the rubber access door.

Installing the SIM Card

Global System for Mobile communications (GSM) phone service requires a SIM card. Obtain the card from a service provider. The card fits into the MC67 and can contain the following information:

- Mobile phone service provider account details
- Information regarding service access and preferences
- Contact information, which can be moved to Contacts on the MC67
- Any additional subscribed services.

Note: For more information about SIM cards, refer to the service provider's documentation.

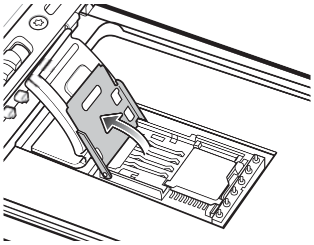
Procedure:

1 To install the SIM card, lift rubber access door.

2 Slide the SIM card holder up to unlock.

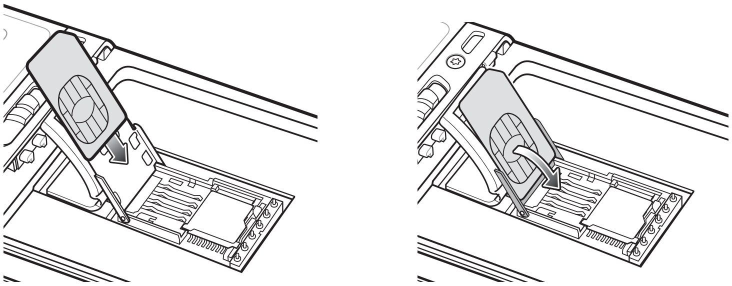
3 Lift the SIM card holder door.

Figure 4: Lifting the SIM Cover



4 Insert the SIM card, as shown in *Figure 5: Inserting the SIM Card on page 25* ensuring that the card slides into the holding tabs on each side of the door.

Figure 5: Inserting the SIM Card



5 Close the SIM card holder door and slide down to lock into place.
6 Close the rubber access door.
7 Install the battery.

Installing the Battery

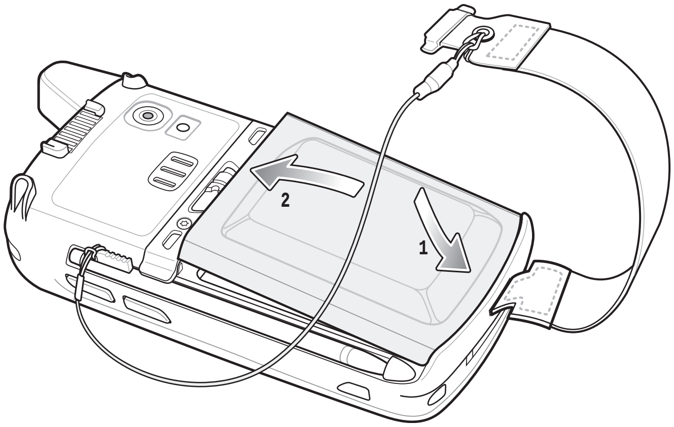
Procedure:

1 Insert the battery, bottom first, into the battery compartment in the back of the MC67.
2 Press the battery down into the battery compartment until the battery release latch snaps (two clicks) into place.

Note: If the battery has significant charge, the MC67 turns on.

3 Replace the handstrap.

Figure 6: Inserting the Battery



Charging the Battery

Before using the MC67 for the first time, charge the main battery until the amber Charging/Battery Status light emitting diode (LED) remains lit. To charge the MC67, use a cable or a cradle with the appropriate power supply. For information about the accessories available for the MC67, see *Accessories on page 33* for more information.

The MC67 is equipped with a backup battery which automatically charges from the fully-charged main battery. When using the MC67 for the first time, the backup battery requires approximately 40 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 MC67's main battery is removed. When the MC67 reaches a very low battery state, the combination of main battery and backup battery retains RAM data in memory for at least 36 hours.

For cable and cradle setup and charging procedures refer to the *MC67 Integrator Guide*.

- USB Charging Cable

- Charge Only Cable
- Single Slot USB Cradle
- Four Slot Charge Only Cradle
- Four Slot Ethernet Cradle.

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Note that charging is intelligently controlled by the MC67. To accomplish this, for small periods of time, the MC67 or accessory alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

Procedure:

1. To charge the main battery, connect the charging accessory to the appropriate power source.
2. Insert the MC67 into a cradle or attach to a cable. The MC67 turns on and begins charging. The Charging/Battery Status LED blinks amber while charging, then turns solid amber when fully charged.

LED Charging Indicators

Table 1: LED Charging Indicators

Charging/Battery Status LED	Indication
Off	MC67 is not charging. MC67 is not inserted correctly in the cradle or connected to a power source. Charger/cradle is not powered.
Slow Blinking Amber (1 blink every 2 seconds)	MC67 is charging.
Solid Amber	Charging complete. Note: When the battery is initially inserted in the MC67, the amber LED flashes once if the battery power is low or the battery is not fully inserted.
Fast Blinking Amber (2 blinks/second)	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).

Powering On the MC67

Note: If during installation of the battery, the battery has significant charge, the MC67 turns on automatically.

Procedure:

1. Press the Power button to turn on the MC67.

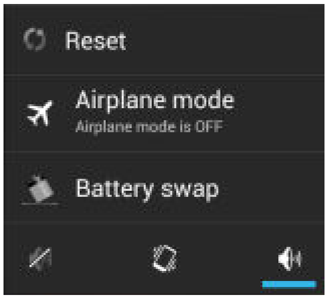
The splash screen displays for about a minute as the MC67 initializes its flash file system.

Replacing the Battery

Procedure:

1. If the MC67 is in a cradle, remove it before performing a Safe Battery Swap.
2. Unclip the handstrap.
3. Press and hold the Power button until the menu appears.

Figure 7: Power Button Menu



Reset

Airplane mode

Airplane mode is OFF

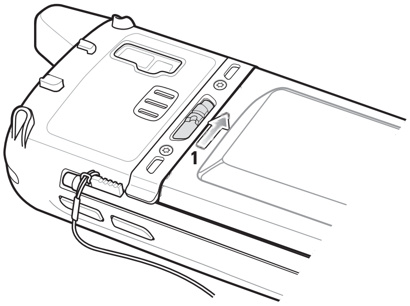
Battery swap

4 Touch **Battery swap**.

5 Wait for the red Data Capture LED to turn off.

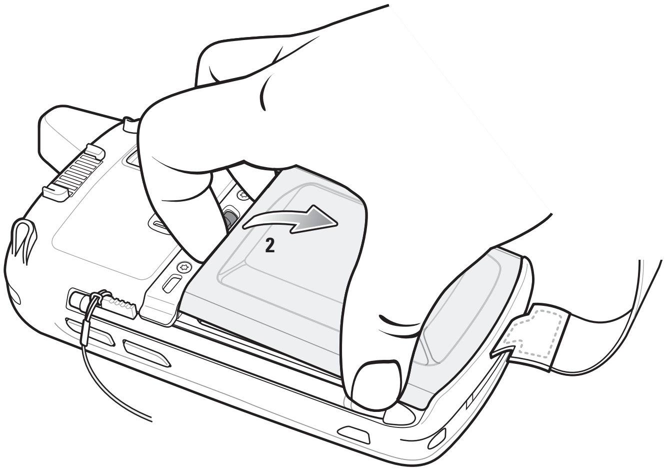
6 Slide the battery latch to the right. The battery ejects slightly.

Figure 8: Slide Latch to the Right



7 Lift the battery from the MC67.

Figure 9: Lift the Battery



8 Insert the replacement battery, bottom first, into the battery compartment in the back of the MC67.

9 Press the battery down until the battery release latch snaps (two clicks) into place.

10 Replace the handstrap.

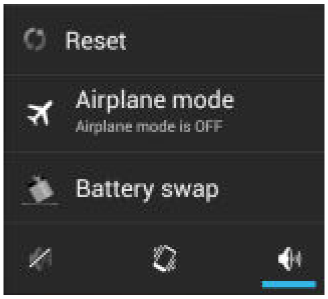
11 Press the Power button to wake the MC67.

Replacing the microSD Card

Procedure:

1. If the MC67 is in a cradle, remove it before performing a Safe Battery Swap.
2. Unclip the handstrap.
3. Press and hold the Power button until the menu appears.
4. Touch **Battery swap**.

   Figure 10: Power Button Menu

5. Wait for the red Data Capture LED to turn off.
6. Remove the battery.
7. Lift the rubber access door.
8. Slide SIM card holder door up to unlock.
9. Lift SIM Card holder door.
10. Lift the microSD card holder door.
11. Remove microSD card from holder.
12. Close microSD card holder door.
13. Close SIM card holder door.
14. Slide SIM card holder door down to lock into place.
15. Close the rubber access door.
16. Insert the battery, bottom first, into the battery compartment in the back of the MC67.
17. Press the battery down until the battery release latch snaps (two clicks) into place.
18. Replace the handstrap.
19. Press the Power button to wake the MC67.
20. If a SIM card is installed, perform a soft reset.

    See *Performing a Soft Reset on page 29*.

Replacing the SIM Card

Procedure:

1. If the MC67 is in a cradle, remove it before performing a Safe Battery Swap.
2. Unclip the handstrap.
3. Press and hold the Power button until the menu appears.
4. Touch **Battery swap**.
5. Wait for the red Data Capture LED to turn off.
6. Remove the battery.
7. Lift the rubber access door.
8. Slide SIM card holder door up to unlock.

9 Lift the SIM Card holder door.
10 Remove SIM card from holder.
11 Close SIM card holder door.
12 Slide SIM card holder door down to lock into place.
13 Close the rubber access door.
14 Insert the battery, bottom first, into the battery compartment in the back of the MC67.
15 Press the battery down until the battery release latch snaps (two clicks) into place.
16 Replace the handstrap.
17 Perform a soft reset.

See *Performing a Soft Reset on page 29*.

Resetting the MC67

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.

Procedure:

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

Performing a Hard Reset

⚠ **Caution:** Performing a hard reset with a SIM card installed in the MC67 may cause damage or data corruption to the SIM card.

Perform a hard reset if the MC67 stops responding.

Procedure:

1 On a numeric or DSD keypad, simultaneously press the Power button and the 1 and 9 keys.
2 On a alpha-numeric keypad, simultaneously press the Power button and the W and C keys.
3 The MC67 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.

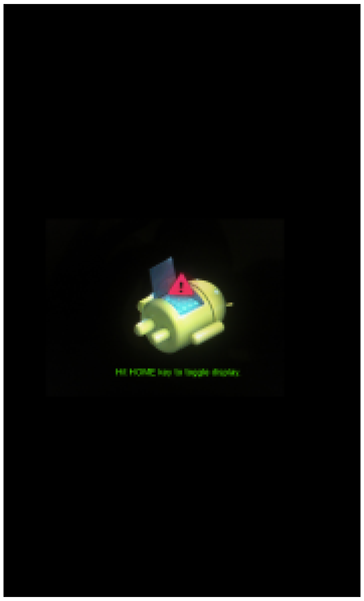
Before performing an Enterprise Reset, copy all applications and the key remap configuration file that you want to persist after the reset into the `/enterprise/usr/persist` folder.

Procedure:

1 Download the Enterprise Reset file from the Motorola Solutions Support Central web site.
2 Copy the `M67N0JXXVRExxxxxxx.zip` file to the root directory of the microSD card. See *USB Communication on page 61*.

3 Press and hold the Power button until the menu appears.
4 Touch **Reset**.
5 Touch **OK**. The MC67 resets.
6 Press and hold the Right Scan/Action button.
7 When the Recovery Mode screen appears, release the button.

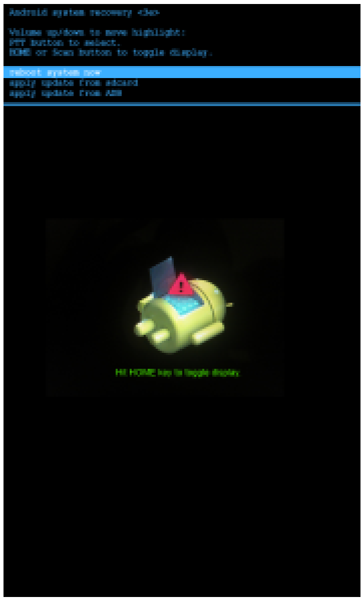
Figure 11: Recovery Mode Screen



```
Hit HOME key to toggle display.
```

8 Touch ⌂. The System Recovery screen appears.

Figure 12: System Recovery Screen



```
Android system recovery <3e>

Volume up/down to move highlight:
PTT button to select.
HOME or Scan button to toggle display.

reboot system now
apply update from sdcard
apply update from ADB

Hit HOME key to toggle display.
```

9 Press the Up and Down Volume buttons to navigate to the **apply update from sdcard** option.
10 Press the Right Scan/Action button.
11 Press the Up and Down Volume buttons to navigate to the `M67N0JXXVRExxxxx.zip` file.
12 Press the Right Scan/Action button. The Enterprise Reset occurs and then the device resets.

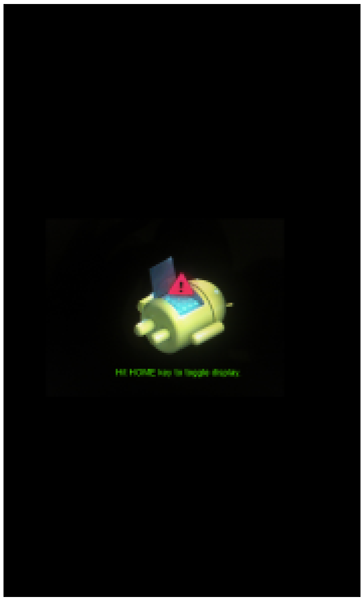
Performing a Factory Reset

A Factory Reset erases all data in the /cache, /data and /enterprise partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See *Updating the System on page 126* for more information.

Procedure:

1. Download the Enterprise Reset file from the Motorola Solutions Support Central web site.
2. Copy the `M67N0JXXVRFxxxxxxx.zip` file to the root directory of the microSD card. See *USB Communication on page 61*.
3. Press and hold the Power button until the menu appears.
4. Touch **Reset**.
5. Touch **OK**. The device resets.
6. Press and hold the Right Scan/Action button.
7. When the Recovery Mode screen appears release the Right Scan/Action button.

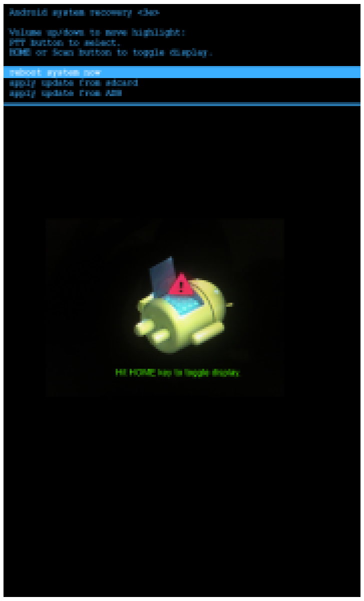
Figure 13: Recovery Mode Screen



Hit HOME key to toggle display.

8. Touch ⌂.

Figure 14: System Recovery Screen



```
Android system recovery <3e>

Volume up/down to move highlight:
PTT button to select.
HOME or Scan button to toggle display.

reboot system now
apply update from sdcard
apply update from ADB
```

Hit HOME key to toggle display.

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

10 Press the Right Scan/Action button.

11 Press the Up and Down volume buttons to navigate to the `M67N0JXXVRFxxxxxxx.zip` file.

12 Press the Right Scan/Action button. The Factory Reset occurs and then the device resets.

Chapter 2

Accessories

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

Accessories

This table lists the accessories available for the MC67.

Table 2: MC67 Accessories

Accessory	Part Number	Description
Cradles		
Single Slot USB Cradle	CRD5500-1000UR	Charges the MC67 main battery and a spare battery. Synchronizes the MC67 with a host computer through a USB connection.
Four Slot Charge Only Cradle	CRD5501-4000CR	Charges up to four MC67 devices.
Four Slot Ethernet Cradle	CRD5501-4000ER	Charges up to four MC67 devices and connects the MC67 with an Ethernet network. CRD5501-4000ER provides up to a maximum of 1 Gbps.
Vehicle Cradle	VCD5500-1001R	Installs in a vehicle and charges the MC67 main battery.
Vehicle Holder	VCH5500-1000R	Provides an alternative mounting solution for the MC67 in a vehicle. Requires the Auto Charge cable for charging the MC67 battery.
Chargers		
Four Slot Spare Battery Charger	SAC5500-4000CR	Charges up to four MC67 battery packs.
Power Supply	PWRS-14000-249R	Provides power to the MC67 using the USB Charging Cable or Charge Only Cable.
Power Supply	PWRS-14000-148R	Provides power to the Single Slot USB cradle and Four Slot Spare Battery Charger.
Power Supply	PWRS-14000-241R	Provides power to the Four Slot Charge Only cradle or Four Slot Ethernet cradles.
USB Charging Cable	25-108022-03R	Provides power to the MC67 and USB communication with a host computer.

Table continued…

Accessory	Part Number	Description
Charge Only Cable	25-112560-01R	Connects to a power supply to provide power to the MC67.
Auto Charge Cable	VCA5500-01R	Charges the MC67 using a vehicle's cigarette lighter.
DC Cable	50-16002-029R	Provides power from the power supply to the Four Slot cradles.
Miscellaneous		
Spare 3600 mAh lithium-ion battery	BTRY-MC55EAB02 BTRY-MC55EAB02-10 BTRY-MC55EAB02-50	Replacement 3600 mAh battery. (10-pack) (50-pack)
DEX Cable	25-127558-01R	For use with electronic data exchange For example, vending machines.
USB Client Communication Cable	25-68596-01R	Provides USB communication between the Single Slot USB Cradle and a host computer.
Printer Cable	25-136283-01R	Provides connection to a Monarch/Paxar Serial printer.
Magnetic Stripe Reader	MSR5500-100R	Captures data from magnetic stripe cards.
Mobile Payment Module	MPM-100R	Adds payment processing capabilities to the MC67 using Bluetooth for credit, debit, loyalty and gift magnetic stripe cards, Chip and PIN-based cards or NFC payments via a mobile phone.
Belt Mounted Rigid Holster	SG-MC5511110-01R	Clips onto belt to hold the MC67 when not in use.
Fabric Holster	SG-MC5521110-01R	Soft holder for added protection.
Stylus	KT-119150-03R KT-119150-50R	Replacement stylus (3-pack). Replacement stylus (50-pack).
Spring Loaded Stylus	STYLUS-00001-10R	Optional spring loaded stylus (10-pack).
Stylus with Tether	Stylus-00003-03R Stylus-00003-50R	Spare stylus with tether (3-pack). (50-pack).
Spare Tether	KT-122621-03R KT-122621-50R	Replacement tether (3-pack). (50-pack).
Handstrap	SG-MC5523341-03R	Replacement handstrap with pin
Wall Mounting Kit	KT-136648-01R	Use for wall mounting the four slot cradles.
Screen Protector	KT-137521-03R	Package of 3 screen protectors.

Single Slot USB Cradle

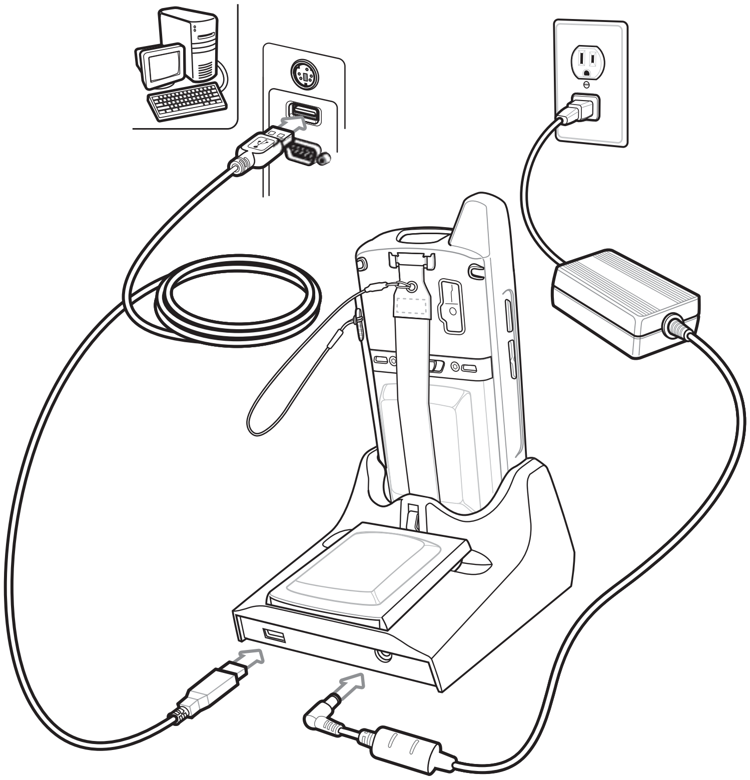
This section describes how to set up and use a Single Slot USB cradle with the MC67. For USB communication setup procedures see *USB Communication on page 61*.

The Single Slot USB cradle:

- Provides 5.4 VDC power for operating the MC67.
- Synchronizes information between the MC67 and a host computer. See *USB Communication on page 61* for information on setting up a partnership between the MC67 and a host computer.
- Charges the MC67's battery.
- Charges a spare battery.

Setup

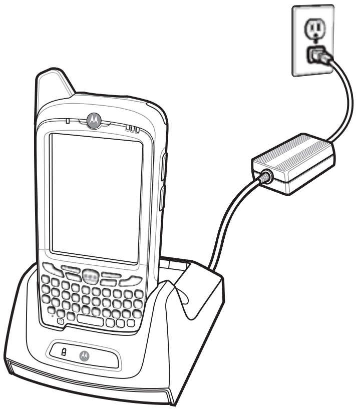
Figure 15: Single Slot USB Cradle Power and USB Connections



Charging the MC67 Battery

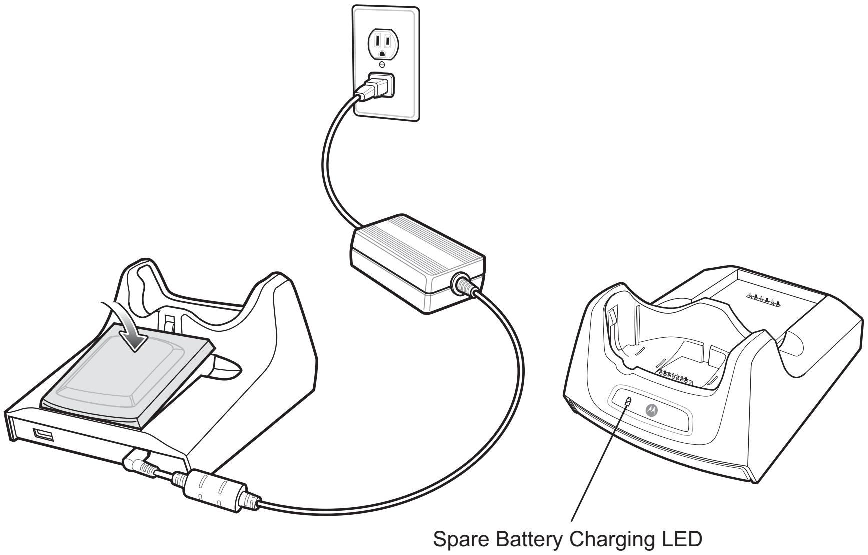
Connect the cradle to power. Insert the MC67 into the MC67 slot to begin charging.

Figure 16: MC67 Battery Charging



Charging the Spare Battery

Figure 17: Spare Battery Charging



Battery Charging

The Single Slot USB cradle charges the MC67's main battery and a spare battery simultaneously.

The MC67's Charging/Battery Status LED indicates the status of the battery charging in the MC67. See *LED Charging Indicators on page 26* for charging status indications.

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

The 3600 mAh battery fully charges in approximately six hours.

Table 3: Spare Battery LED Charging Indicators

Spare Battery LED (on cradle)	Indication
Slow Blinking Amber	Spare battery is charging.

Table continued…

Spare Battery LED (on cradle)	Indication
Solid Amber	Spare battery is fully charged.
Fast Blinking Amber	Charging error.
Off	Not charging.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC67.

To accomplish this, for small periods of time, the MC67 or cradle alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 or cradle indicates when charging is disabled due to abnormal temperatures via its LED.

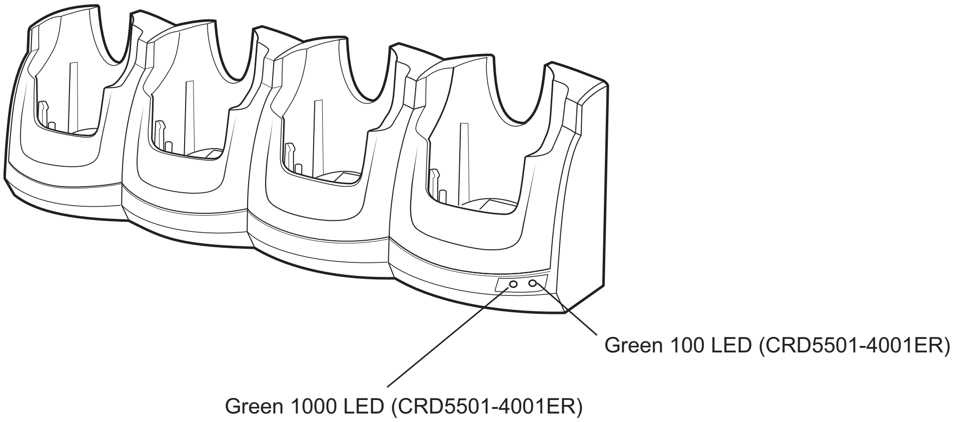
Four Slot Ethernet Cradle

This section describes how to set up and use a Four Slot Ethernet cradle with the MC67.

The Four Slot Ethernet cradle:

- Provides 5.4 VDC power for operating the MC67.
- Connects the MC67 (up to four) to an Ethernet network.
- Simultaneously charges up to four MC67s.

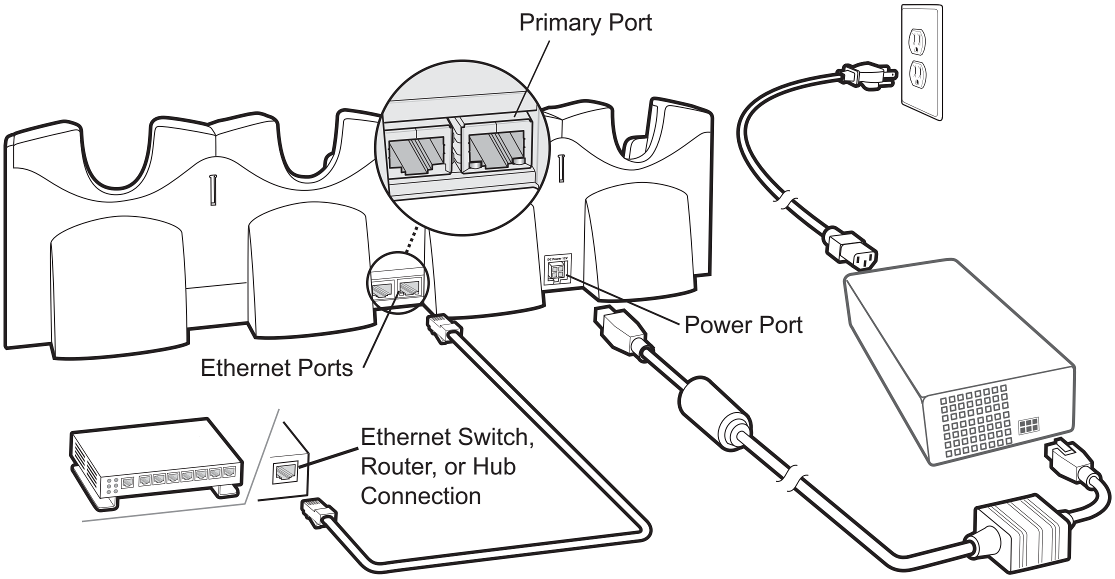
Figure 18: Four Slot Ethernet Cradle


Green 100 LED (CRD5501-4001ER)
Green 1000 LED (CRD5501-4001ER)

CRD5501-4001ER Setup

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

Figure 19: CRD5501-4001ER Four Slot Ethernet Cradle Connection



Daisychaining Ethernet Cradles

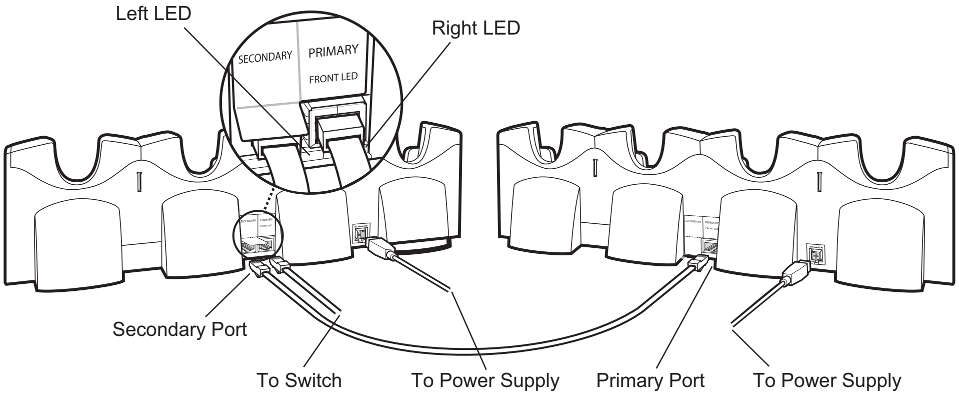
Daisychain up to four Four Slot Ethernet cradles to connect several cradles to an Ethernet network. Use either a straight or crossover cable. Daisy-chaining should not be attempted when the main Ethernet connection to the first cradle is 10 Mbps as throughput issues will almost certainly result.

To daisychain more than Four Slot Ethernet cradles:

Procedure:

1. Connect power to each Four Slot Ethernet cradle.
2. Connect an Ethernet cable to the Primary Port of the first cradle and to the Ethernet switch.
3. On the first Four Slot Ethernet cradle, lift or remove the label flap and connect a second Ethernet cable to the Secondary Port.
4. Connect the other end of the Ethernet cable to the Primary Port of the second Four Slot Ethernet cradle.
5. Connect additional cradles as described in *step 3* and *step 4*.

Figure 20: Daisychaining Four Slot Ethernet Cradles



LED Indicators (CRD5501-4001ER)

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

Table 4: CRD5501-4001ER LED Indicators

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

Ethernet Settings

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The MC67 includes Ethernet cradle drivers. After inserting the MC67, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch **Ethernet**.

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

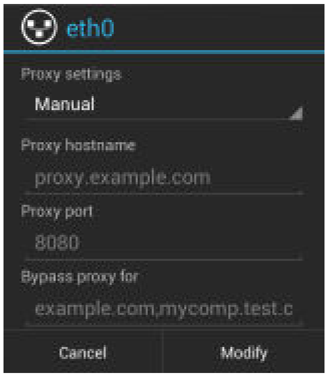
5 Place the MC67 into the Ethernet cradle slot.

6 Touch **Ethernet**.

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

8 Touch **Modify Proxy**.

Figure 21: Ethernet Proxy Settings



eth0

Proxy settings: Manual

Proxy hostname: proxy.example.com

Proxy port: 8080

Bypass proxy for: example.com,mycomp.test.c

9 Touch the **Proxity settings** drop-down list and select **Manual**.

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

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

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

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

13 Touch **Mofidy**.

14 Touch ⌂.

Configuring Ethernet Static IP Address

The MC67 includes Ethernet cradle drivers. After inserting the MC67, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ☰.

3 Touch **Ethernet**.

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

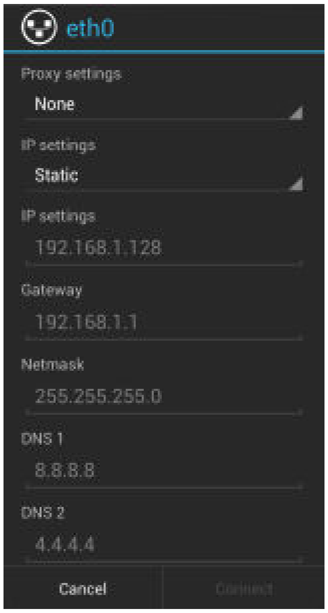
5 Place the MC67 into the Ethernet cradle slot.

6 Touch **Ethernet**.

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

8 Touch **Disconnect**.

Figure 22: Ethernet Proxy Settings



eth0

Proxy settings
None

IP settings
Static

IP settings
192.168.1.128

Gateway
192.168.1.1

Netmask
255.255.255.0

DNS 1
8.8.8.8

DNS 2
4.4.4.4

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

10

11 Touch the **IP setting** drop-down list and select **Static**.

12 In the **IP adress** field, enter the proxy server address.

13 If required, in the **Gateway** text box, enter a gateway address for the device.

14 If required, in the **Network prefix length** text box, enter a the prefix length.

15 If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.

16 If required, in the **DNS 2** text box, enter a DNS address.

17 Touch **Connect**.

18 Touch ⌂.

Charging the MC67

Insert the MC67 into a slot to begin charging. The MC67’s Charging/Battery Status LED shows the status of the battery charging in the MC67.

The 3600 mAh battery fully charges in approximately six hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC67.

To accomplish this, for small periods of time, the MC67 alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 indicates when charging is disabled due to abnormal temperatures via its LED.

Four Slot Charge Only Cradle

This section describes how to set up and use a Four Slot Charge Only cradle with the MC67.

The Four Slot Charge Only cradle:

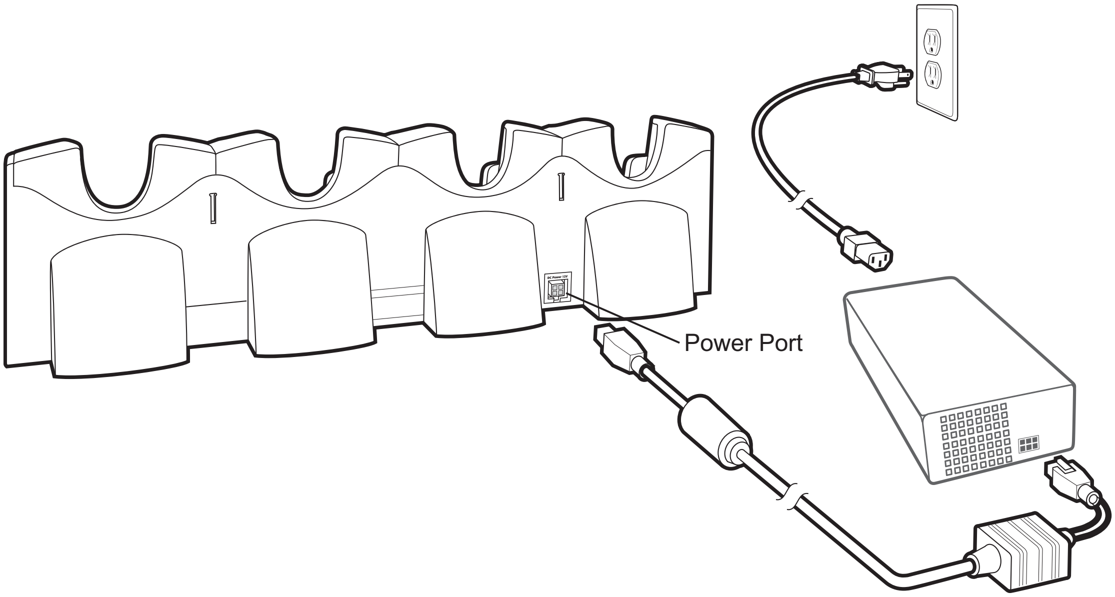
- Provides 5.4 VDC power for operating the MC67.
- Simultaneously charges up to four MC67s.

The user cannot ActiveSync using the Four Slot Charge Only cradle. To ActiveSync with a host computer, use the Single Slot USB cradle.

Setup

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

Figure 23: Four Slot Charge Only Cradle Setup



Charging the MC67

Insert the MC67 into a slot to begin charging. The MC67’s Charging/Battery Status LED shows the status of the battery charging in the MC67.

The 3600 mAh battery fully charges in approximately six hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC67.

To accomplish this, for small periods of time, the MC67 alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 indicates when charging is disabled due to abnormal temperatures via its LED.

Wall Mount Bracket

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

Procedure:

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

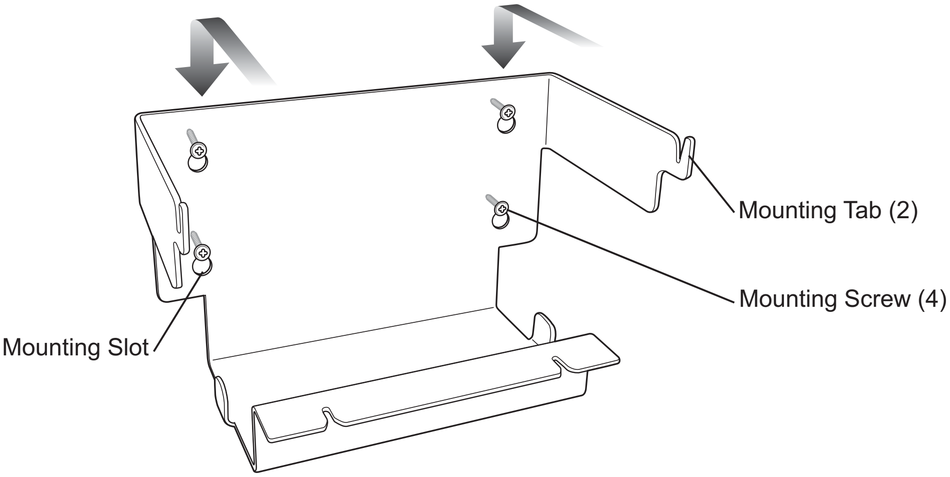
> **Note:** Use fasteners appropriate for the type of wall and the Wall Mount Bracket mounting slots. The Wall Mount Bracket mounting slots are designed for a fastener with a #8 pan head. Fasteners must be able to hold a minimum of 4.9 Kg (10.8 lbs).

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

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

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

Figure 24: Wall Mount Bracket



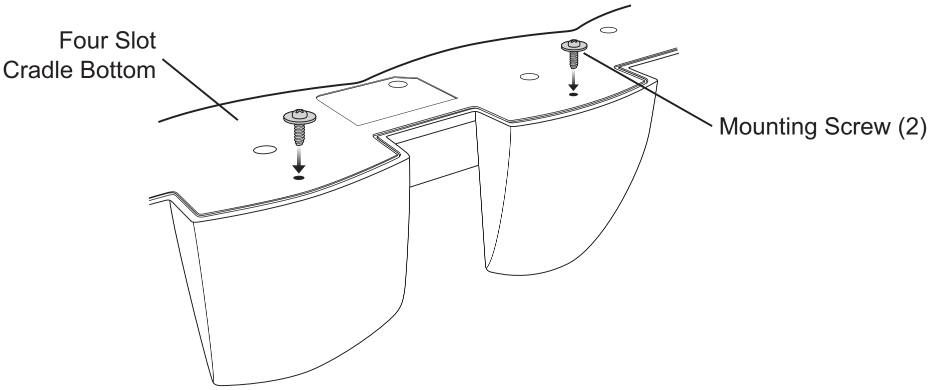
Mounting a Four Slot Cradle

To mount a four slot cradle:

Procedure:

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

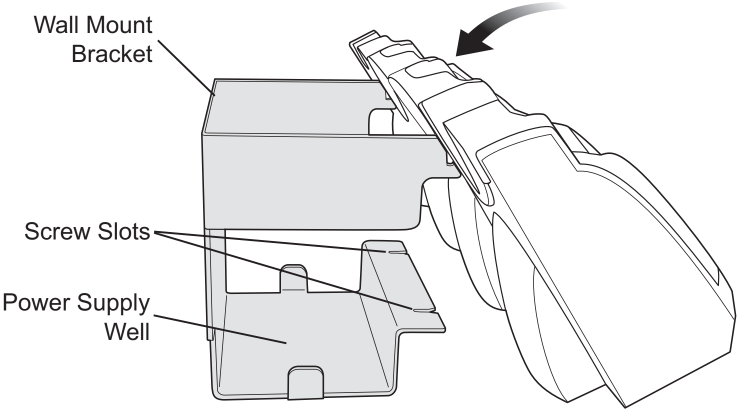
Figure 25: Cradle Mounting Screws



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

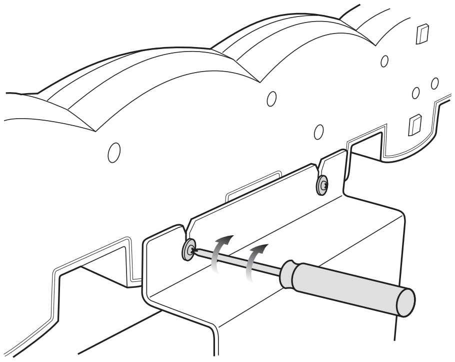
3 Swing the four slot cradle down onto the mounting bracket and align the mounting screws so that they fit into the screw slots.

Figure 26: Wall Mount Bracket



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

Figure 27: Mounting Screws



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

VCD5500 Vehicle Cradle

This section describes how to set up and use a VCD5500 vehicle cradle with the MC67.

Once installed in a vehicle, the cradle:

- holds the MC67 securely in place
- provides power for operating the MC67
- re-charges the battery in the MC67

Requirements

For mounting:

- four #8-32 self-locking nuts
- four #8 washers
- a drill with a #6 drill bit (.204”)

For power connection:

- power input cable (optional), p/n 25-61987-01R or 25-128974-01R
- UL Listed in-line fuse rated 250V, 5A (included), must be used if not connecting to vehicle’s fuse panel
- in-line fuse holder (included), must be used if not connecting to vehicle’s fuse panel

Connector Pin-Outs

Figure 28: VCD5500 Power Connection

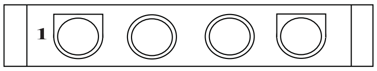


Table 5: Power Input Cable

Pin	Signal
1	Chassis ground (Black Wire)
2	Chassis ground (Bare Wire)
3	V+ (Red Wire)
4	V+ (Red Wire)

Caution: ROAD SAFETY - Do not use the MC67 while driving. Park the vehicle first. Always ensure the MC67 is fully inserted into the cradle. Do not place it on the seat or where it can break loose in a collision or sudden stop. Lack of proper insertion may result in property damage or personal injury. Motorola, Inc. is not responsible for any loss resulting from the use of the products while driving. Remember: Safety comes first.

Mounting the Cradle

Caution: Only mount the Vehicle Cradle in a vertical position with the release level at the top or in a horizontal position with the MC67 display facing up. Never mount the vehicle cradle on the side or upside down or on a wall that can be subject to impact or collision of greater than 40Gs, in accordance with SAE J1455 Section 4.10.3.5

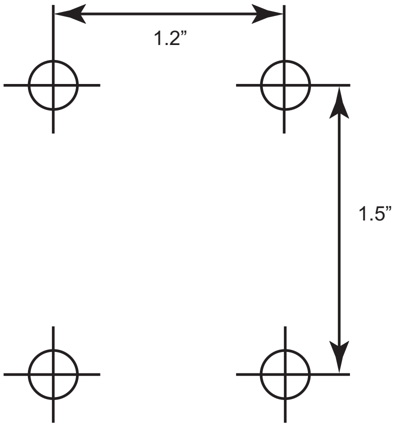
Procedure:

1 Select a mounting location for the cradle. It should be flat, and must provide adequate support for the cradle.

Note: If using the GPS functionality of the MC67, ensure that the vehicle cradle is positioned so that the MC67 has a clear unobstructed view of the sky.

2 Prepare the mounting surface to accept four #8-32 studs, using the mounting template below. Drill four holes with a #6 drill bit.

Figure 29: Vehicle Cradle Mounting Template



3 Position the cradle on the mounting surface.

4 Fasten it using four #8 washers and four #8-32 self-locking nuts.

Caution: Do not install a VCD5500 Vehicle Cradle on or near an air bag cover plate or within an aerobic zone. Also, do not install it in a location that affects vehicle safety or driveability.

Power Connection

Please read all of the following instructions before beginning.

Warning: A properly trained technician must perform the power connection. Improper connection can damage your vehicle, cradle or MC67. Refer to the vehicle’s Owner’s Manual for instructions for removing power.

To connect the cradle to power:

Caution: When setting up connection for this cradle, only use the power input cable, part number 25-61987-01R or 25-128974-01R.

Procedure:

1 Locate the vehicle power source.

Note: The ideal location for connecting the vehicle cradle power input cable would be an accessory output in your vehicle’s fuse panel. The vehicle cradle should be added to a circuit with a maximum load capacity for the cradle and the original circuit. Refer to the vehicle’s Owner’s Manual for identification of the circuit. If a fused output is not available, the vehicle cradle must be installed with the provided in-line fuse holder and UL Listed 5A fuse. The fuse protects the vehicle from an electrical short on the power line to the cradle.

To use the cradle to charge the MC67 and spare battery, when the vehicle’s ignition is off, connect the cradle to unswitched power.

2 Route the power input cable from the cradle’s power port to the connection point for the vehicle’s power source.

Caution: The means of routing and securing the power input cable from the cradle through to the vehicle power source is extremely important. Hazards associated with improper wiring can be severe. To avoid unintentional contact between the wire and any sharp edges, provide the cable with proper bushings and clamping where it passes through openings. If the wire is subjected to sharp surfaces and excess engine vibration, the wiring harness insulation can wear away, causing a short between the bare wire and chassis. This can start a fire.

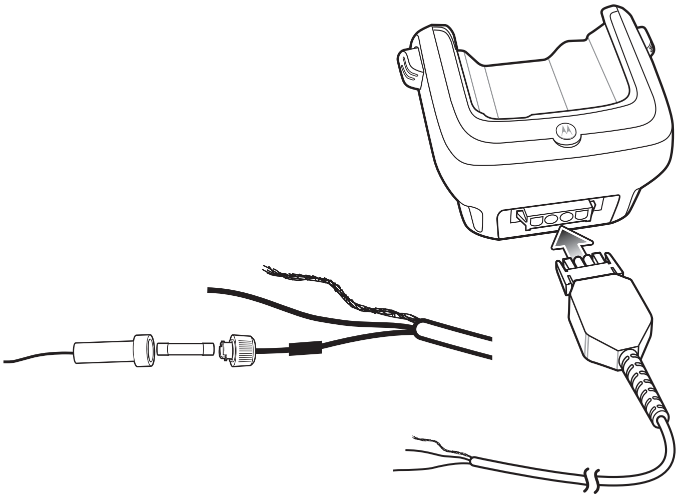
To avoid any mishaps, all wiring should be routed away from moving parts, high temperature areas and any contaminants.

3 When using the supplied in-line fuse holder (which must be used if not connecting to vehicle's fuse panel):

a Ensure the fuse holder contains a 5A UL Listed slow-blow fuse.

b Splice the fuse holder to the end of the red V+ wire, as shown above. Make the distance from the fuse to the power connection point as short as possible.

Figure 30: Vehicle Cradle Power Connection



4 Prepare the cable termination.

a Red wire: connect to a +12/24 V vehicle power source.

b Black wire and Shield wire: connect to vehicle ground wire or chassis ground.

Note: How the cable terminates depends on the vehicle. If the vehicle has a power output connector, then you must attach a mating connector to the end of the power cable. You may be able to connect to a fuse panel with a simple blade terminal or commercially available connector. Consult the vehicle Owner's Manual for information on how to access the power supply in the vehicle.

5 Connect the power input cable into the power port on the cradle.

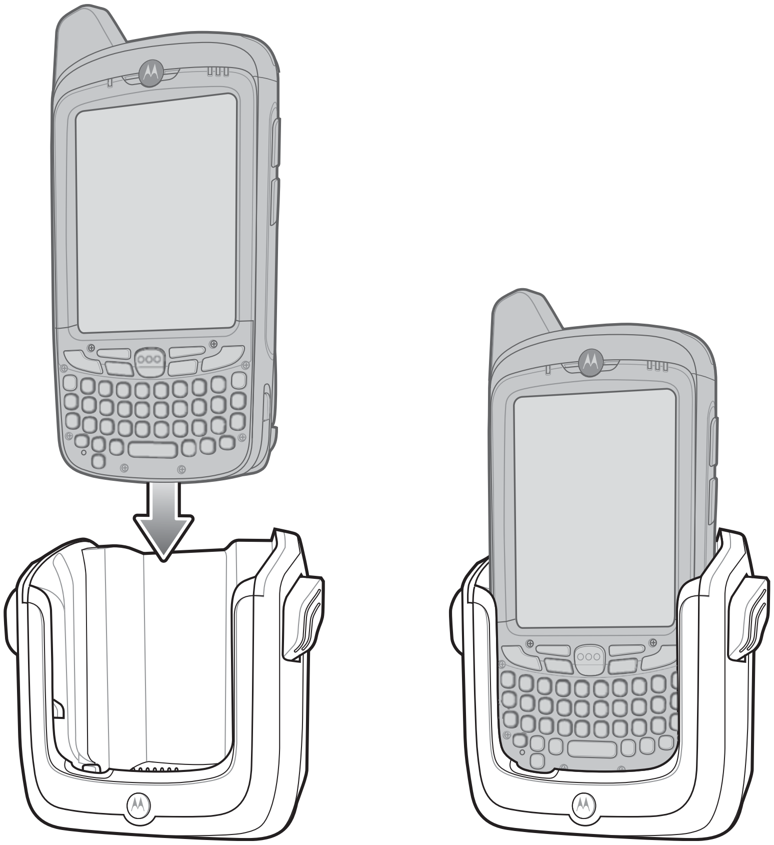
Post requisites: To see if the cradle has power, insert the MC67. The Charging LED on the MC67 blinks slowly to indicate charging and turns solid amber when the battery is completely charged. See *LED Charging Indicators on page 26* for other indications.

Charging the MC67 Battery

Procedure:

1 Insert the MC67 into the vehicle cradle to begin charging.

Figure 31: MC67 Battery Charging



2 Press the MC67 down to ensure it is seated properly.

A click indicates that the MC67 button release locking mechanism is enabled and the MC67 is locked in place.

⚠ **Caution:** Ensure the MC67 is fully inserted in the cradle. Lack of proper insertion may result in property damage or personal injury. Motorola is not responsible for any loss resulting from the use of the products while driving.

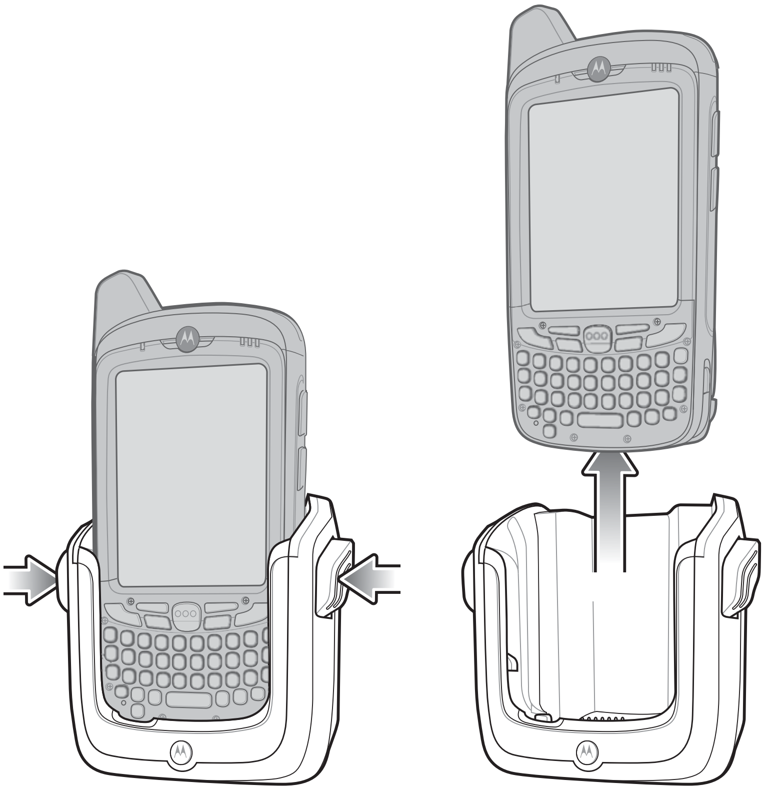
Removing the MC67

Procedure:

1 Press the release levers on the cradle.

2 Pull the MC67 up and out of the cradle.

Figure 32: Removing the MC67



Charging the MC67

Insert the MC67 into a slot to begin charging. The MC67's Charging/Battery Status LED shows the status of the battery charging in the MC67.

The 3600 mAh battery fully charges in approximately six hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC67.

To accomplish this, for small periods of time, the MC67 alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 indicates when charging is disabled due to abnormal temperatures via its LED.

Four Slot Battery Charger

This section describes how to use the Four Slot Battery Charger to charge up to four MC67 spare batteries.

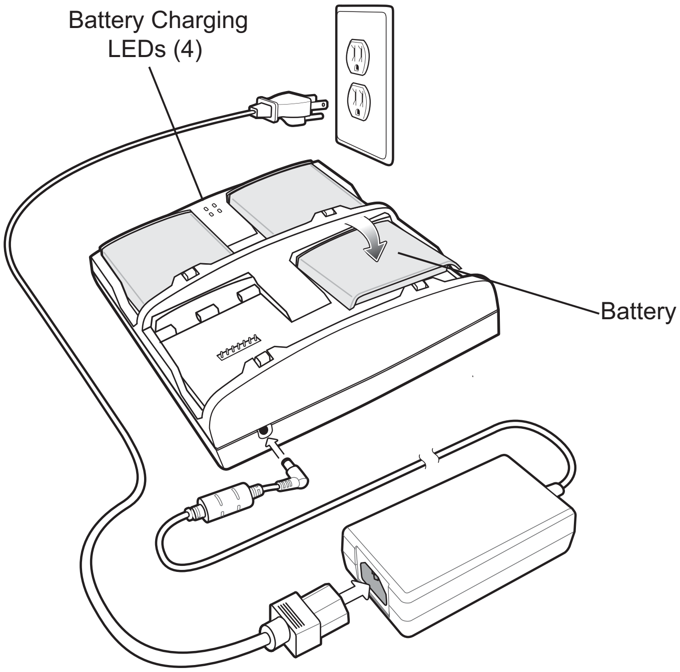
Spare Battery Charging

Procedure:

1 Connect the charger to a power source.

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

Figure 33: Four Slot Battery Charger Setup



Battery Charging Indicators

An amber LED is provided for each battery charging well. See *Table 6: Spare Battery LED Charging Indicators on page 49* for charging status indications. The 3600 mAh battery charges in approximately six hours.

Charging Temperature

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 its LED. See *Table 6: Spare Battery LED Charging Indicators on page 49*.

Table 6: Spare Battery LED Charging Indicators

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

Cables

This section describes how to set up and use the cables. The cables are available with a variety of connection capabilities.

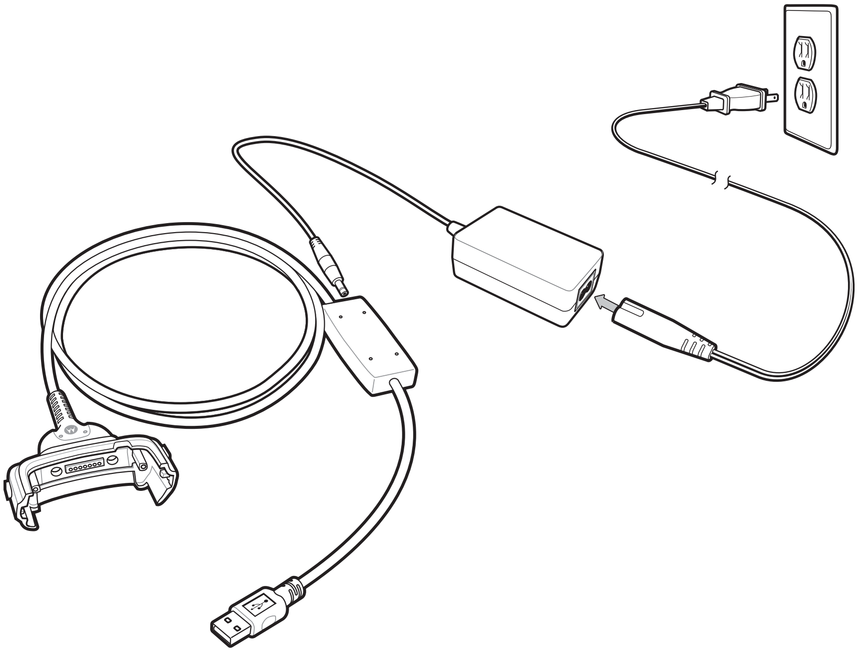
The following communication/charge cables are available:

- USB Charging cable
- Charge Only cable
- Auto Charge cable
- DEX cable.

USB Charging Cable

The USB Charging cable provides the MC67 with operating and charging power when used with the Motorola approved power supply and AC line cord and synchronize information between the MC67 and a host computer.

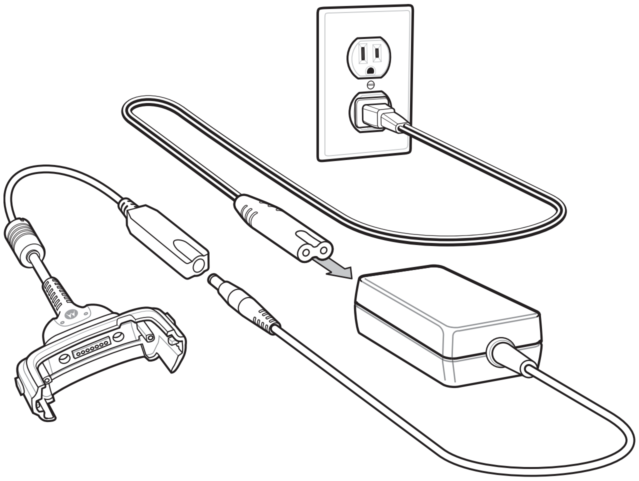
Figure 34: USB Charging Cable Setup



Charge Only Cable

The Charge Only cable provide the MC67 with operating and charging power when used with the Motorola approved power supply.

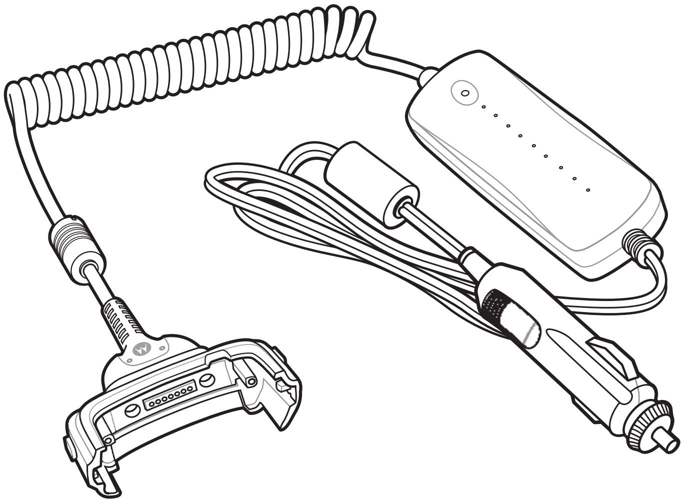
Figure 35: Charge Only Cable Setup



Auto Charge Cable

The Auto Charge cable plugs into a vehicle cigarette lighter and provide the MC67 with operating and charging power.

Figure 36: Auto Charge Cable



Connecting Cables to the MC67

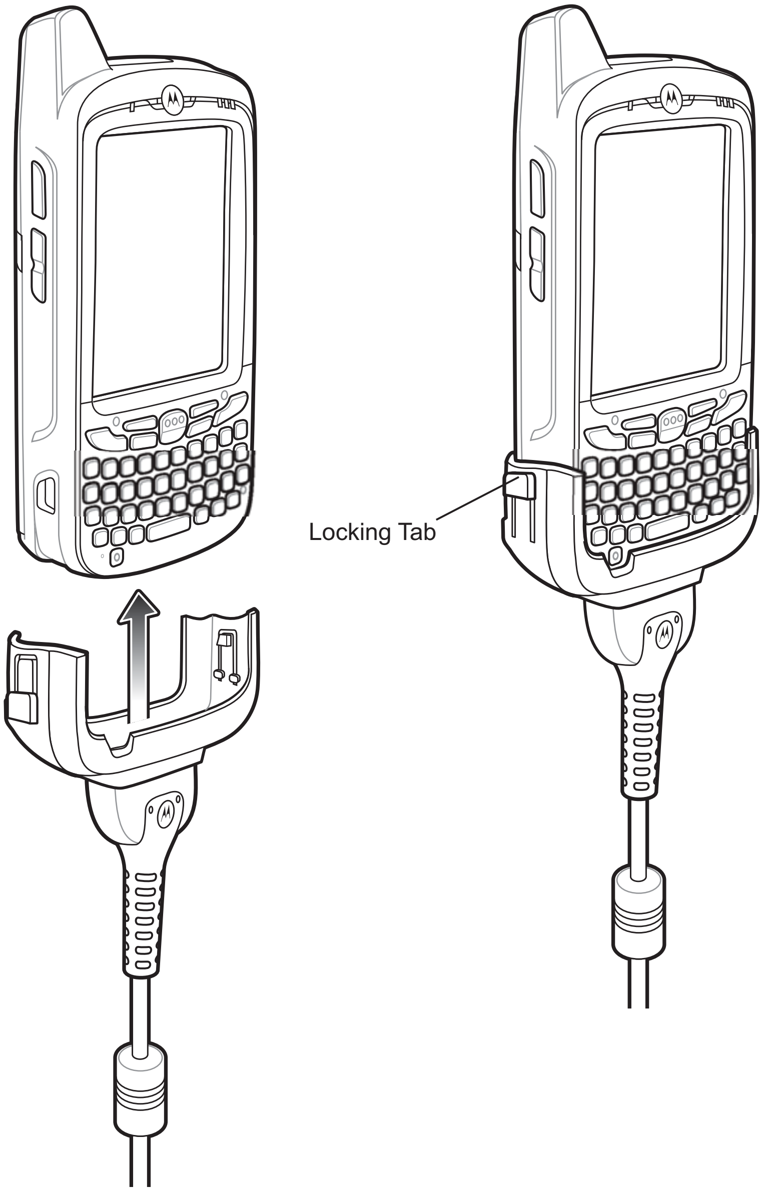
Procedure:

1 If required, connect the cable power input connector to the Motorola approved power source.

2 Slide the bottom of the MC67 into the connector cup end of the cable until the MC67 is firmly seated in the cup.

3 Slide the two locking tabs up until they both lock into position.

Figure 37: Cable Cup Locking Tabs



4 To remove, slide the two locking tab down and remove the cable from the MC67.

Charging the MC67

Insert the MC67 into a slot to begin charging. The MC67's Charging/Battery Status LED shows the status of the battery charging in the MC67.

The 3600 mAh battery fully charges in approximately six hours.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the MC67.

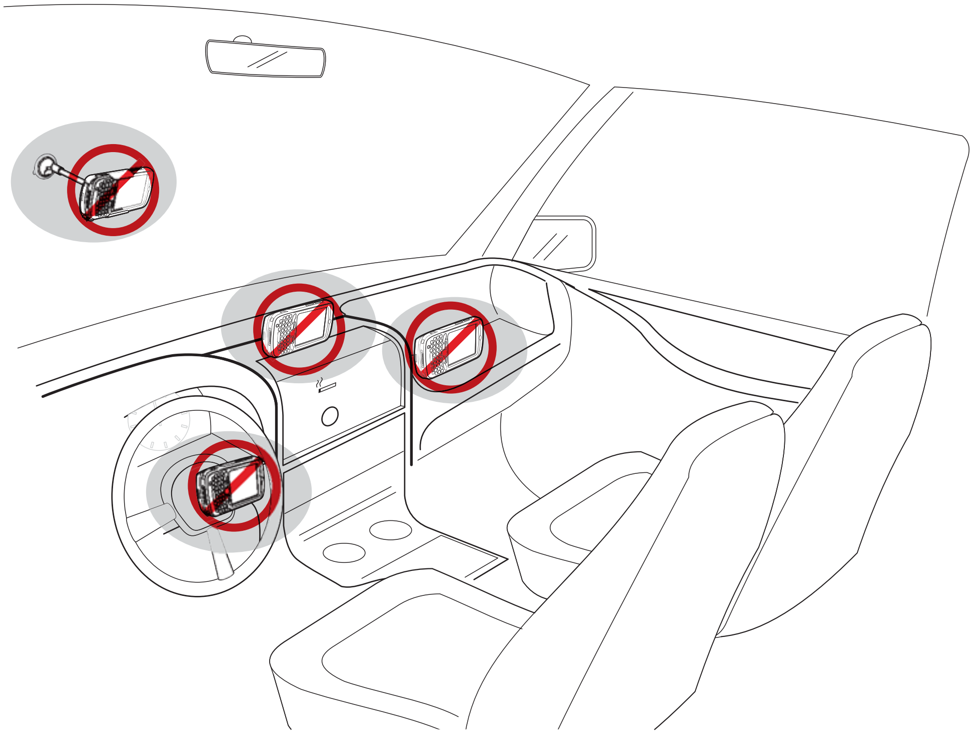
To accomplish this, for small periods of time, the MC67 alternately enables and disables battery charging to keep the battery at acceptable temperatures. The MC67 indicates when charging is disabled due to abnormal temperatures via its LED.

Vehicle Holder

Warning: Some countries prohibit the mounting of any electronic device in any location on the vehicle dashboard and windshield. Be sure to check your local laws acceptable mounting areas before installing the auto mounting kit.

Installation Reminders

Figure 38: Vehicle Holder Mounting



- Do not mount the vehicle holder where it will obscure the driver’s view of the road.
- Do not mount the vehicle holder near the driver seat air bag deployment area.
- Do not place the MC67 on top of the dashboard or anywhere without securing it in the vehicle holder.
- Do not mount the vehicle holder near the passenger seat air bag deployment area.
- Install the vehicle holder on the surface of your vehicle that is reasonably flat and free of dirt and oil.

Device Mounting Precautions

- Some countries prohibit the mounting of any electronic device in any location on the vehicle dashboard. Be sure to check your local laws acceptable mounting areas before installing the vehicle holder.
- The heating and cooling cycle of a vehicle’s interior will in some cases loosen the adhesion of the suction cup. Check the vacuum seal of the vehicle mount kit for adequate adhesion each time you use the unit, and reinstall if necessary.
- If the vehicle holder has problems staying on, clean the plastic suction cup with alcohol, then reinstall.

Installation

Install the vehicle mount on the surface of your vehicle that is reasonably flat and free of dirt and oil. Clean the mounting surface with a glass cleaner and a clean cotton cloth. Install the vehicle mount on the windshield or other flat car surface using the supplied mounting disc.

Assembly

Procedure:

1 Insert the vehicle holder’s cradle plate to the holes on the back of the cradle.

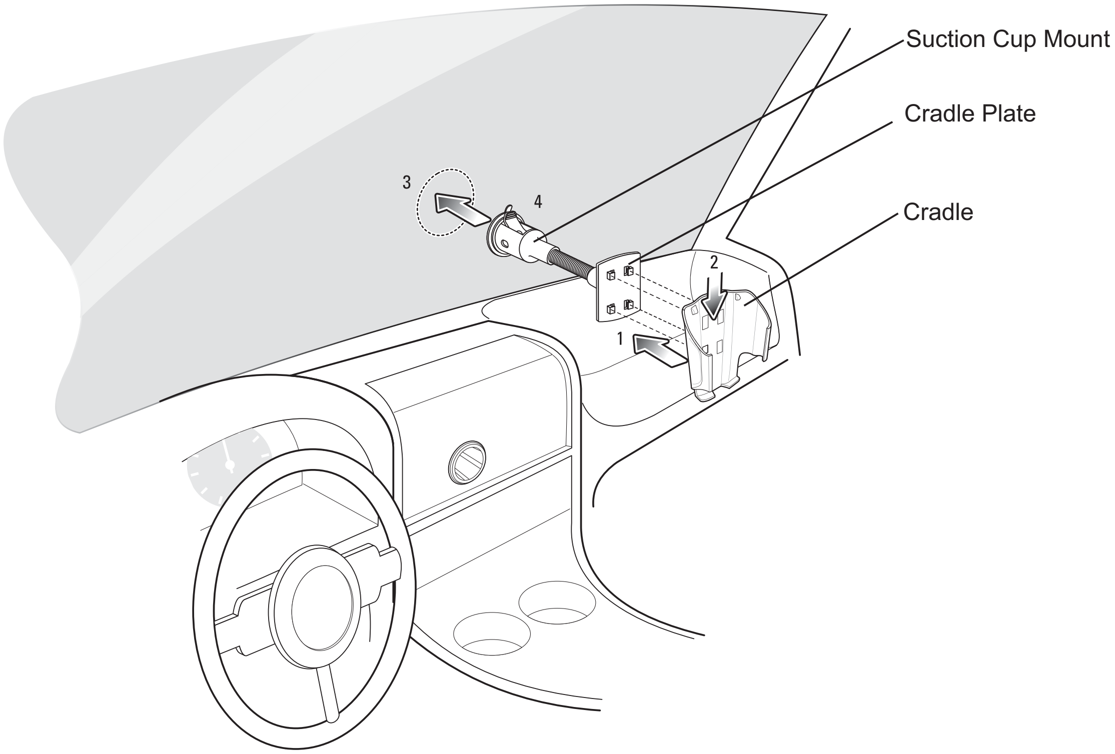
2 Push the cradle down until both parts are engaged.

Windshield Installation

Procedure:

1 Fix the suction cup mount to the selected area with the suction lever facing up.

Figure 39: Windshield Installation

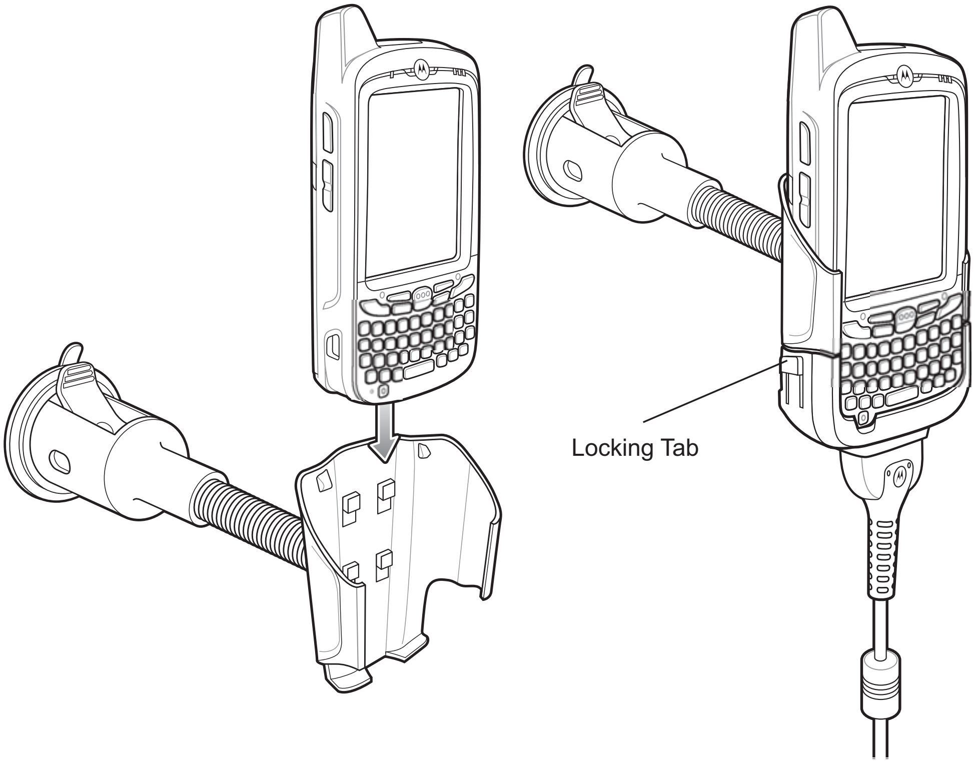


2 Flip the lever down to create a vacuum between the suction cup and the mounting surface.

3 Make sure that the suction bond is strong enough before proceeding to the next step.

4 Slide the MC67 into the cradle.

Figure 40: Insert MC67 into Vehicle Holder



5 Connect the auto charger cable to the MC67 and slide the two locking tabs up to secure the cable cup to the MC67.

6 Connect the other end to the cigarette lighter socket.

Note: Prior to removing the MC67 from the vehicle holder, disconnect the auto-charge cable from the MC67.

The LED indicator on the right side of the touch screen lights up orange during charging.

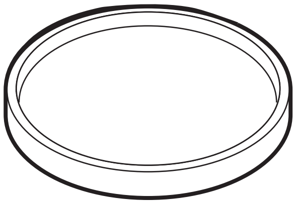
Flat Surface Installation

Procedure:

1 Remove the plastic sheet on the bottom of the mounting disc.

2 Place the disc, sticky side down, on a clean flat surface.

Figure 41: Mounting Disk



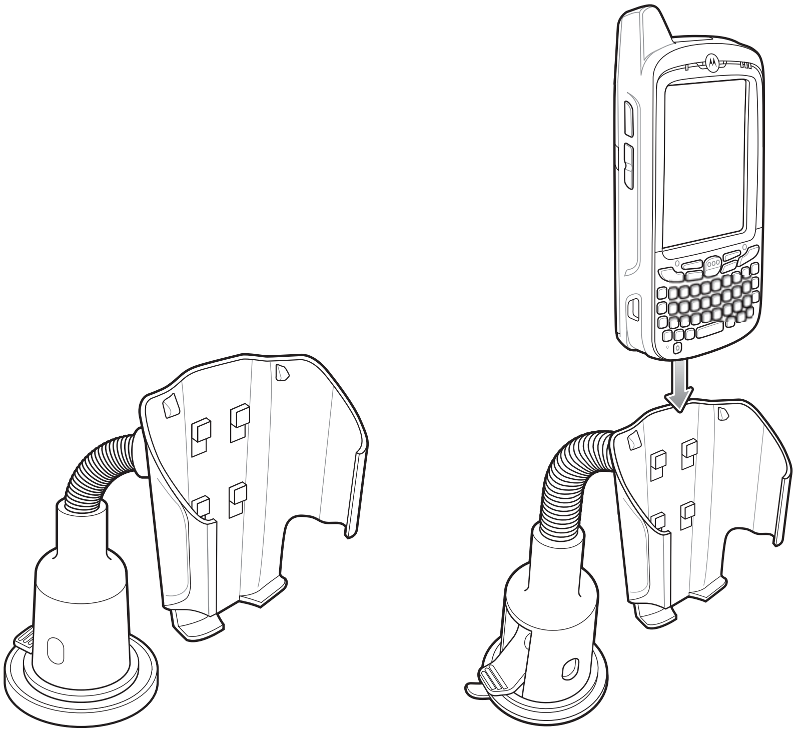
3 Fix the suction cup mount to the disc with the suction lever facing up.

4 Flip the lever down to create a vacuum between the suction cup and the disc.

5 Make sure that the suction bond is strong enough before proceeding to the next step.

6 Slide the MC67 into the cradle.

Figure 42: Vehicle Holder Mounted on Flat Surface



7 Connect the auto charger cable to the MC67 and slide the two locking tabs up to secure the cable cup to the MC67.

8 Connect the other end to the cigarette lighter socket.

The LED indicator on the right side of the touch screen lights up orange during charging.

Handstrap Replacement

Removal

To remove a handstrap from the MC67:

⚠ **Caution:** Close all running applications prior to replacing the handstrap. The backup battery maintains data for up to 15 minutes. If replacement takes longer than 15 minutes data may be lost.

Procedure:

1 If the MC67 is in suspend mode, press the red **Power** button to wake the MC67.

2 Press the red **Power** button.

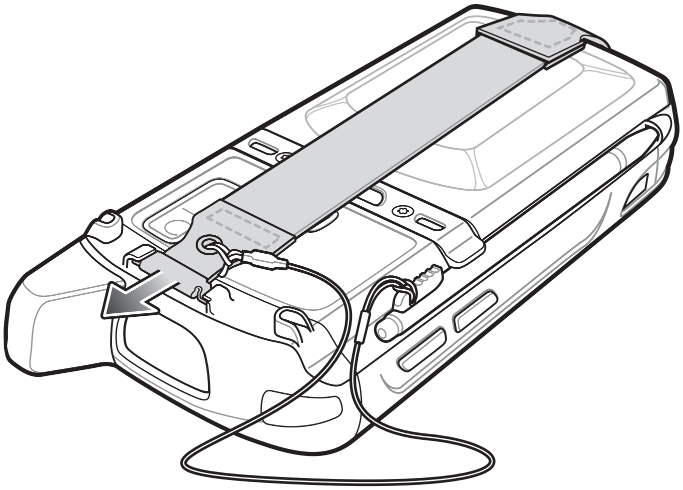
The **Power Action Key** window appears.

3 Tap **Safe Battery Swap**.

The Data Capture LED lights red.

4 When the LED turns off, remove the handstrap.

Figure 43: Handstrap Clip Removal



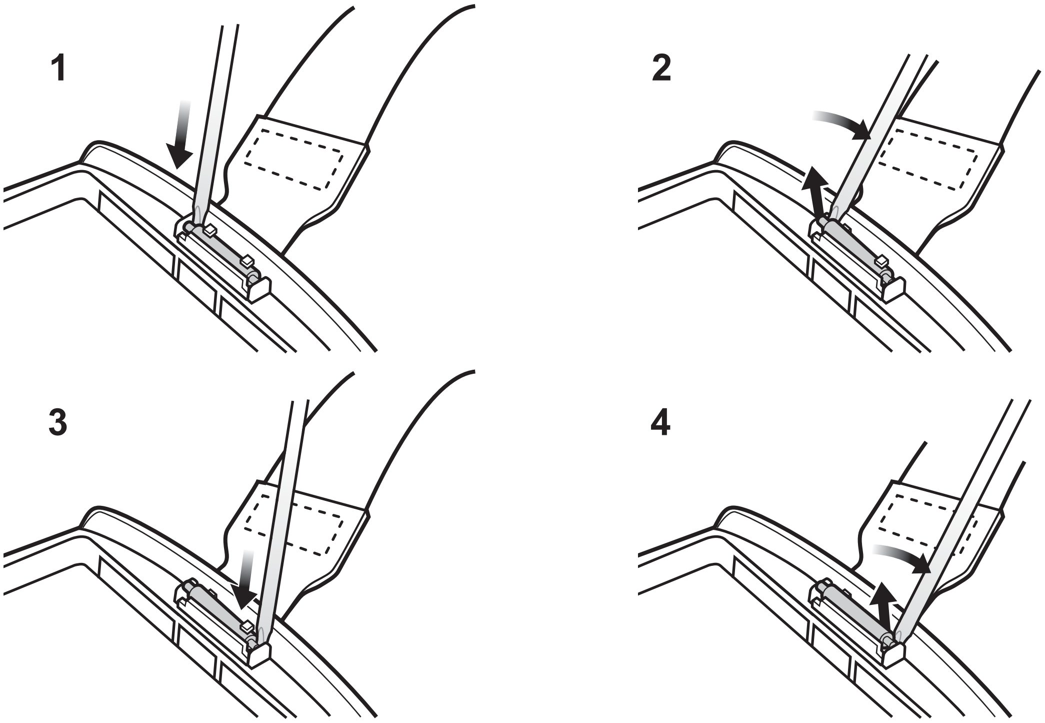
5 Remove the battery.

Caution: When removing handstrap pin, be careful not to damage handstrap mounting area.

6 Using a small flat screwdriver, push the head of the screwdriver between the handstrap pin and the bottom of the housing as shown below.

7 Pry the handstrap and pin up and out of the handstrap mount area.

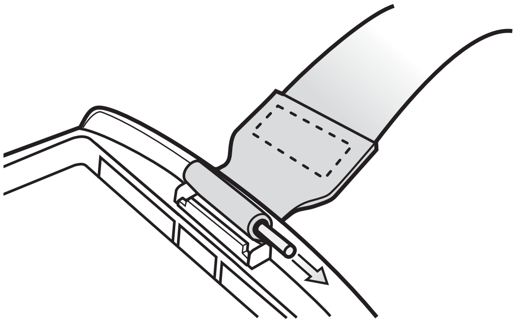
Figure 44: Handstrap and Pin Removal



8 Repeat for the other side of the handstrap.

9 Remove pin from the handstrap.

Figure 45: Pin Removal



10 Pull handstrap through handstrap slot.

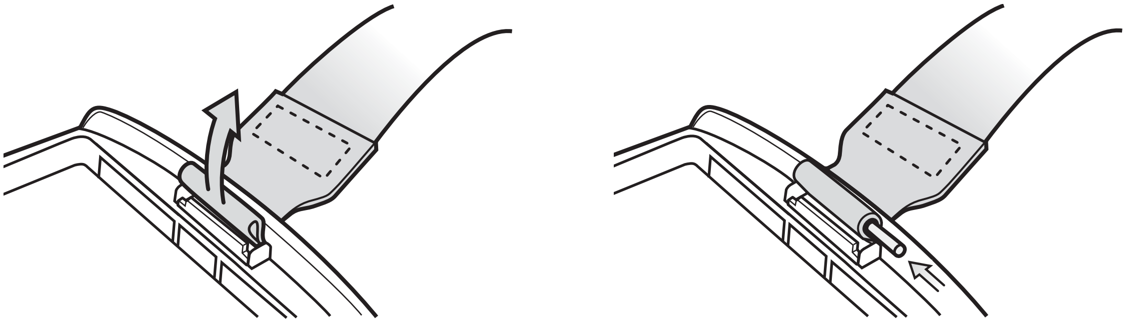
Installation

To install a new handstrap:

Procedure:

1 Feed bottom end of handstrap into handstrap slot on the bottom of the MC67.

Figure 46: Feed Handstrap into Handstrap Slot



2 Slide pin into bottom of handstrap.

3 Center the pin in the handstrap loop.

> **Note:** Handstrap and pin should fit securely into the handstrap mounting area. When pulling on handstrap use enough force to engage pin into place.

4 Pull handstrap so that the pin and bottom of handstrap slide into position in the mounting area.

Figure 47: Pin and handstrap in Mounting Area

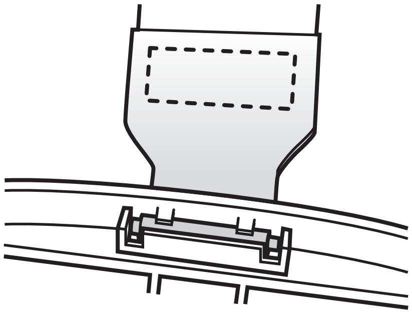
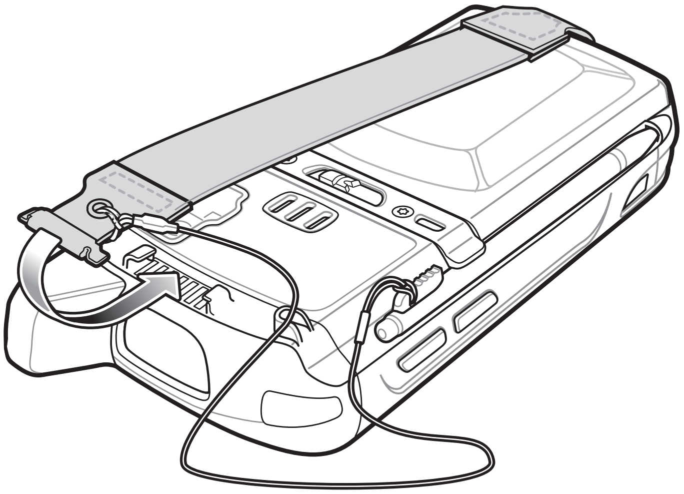


Figure 48: Slide Handstrap and Tether Over Handstrap Mount



5 Slide tether loop over handstrap.

6 Insert the handstrap clip into the slot on the device. Ensure that it is securely in place.

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 MC67 to a host computer using the USB Charging cable or Single Slot USB cradle to transfer files between the MC67 and the host computer.

Caution:

When connecting the MC67 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Note: A microSD card must be installed in the MC67 to transfer files between the MC67 and host computer.

Connecting to the MC67 as a Media Device

Procedure:

1. Connect the USB Charging cable to the MC67 and then to the host computer or place the MC67 into a Single Slot USB cradle that is connected to a host computer.

   Connected as a media device or **Connected as an installer** appears on the Status bar.
2. If **Connected as an installer** appears, pull down the Notification shade and touch **Connected as an installer** and then touch **Media device (MTP)**.
3. On the host computer, open a file explorer application.
4. Locate the **MC67NA** as a portable device.
5. Open the **SD card** folder.
6. Copy or delete files as required.

Connecting to the MC67 as an Installer

Procedure:

1. Connect the USB Charging cable to the MC67 and then to the host computer or place the MC67 into a Single Slot USB cradle that is connected to a host computer.

   Connected as a media device or **Connected as an installer** appears on the Status bar.
2. If **Connected as media device** appears, pull down the Notification shade and touch **Connected as media device** and then touch **Media device (MTP)** to de-select.
3. Touch **Turn on USB Storage**.
4. On the host computer, open a file explorer application.

   The MC67 storage appears as Removable Disk.
5. Locate the MC67 as a devices within Removable Storage.

6. Open the **Removable Disk**.
7. Copy or delete files as required.
8. On the MC67, touch **Turn off USB storage**

Disconnect from the Host Computer

⚠ **Caution:**

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

Procedure:

1. On the host computer, unmount the device.
2. Remove the USB Charging cable from the MC67 or remove the MC67 from the Single Slot USB cradle.

Chapter 4

DataWedge Configuration

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:

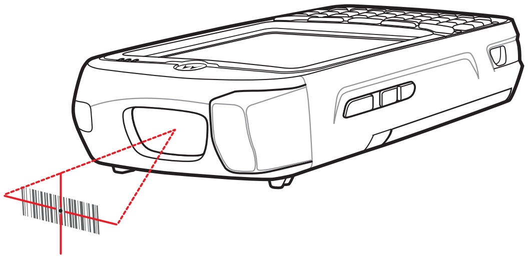
Procedure:

1 Ensure that an application is open on the MC67 and a text field is in focus (text cursor in text field).

2 Aim the exit window at a bar code.

3 Press and hold the a Scan button. 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 Data Capture LEDs light red to indicate that data capture is in process.

Figure 49: Data Capture



4 The Data Capture LED light green, a beep sounds and the MC67 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:

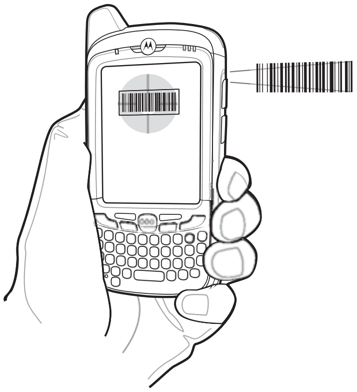
Procedure:

1 Ensure that an application is open on the MC67 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 a Scan button. By default, a preview window appears on the screen. The Data Capture LEDs light red to indicate that data capture is in process.

Figure 50: Data Capture with Camera



4 Move the MC67 until the bar code is centered under the red target.

5 The Left and Right LEDs light green, a beep sounds and the MC67 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.
  - **DWDemo** - provides support for the DWDemo application.
- Hidden profiles (not shown to the device):
  - **RD Client** - provides support for MSP.
  - **MSP Agent** - provides support for MSP.
  - **MspUserAttribute** - provides support for MSP.
  - **Camera** - disables scanning when the default camera application is in foreground.
  - **RhoElements** - disables scanning when RhoElements is in foreground.

Profile0

Profile0 can be edited but cannot be associated with an application. That is, **DataWedge** allows manipulation of plug-in settings for **Profile0** but it does not allow assignment of a foreground application. This configuration allows

DataWedge to send output data to any foreground application other than applications associated with user-defined profiles when **Profile0** is enabled.

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

Plug-ins

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

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

Input Plug-ins

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

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

Process Plug-ins

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

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

Output Plug-ins

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

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

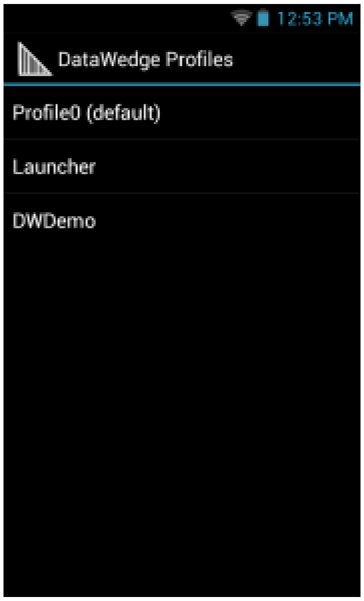
Profiles Screen

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 51: DataWedge Profiles Screen



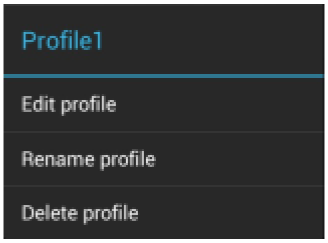
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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.

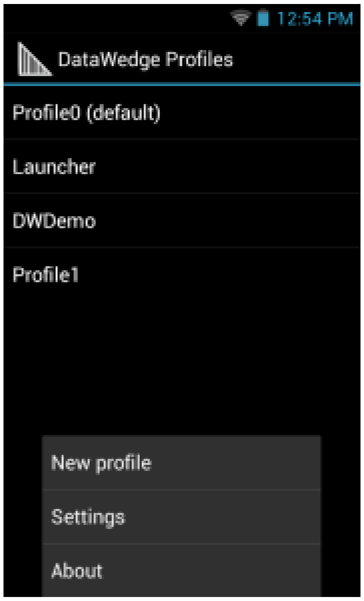
Figure 52: Profile Context Menu



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

Options Menu

Figure 53: DataWedge Options Menu



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

Disabling DataWedge

Procedure:

1. Touch⊙.
2. Touch ◣.
3. Touch ≡.
4. Touch **Settings**.
5. Touch **DataWedge enabled**.

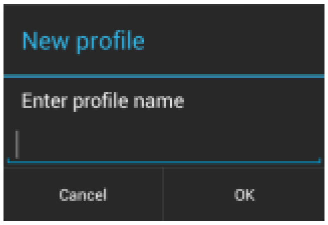
   The blue check disappears from the checkbox indicating that DataWedge is disabled.

Creating a New Profile

Procedure:

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

Figure 54: New Profile Name Dialog Box



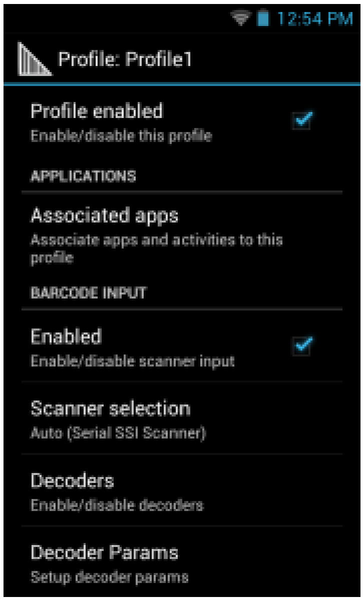
6 Touch **OK**.

The new profile name appears in the **DataWedge profile** screen.

Profile Configuration

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

Figure 55: Profile Configuration Screen



Profile enabled ☑
Enable/disable this profile

APPLICATIONS

Associated apps
Associate apps and activities to this profile

BARCODE INPUT

Enabled ☑
Enable/disable scanner input

Scanner selection
Auto (Serial SSI Scanner)

Decoders
Enable/disable decoders

Decoder Params
Setup decoder params

The configuration screen lists the following sections:

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

Bar Code Input

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

Enabled

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

Scanner Selection

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

- **Auto** - The software automatically selects the 2D Imager.
- **Camera scanner** - Scanning is performed with the rear-facing camera.
- **2D Imager** - Scanning is performed using the 2D Imager.

Decoders

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

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

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

Touch ↩ to return to the previous screen.

Decoder Params

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

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

    There are three options for transmitting a UPCA preamble:

    - **Preamble None** - Transmit no preamble.
    - **Preamble Sys Char** - Transmit System Character only (default).
    - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA). Select the appropriate option to match the host system.
- **UPCE0**

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

      There are three options for transmitting a UPCE0 preamble:

        - **Preamble Sys Char** - Transmit System Character only.
        - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
        - **Preamble None** - Transmit no preamble (default).
    - **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).
- **Code128**
    - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 73* for more information.
    - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 73* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
    - **Enable Plain Code 128** - Flag to enable other 128 sub types (besides GS1-128 and ISBT-128).
    - **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
    - **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
    - **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:
        - **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
        - **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
        - **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
    - **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
    - **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.
        - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
        - **Security Level 1** - This setting eliminates most misdecodes (default).
        - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
        - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.
- **Code39**
    - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 73* for more information.
    - **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 73* for more information.
    - **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that

include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).

  - **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
  - **Full ASCII** - Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled),
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
  - **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character “A” to all Code 32 bar codes (default - disabled).
  - **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).
- **Interleaved 2 of 5**
  - **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **Check Digit**
    - **No Check Digit** - A check digit is not used. (default)
    - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
    - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
  - **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).
  - **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
- **Composite AB**
  - **UCC Link Mode**
    - **Link Flag ignored** - 1D component is transmitted regardless of whether a 2D component is detected.
    - **Always Linked** - 1D and the 2D components are transmitted. If 2D is not present, the 1D component is not transmitted.
    - **Auto Discriminate** - the digital scanner determines if there is a 2D portion, then transmits the 1D component, as well as the 2D portion if present. (default).
- **UK Postal**
  - **Report Check Digit** - Transmit UK Postal data with or without the check digit. A check in the checkbox indicates to send UK Postal data with check digit (default - disabled).
- **Codabar**
  - **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
  - **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).

- **MSI**
  - **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 73* for more information.
  - **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
    - **One Check Digit** - Verify one check digit (default).
    - **Two Check Digits** - Verify two check digits.
  - **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
    - **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
    - **Mod-10-10** - Both check digits are MOD 10.
  - **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).
- **Code93**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Discrete 2 of 5**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Code 11**
  - **Length1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code.
    - **No Check Digit** - Do not verify check digit.
    - **1 Check Digit** - Bar code contains one check digit (default).
    - **2 Check Digits** - Bar code contains two check digits.
  - **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).
- **Matrix 2 of 5**
  - **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 73* for more information.
  - **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 73* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
  - **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).
- **UPCE1**

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

  There are three options for transmitting a UPCE1 preamble:

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

Decode Lengths

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

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

UPC EAN Params

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

- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
  - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding “in-spec” UPC/EAN bar codes (default).
  - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
  - **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
  - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.
- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.

  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
  - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).
- **Bookland** - Enable or disable this option. A check in the checkbox indicates that the option is enabled.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled.
- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.

Reader Params

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

- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -15000).
- **Linear Security Level** - Sets the number of times a bar code is read to confirm an accurate decode.
  - **Security Short or Codabar** - Two times read redundancy if short bar code or Codabar.
  - **Security All Twice** - Two times read redundancy for all bar codes (default).
  - **Security Long and Short** - Two times read redundancy for long bar codes, three times for short bar codes.
  - **Security All Thrice** - Three times read redundancy for all bar codes.
- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.
  - **Disable** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Centered** - Enables the Picklist mode so that only the bar code in the center of the image is decoded. This is most useful when used in conjunction with the static and dynamic reticle viewfinder modes. Note: This mode is only valid for decoder modules that supports a viewfinder. If one tries to set this for a unsupported decoder then the device would issue an error. (Camera scanner only).
  - **Reticle** - Enables the Picklist mode so that only the bar code that is directly under the cross-hair (reticle) is decoded. This is useful when used in conjunction with the static and dynamic reticle viewfinder modes. (Scan Module Only)

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

Scan Params

Allows the configuration of Code ID and decode feedback options.

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

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

- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).

MSR Input

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

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

Keystroke Output

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

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code or MSR data for use in native Android applications. This feature is helpful when populating or executing a form.
  - **None** - Action key character feature is disabled (default).
  - **Tab** - Tab character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.

  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 81* for more information.
- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Output

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).
- **Intent delivery** - Select the method by which the intent is delivered:
  - Send via StartActivity
  - Send via startService (default)
  - Broadcast intent
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 81* 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.getStringtExtra()` and `Intent.getSerializableExtra()` calls, using the following String tags:

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

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

- String MSR_DATA_TAG = “com.motorolasolutions.emdk.datawedge.msr_data”;
  - String contains the output data as a String. The data from the MSR tracks is concatenated and sent out as a single string.
- String MSR_TRACK1_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1”;
  - MSR track 1 data is returned as a byte array.

- String MSR_TRACK2_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2”;
  - MSR track 2 data is returned as a byte array.
- String MSR_TRACK3_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3”;
  - MSR track 3 data is returned as a byte array.
- String MSR_TRACK1_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1_status”;
  - MSR track 1 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK2_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2_status”;
  - MSR track 2 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK3_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3_status”;
  - MSR track 3 decode status as an Integer where 0 indicates a successful decode.

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

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

IP Output

Note: IPWedge application is required on a host computer. Download the IPWedge application from the Motorola Solutions Support Central web site: *http://www.motorolasolutions.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.

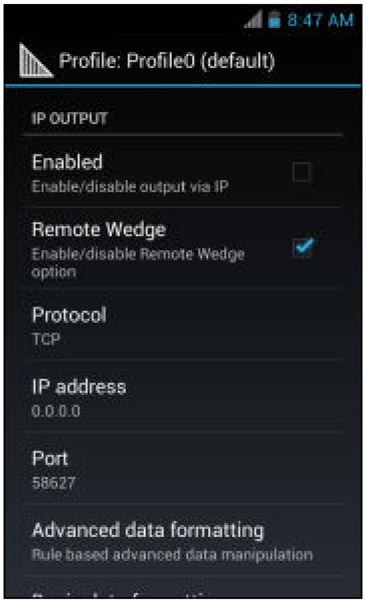
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol 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 81* 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 56: IP Output Screen



8:47 AM

Profile: Profile0 (default)

IP OUTPUT

Enabled
Enable/disable output via IP □

Remote Wedge
Enable/disable Remote Wedge option ☑

Protocol
TCP

IP address
0.0.0.0

Port
58627

Advanced data formatting
Rule based advanced data manipulation

Using IP Output with IPWedge

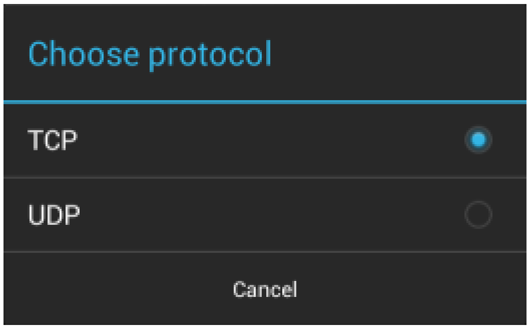
IPWedge is a computer application that can be easily configured to retrieve data sent over network by DataWedge IP Output. Refer to the *IPWedge User Manual* on how to install and configure in a host computer. To enable IP Output to send captured data to a remote computer that is installed with IPWedge:

Procedure:

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

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

Figure 57: Protocol Selection



Choose protocol

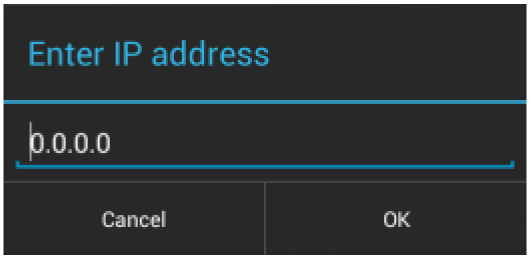
TCP ●

UDP ○

5 Touch **IP Address**.

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

Figure 58: IP Address Entry



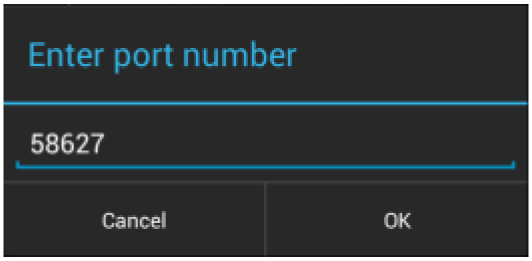
Enter IP address

0.0.0.0

7 Touch **Port**.

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

Figure 59: Port Number Entry



Enter port number

58627

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

Using IP Output without IPWedge

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

Procedure:

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

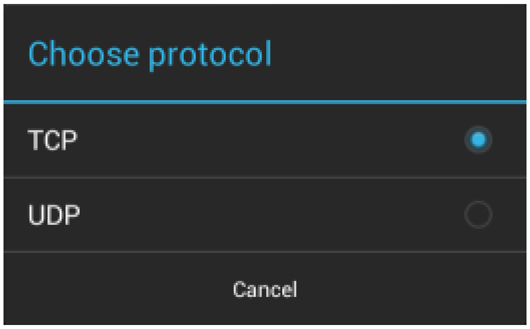
A check appears in the checkbox.

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

3 Touch **Protocol**.

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

Figure 60: Protocol Selection



Choose protocol

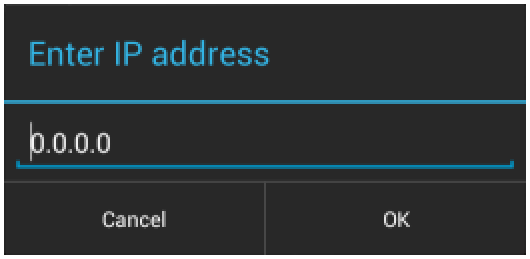
● TCP

○ UDP

5 Touch **IP Address**.

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

Figure 61: IP Address Entry



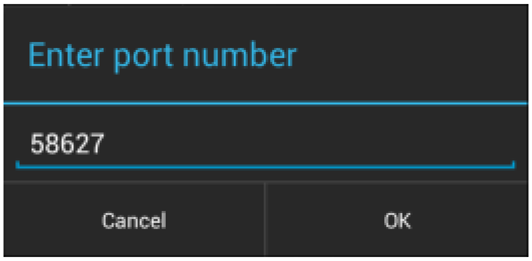
Enter IP address

0.0.0.0

7 Touch **Port**.

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

Figure 62: Port Number Entry



Enter port number

58627

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

Generating Advanced Data Formatting Rules

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

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

first number of characters to the Output plug-in, pad the output data with spaces or zeros, remove spaces in data, etc.

Configuring ADF Plug-in

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

Procedure:

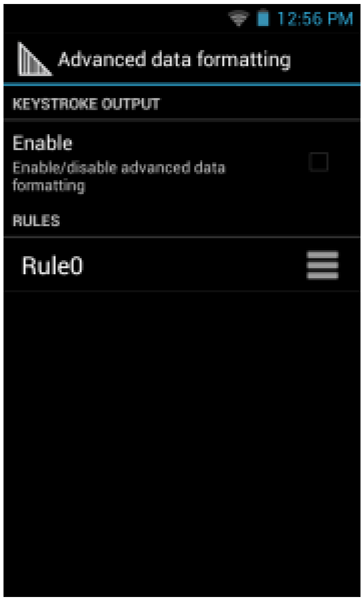
1 Touch .

2 Touch .

3 Touch a DataWedge profile.

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

Figure 63: Advanced Data Formatting Screen



12:56 PM

Advanced data formatting

KEYSTROKE OUTPUT

Enable ☐
Enable/disable advanced data formatting

RULES

Rule0

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

Creating a Rule

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

Procedure:

1

2 Touch **New rule**.

3 Touch the **Enter rule name** text box.

4 In the text box, enter a name for the new rule.

5 Touch **Done**.

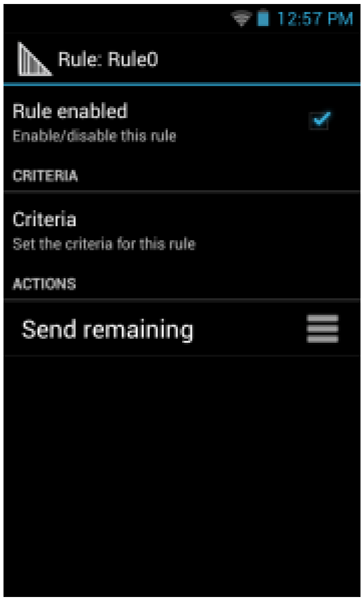
6 Touch **OK**.

Defining a Rule

Procedure:

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

Figure 64: Rule List Screen



12:57 PM

Rule: Rule0

Rule enabled ☑
Enable/disable this rule

CRITERIA

Criteria
Set the criteria for this rule

ACTIONS

Send remaining

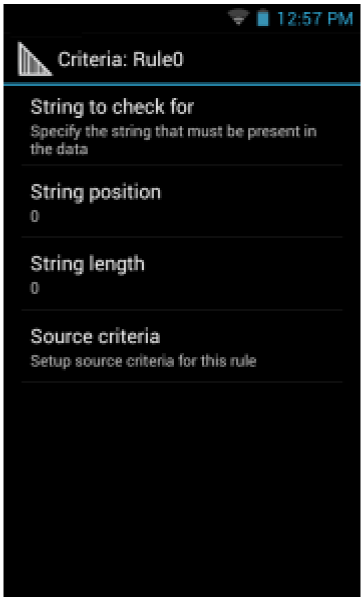
2 Touch the **Rule enabled** checkbox to enable the current rule.

Defining Criteria

Procedure:

1 Touch **Criteria**.

Figure 65: Criteria Screen



12:57 PM

Criteria: Rule0

String to check for
Specify the string that must be present in the data

String position
0

String length
0

Source criteria
Setup source criteria for this rule

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

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

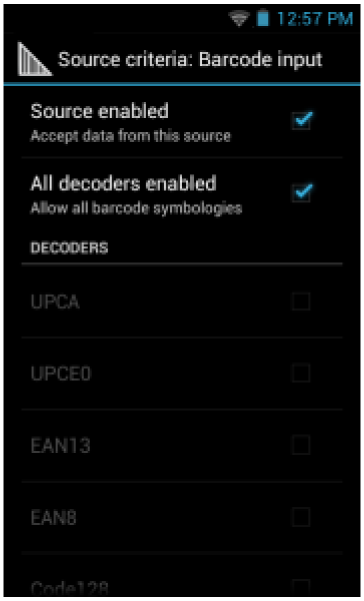
4 Touch **Done**.

5 Touch **OK**.

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

7 Touch the + or **-** to change the value.
8 Touch **OK**.
9 Touch **String length option** to specify a length for the received data. The ADF rule only applies to the bar code data with that specified length.
10 Touch the + or **-** to change the value.
11 Touch **OK**.
12 Touch **Source criteria** option to associate an input device to an ADF rule. The ADF rule only applies to data received from associated input devices.
13 Touch **Barcode input** or **MSR input**. Options vary depending upon the device configuration.
14 Touch the **Source enabled** checkbox to accept data from this source.

Figure 66: Barcode Input Screen



12:57 PM

Source criteria: Barcode input

Source enabled
Accept data from this source ☑

All decoders enabled
Allow all barcode symbologies ☑

DECODERS

UPCA □

UPCE0 □

EAN13 □

EAN8 □

Code128 □

15 For **Barcode inputs**, touch the **All decoders enabled** checkbox to select all bar code symbologies. Deselect the **All decoders enabled** checkbox to individually select the symbologies.
16 Touch ↩ until the **Rule** screen appears.
17 If required, repeat steps to create another rule.
18 Touch ↩ until the **Rule** screen appears.

Defining an Action

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

Procedure:

1 Touch ≡.
2 Touch **New action**.
3 In the **New action** menu, select an action to add to the **Actions** list. See *Table 7: ADF Supported Actions on page 85* for a list of supported ADF actions.
4 Some Actions require additional information. Touch the Action to display additional information fields.
5 Repeat steps to create more actions.
6 Touch ↩.
7 Touch ↩.

Deleting a Rule

Procedure:

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

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

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

Order Rules List

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

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

Table 7: ADF Supported Actions

Type	Actions	Description
Cursor Movement	Skip ahead	Moves the cursor forward by a specified number of characters. Enter the number of characters to move the cursor ahead.
	Skip back	Moves the cursor back by a specified number of characters. Enter the number of characters to move the cursor back.
	Skip to start	Moves the cursor to the beginning of the data.
	Move to	Moves the cursor forward until the specified string is found. Enter the string in the data field.
	Move past a	Moves the cursor forward past the specified string. Enter the string in the data field.
Data Modification	Crunch spaces	Remove spaces between words to one and remove all spaces at the beginning and end of the data.
	Stop space crunch	Stops space crunching. This disables the last **Crunch spaces** action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last **Remove all spaces** action.
	Remove leading zeros	Remove all zeros at the beginning of data.
	Stop zero removal	Stop removing zeros at the beginning of data. This disables the previous **Remove leading zeros** action.
	Pad with zeros	Left pad data with zeros to meet the specified length. Enter the number zeros to pad.
	Stop pad zeros	Stop padding with zeros. This disables the previous **Pad with zeros** action.
	Pad with spaces	Left pad data with spaces to meet the specified length. Enter the number spaces to pad.
	Stop pad spaces	Stop padding with spaces. This disables the previous **Pad with spaces** action.

Table continued…

Type	Actions	Description
	Replace string	Replaces a specified string with a new string. Enter the string to replace and the string to replace it with.
	Stop all replace string	Stop all **Replace string** actions.
Data Sending	Send next	Sends the specified number of characters from the current cursor position. Enter the number of characters to send.
	Send remaining	Sends all data that remains from the current cursor position.
	Send up to	Sends all data up to a specified string. Enter the string.
	Send pause	Pauses the specified number of milliseconds before continuing the next action. Enter the amount of time in milliseconds.
	Send string	Sends a specified string. Enter the string to send.
	Send char	Sends a specified ASCII/ Unicode character. Enter a character value. The maximum Unicode character value can be entered is U-10FFFF (= 1114111 in decimal).

Deleting an Action

Procedure:

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

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

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

Modify the data as follows:

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

To create an ADF rule for the above example:

Procedure:

1 Touch ⊞.
2 Touch **DataWedge**.
3 Touch **Profile0**.
4 Under **Keystroke Output**, touch **Advanced data formatting**.
5 Touch **Enable**.
6 Touch **Rule0**.
7 Touch **Criteria**.
8 Touch **String to check for**.
9 In the **Enter the string to check for** text box, enter `129` and then touch **OK**.
10 Touch **String position**.
11 Change the value to `0`.

12 Touch **OK**.

13 Touch **String length**.

14 Change value to `12`.

15 Touch **OK**.

16 Touch **Source criteria**.

17 Touch **Barcode input**.

18 Touch **All decoders enabled** to disable all decoders.

19 Touch **Code 39**.

20 Touch ↩ three times.

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

22 Touch **Delete action**.

23 Touch ≣ .

24 Touch **New action**.

25 Select **Pad with zeros**.

26 Touch the **Pad with zeros** rule.

27 Touch **How many**.

28 Change value to `8` and then touch **OK**.

29 Touch ↩ three times.

30 Touch ≣ .

31 Touch **New action**.

32 Select **Send up to**.

33 Touch **Send up to** rule.

34 Touch **String**.

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

36 Touch **OK**.

37 Touch ↩ three times.

38 Touch ≣ .

39 Touch **New action**.

40 Select **Send char**.

41 Touch **Send char** rule.

42 Touch **Character code**.

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

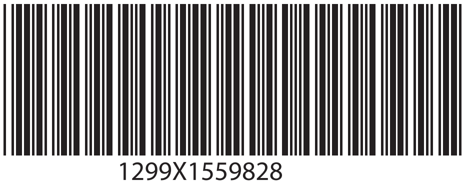
44 Touch **OK**.

45 Touch ↩.

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

47 Aim the exit window at the bar code.

Figure 67: Sample Bar Code



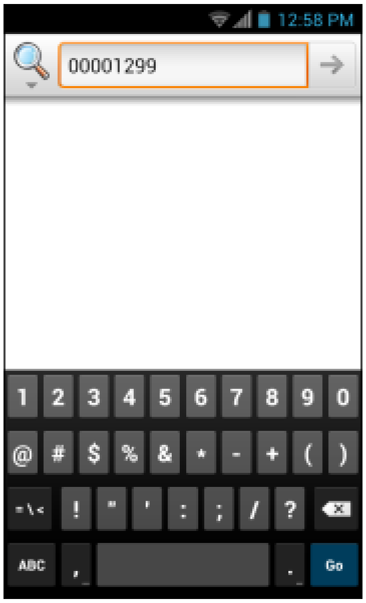
48 Press and hold the scan button.

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

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

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

Figure 68: Formatted Data

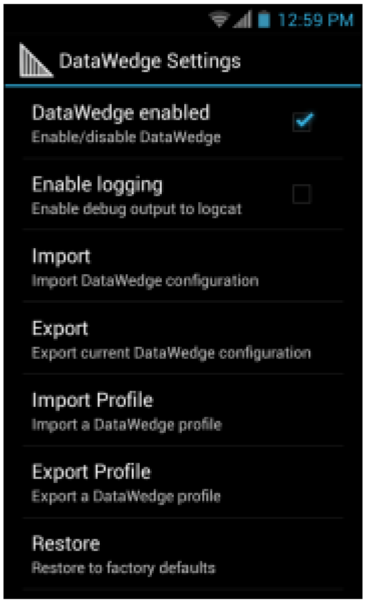


00001299

DataWedge Settings

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

Figure 69: DataWedge Settings Window



DataWedge Settings

DataWedge enabled ☑
Enable/disable DataWedge

Enable logging □
Enable debug output to logcat

Import
Import DataWedge configuration

Export
Export current DataWedge configuration

Import Profile
Import a DataWedge profile

Export Profile
Export a DataWedge profile

Restore
Restore to factory defaults

- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option.
- **Enable logging** - Enables or disables debug output file to logcat. To enable logging check this option.
- **Import** - allows import of a DataWedge configuration file. The imported configuration replaces the current configuration.

- **Export** - allows export of the current DataWedge configuration to the microSD card.
- **Import Profile** - allows import of a DataWedge profile file.
- **Export Profile** - allows export of a DataWedge profile.
- **Restore** - return the current configuration back to factory defaults.

Importing a Configuration File

Procedure:

1 Copy the configuration file to the root of the microSD card.
2 Touch ⊞.
3 Touch ▥.
4 Touch ☰.
5 Touch **Settings**.
6 Touch **Import**.
7 Touch **SD Card**.
8 Touch **Import**. The configuration file (`datawedge.db`) is imported and replaces the current configuration.

Exporting a Configuration File

Procedure:

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

Importing a Profile File

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

Procedure:

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

Exporting a Profile

Procedure:

1 Touch ⊞.

2. Touch ▥.
3. Touch ≡.
4. Touch **Settings**.
5. Touch **Export Profile**.
6. Touch the profile to export.
7. Touch **Export**.
8. Touch **Export**. The profile file (`dwprofile_x.db`, where x = name of the profile) is saved to the root of the microSD card.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

Procedure:

1. Touch ⊞.
2. Touch ▥.
3. Touch ≡.
4. Touch **Settings**.
5. Touch **Restore**.
6. Touch **Yes**.

Configuration and Profile File Management

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

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

Enterprise Folder

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

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

Auto Import

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

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

Note:

A Factory Reset deletes all files in the Enterprise folder.

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

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application

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

Capture Data and Taking a Photo in the Same Application

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

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

Disable DataWedge on MC67 and Mass Deploy

To disable DataWedge and deploy onto multiple MC67 devices:

Procedure:

1 Touch ⊞.

2 Touch **DataWedge**.

3 Touch ☰.

4 Touch **Settings**.

5 Unselect the **DataWedge enabled** check box.

6 Export the DataWedge configuration. See *Exporting a Configuration File on page 89* for instructions. See *Configuration and Profile File Management on page 90* 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.motorolasolutions.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”

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

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

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

Sample

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

Chapter 5

Administrator Utilities

Motorola Solutions provides a suite of utilities that allow an administrator to manage the following features:

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

The following applications help the administrator configure these features.

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

Required Software

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

On-device Application Installation

See *Application Installation on page 123* for instruction on installing applications onto the device.

Multi-user/AppLock Configuration

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

Note: The administrator can also create the account information manually. See *Manual File Configuration on page 103* for more information.

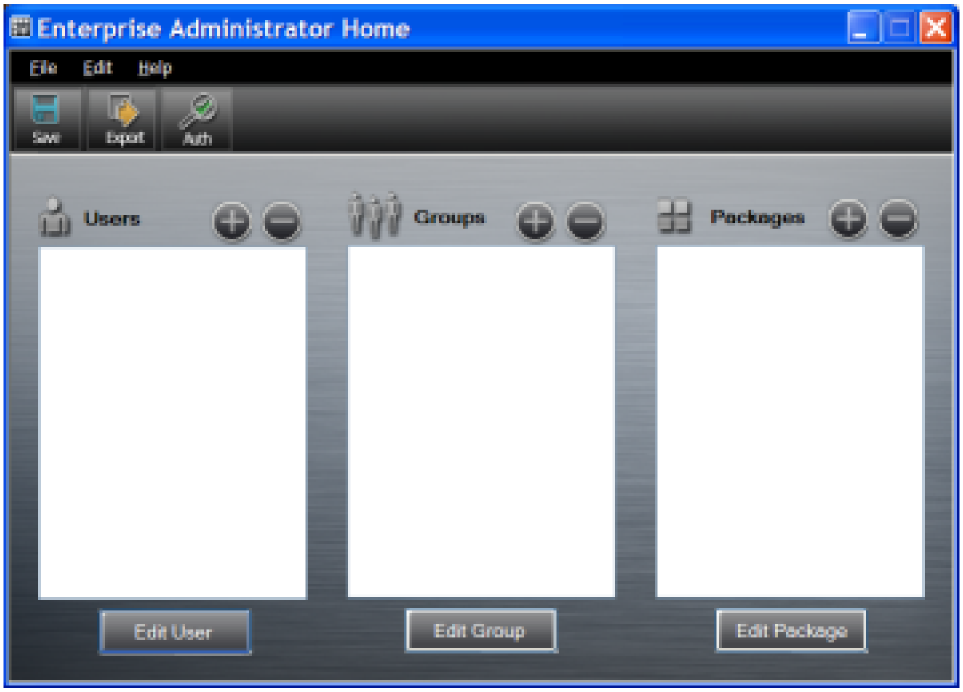
Enterprise Administrator Application

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

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

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

Figure 70: Enterprise Administrator Window



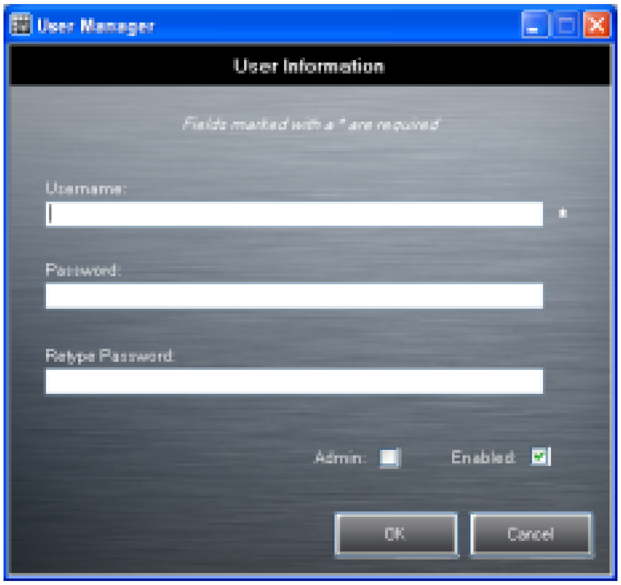
Creating Users

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

Procedure:

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

Figure 71: User Manager Window



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

Adding Packages

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

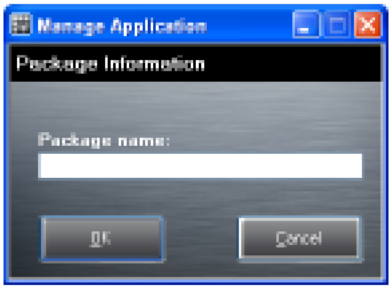
Create a list of installed applications (packages) on the device that are available for use by all the users.

Procedure:

1. Click + next to **Packages**.

   Note: To get a list of all the applications (packages) on the device see *Determining Applications Installed on the Device on page 104*.

Figure 72: Package Information Window



2. In the **Package name** text box, enter the name of an application.
3. Click **OK**.
4. Repeat steps 1 through 3 for each additional package.

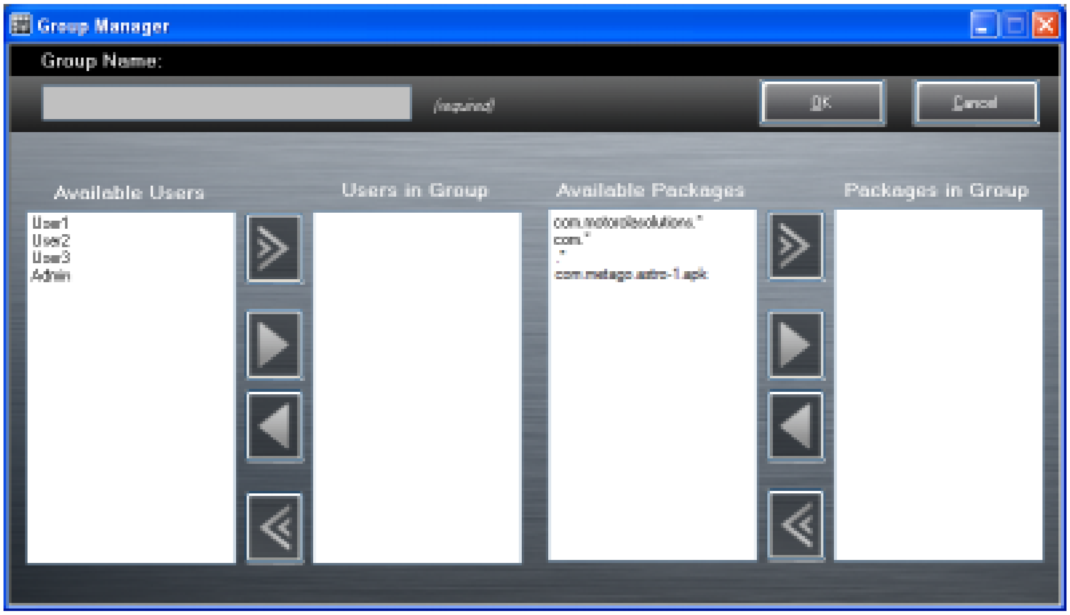
Creating Groups

Create groups of users that have access to specific applications.

Procedure:

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

Figure 73: Group Manager Window



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

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

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

5 Click **OK**.

6 Click **Save**.

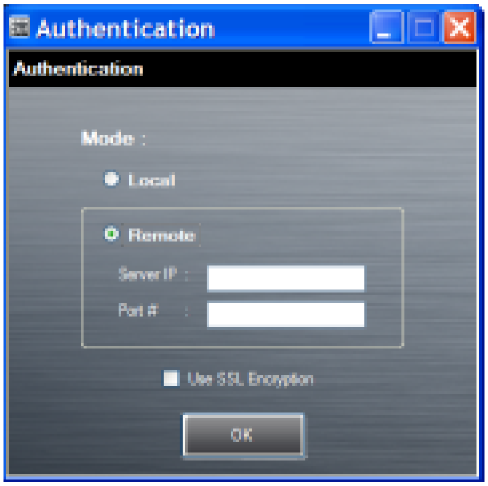
Creating Remote Authentication

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

Procedure:

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

Figure 74: Authentication Window



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

Save Data

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

Exporting File

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

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

Procedure:

1 Click **Export**.
2 In the **Browse For Folder** window, select a folder and then click **OK**.
3 Click **OK**.
4 Click **File** → **Export** → **Server Information**.

The server file is saved in the `<user>\_APP_DATA` folder.

5 Copy all the files to the root of the microSD card. See *USB Communication on page 61* for information on copying files to the device.

Importing User List

Procedure:

1 Click **File** → **Import** → **User List**.
2 Navigate to the location when the *passwd* file is stored.
3 Select the `passwd` file.

4 Click **Open**.

The user information is populated into the **Users** list.

Importing Group List

Procedure:

1 Click **File** → **Import** → **Group List**.
2 Navigate to the location when the `group` file is stored.
3 Select the `group` file.
4 Click **Open**.

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

Importing Package List

To import a package list (see *Package List File on page 104* for instructions for creating a Package List file):

Procedure:

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

The package information is populated into the **Packages** list.

Editing a User

Procedure:

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

Deleting a User

Procedure:

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

Editing a Group

Procedure:

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

Deleting a Group

Procedure:

1 Select a group in the **Groups** list.
2 Click **-**.
3 Click **Yes**. The group name is removed from the list.

Editing a Package

Procedure:

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

Deleting a Package

Procedure:

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

MultiUser Administrator

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

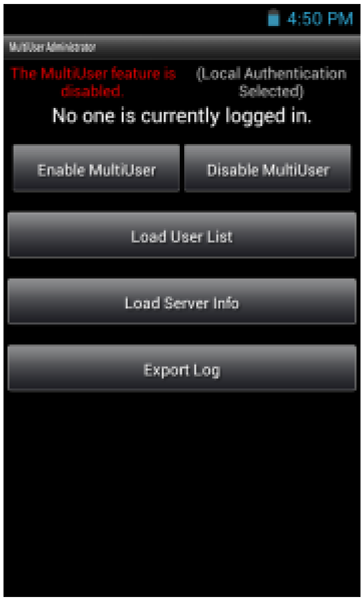
Importing a Password

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

Procedure:

1. Touch ⊞.
2. Touch 👥.

Figure 75: MultiUser Administrator Screen



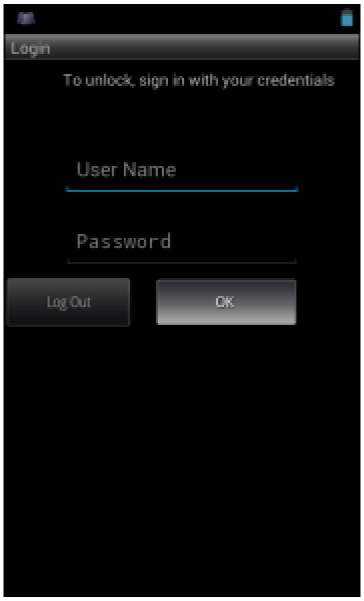
The MultiUser feature is disabled.

(Local Authentication Selected)

No one is currently logged in.

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

Figure 76: MultiUser Login Screen



Login

To unlock, sign in with your credentials

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

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

7 Touch **OK**.

Disabling the Multi-user Feature

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

Procedure:

1 Touch ⊞.

2 Touch 👥.

3 Touch **Disable MultiUser**.

The Multi-user feature is disabled immediately.

Enabling Remote Authentication

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

Procedure:

1 Touch ⊞.

2 Touch 👥.

3 Touch **Load Server Info**. The application reads the data from the *server* file and configures the Multi-user Login feature.

4 Touch ≡.

5 Touch **Enable Remote Authentication**.

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

Disabling Remote Authentication

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

Procedure:

1 Touch ⊞.
2 Touch 👥.
3 Touch ≡.
4 Touch **Disable Remote Authentication**.

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

Enabling Data Separation

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

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

Procedure:

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

Disabling Data Separation

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

Procedure:

1 Touch ⊞.
2 Touch 👥.
3 Touch ≡.
4 Touch **Disable Data Separation**. The current user is logged out to restore the system to common data space for all users.

Delete User Data

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

Procedure:

1 Touch ⊞.
2 Touch 👥.

3 Touch ≡.

4 Touch **Delete Individual User Data**. A dialog box displays with all of the users that currently have data associated with their log in.

5 Select each user to delete or **Select All** to delete all user data.

6 Touch **Delete** to delete the data.

Capturing a Log File

Procedure:

1 Touch ⊞.

2 Touch ▦.

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

3 Touch **Export Log** to copy the log file to the microSD card. The log file can be captured when the multi-user feature is in either the enabled or disabled mode.

4 The log file and a backup log file are named `multiuser.log` and `multiuser.log.bak`, respectively.

AppLock Administrator

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

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

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

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

Enabling Application Lock

Procedure:

1 Touch ⊞.

2 Touch ▦.

3 Touch **Enable Application Lock**.

Disabling Application Lock

Procedure:

1 Touch ⊞.

2 Touch ▦.

3 Touch **Disable Application Lock**.

Manual File Configuration

Groups File

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

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

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

where:

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

`<user1>` through `<userN>` = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 99* for more information.

Note:

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

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

Examples:

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

White List File

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

```
<package1name>
.
.
.
<packageNname>
```

where:

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

Example:

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

```
com.companyname.application
com.motorolasolutions.*
```

where:

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

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

`com.motorolasolutions.*` = any application that has a package name that starts with `com.motorolasolutions` will be permitted for this group.

Note:

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

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

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

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

Package List File

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

Example:

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

Determining Applications Installed on the Device

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

Procedure:

1 Connect the device to the host computer.

Note: See *Development Tools on page 122* for information on installing the USB driver for use with adb.

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

`adb devices`. This returns the device id.

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

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

Secure Storage

Secure Storage Administrator application allows:

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

Installing a Key

Procedure:

1 Touch ⊞.

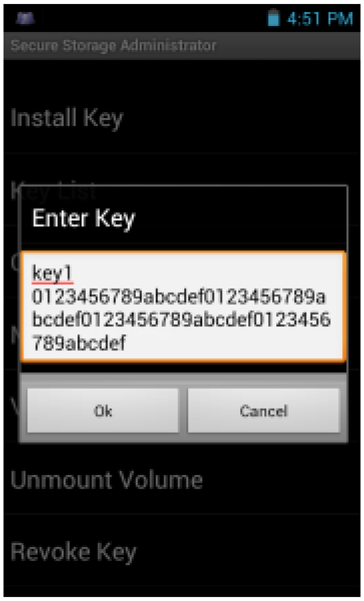
2 Touch 🔒.

3 Touch **Install Key**.

4 Touch **Manual**.

5 Touch **OK**.

Figure 77: Enter Key Dialog Box



key1
0123456789abcdef0123456789a
bcdef0123456789abcdef0123456
789abcdef

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

<Key Name> <Key value in Hex String>

Example: key2 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

The key value must be a 64 hexadecimal character string.

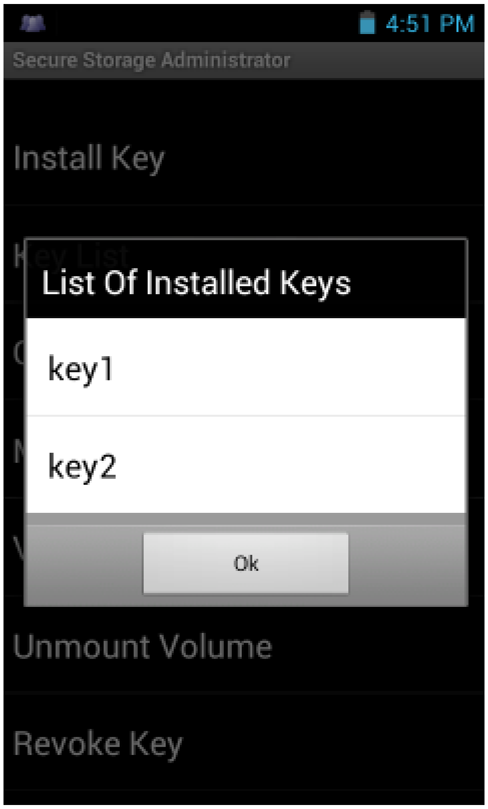
7 Touch **OK**. The key is imported into the device. The message **successfully installed the key** appears on the screen.

Viewing Key List

Procedure:

1 Touch **Key List**.

Figure 78: List of Keys



List Of Installed Keys

key1

key2

2 Touch **OK**.

Deleting a Key

Procedure:

1 Touch **Revoke Key**.
2 Touch the key to deleted.
3 Touch **OK**.

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

Volumes

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

Creating Volume Using EFS File

Procedure:

1 Create an efs file. See *Creating an EFS File on page 108* for instruction on creating the efs file.
2 Copy the `keyfile` and `efsfile` files to root of the microSD card. See *USB Communication on page 61*.
3 Touch **Create Volume**.
4 Touch **Import**.
5 Touch **OK**. The message **Successfully Created the Volume** appears briefly.

Creating a Volume Manually

Procedure:

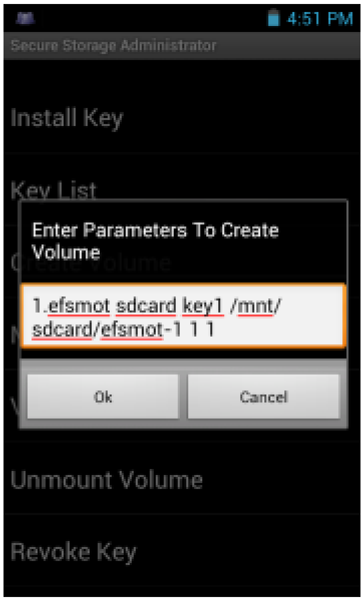
1. Touch **Create Volume**.
2. Touch **Manual**.
3. Touch **OK**.
4. In the **Enter Parameters To Create Volume** text box, enter the parameters in the follow format:

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

   where:

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

   Figure 79: Enter Parameter To Create Volume Dialog Box

   Enter Parameters To Create Volume

   1.efsmot sdcard key1 /mnt/sdcard/efsmot-1 1 1

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

Mounting a Volume

Procedure:

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

Listing Volumes

Procedure:

1. Touch **Volume List**.

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

Unmounting a Volume

Procedure:

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

Deleting a Volume

Procedure:

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

Encrypting an SD Card

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

Procedure:

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

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

Creating an EFS File

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

Procedure:

1. On a host computer, create a text file.
2. In the text file enter the following:

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

   where:

   <Volume Name> = name of the volume

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

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

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

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

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

Example:

MyVolume sdcard key1 /mnt/sdcard/efsfolder 1 1

3 Save the text file as `efsfile`.

Off-line Extraction Tool

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

Connect the device to the host computer.

Usage

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

The following Main Menu appears:

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

Creating an Image

Procedure:

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

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

2 The utility first prompts for the name of the volume to create. Any ASCII string that meets standard Linux file naming rules is valid. Enter the image name and then press **Enter**.

3 The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.

4 The utility then prompts for the image size. Enter the size of the volume in MB. A number must be entered without the units. It is understood that MB. A value of 2000, is 2 GB. Note that 4 GB is the largest volume that is supported on the device.

5 The utility lastly prompts for the filesystem type. Enter ext4 and then press **Enter**.

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

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

```
Press [1] if you want to mount or press [2] if you want to exit
```

6 Press **1** will prompt for the mount point. For example, /mnt is prompted. Press **Enter** to mount the encrypted volume at the selected point. After mounting, an option to return to the Main Menu or Exit is provided.

Press **2** to exit the utility without mounting.

7 If the volume is mounted on the desktop, then that volume can be provisioned with files for deployment.

8 Unmounted volumes can then be copied to the device and subsequently mounted using the Secure Storage Administrator by providing the encryption key used.

Mounting an Image

Procedure:

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

   ```
   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>
   Please enter encryption key (64-bytes hex value):
   Please enter mount path (e.g. /mnt): <existing mount point>

   DONE - OK
   ```

2. Enter the name of the volume and then press **Enter**.
3. The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
4. Enter the mount point where to connect the volume into the file system and then press **Enter**. The example of /mnt is provided.

Unmounting an Image

Procedure:

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

   ```
   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>

   DONE - OK
   ```

2. Enter the name of the volume to unmount.
3. Press **Enter**.

Chapter 6

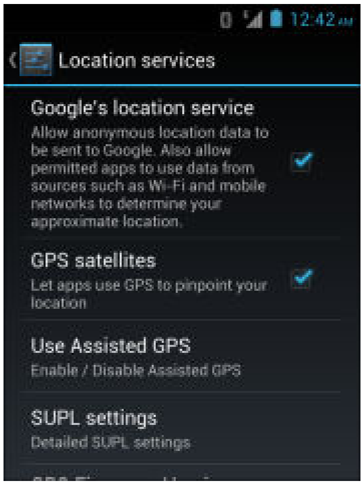
Settings

This chapter describes settings available for configuring the device.

Location Settings

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

Figure 80: Location Access Screen



12:42 AM

Location services

Google's location service ☑
Allow anonymous location data to be sent to Google. Also allow permitted apps to use data from sources such as Wi-Fi and mobile networks to determine your approximate location.

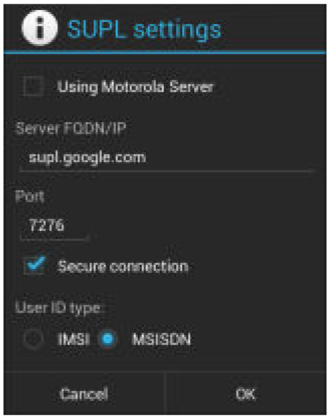
GPS satellites ☑
Let apps use GPS to pinpoint your location

Use Assisted GPS
Enable / Disable Assisted GPS

SUPL settings
Detailed SUPL settings

- **Google's location service** - Check to allow anonymous location data to be sent to Google and to allow permitted applications to use data from sources such as Wi-Fi and mobile networks to determine approximate location.
- **GPS satellites** - Check to allow application to use the MC67 to pinpoint your location.
- **Use Assisted GPS** - Touch to enable or disable Assisted GPS.
- **SUPL settings** - Touch to configure a Secure User Plane Location (SUPL) server.

Figure 81: SUPL Settings



SUPL settings

□ Using Motorola Server

Server FQDN/IP

supl.google.com

Port

7276

☑ Secure connection

User ID type

○ IMSI ● MSISDN

- **Using Motorola Server** - Check to use the Motorola SUPL server.
- **Server FQN/IP** - Enter the address for a SUPL server when not using the Motorola server.
- **Port** - Enter the port address for the SUPL server.
- **Secure connection** - Check to set the server for a secure connection.
- **User ID type** - Select which ID type to use during the SUPL session.

Screen Unlock Settings

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

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

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.
  - **None** - Disable screen unlock security.
  - **Slide** - Slide the lock icon to unlock the screen.
  - **Pattern** - Draw a pattern to unlock screen. See *Set Screen Unlock Using Pattern on page 114* for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 113* for more information.
  - **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 113* 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.

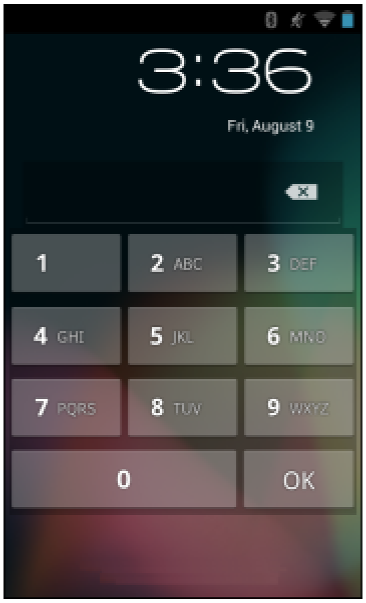
If the PIN or Password screen unlock feature is enabled, enter the PIN or password after unlocking the screen.

Set Screen Unlock Using PIN

Procedure:

1. Touch ⊞.
2. Touch ☰.
3. Touch 🔒 **Security**.
4. Touch **Screen lock**.
5. Touch **PIN**.
6. Touch in the text field.
7. Enter a PIN (between 4 and 16 characters) then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. On the **Security** screen, touch **Vibrate on touch** to enable vibration when the user enters PIN.
10. Touch ⌂. The next time the device goes into suspend mode a PIN is required upon waking.

Figure 82: PIN Screen

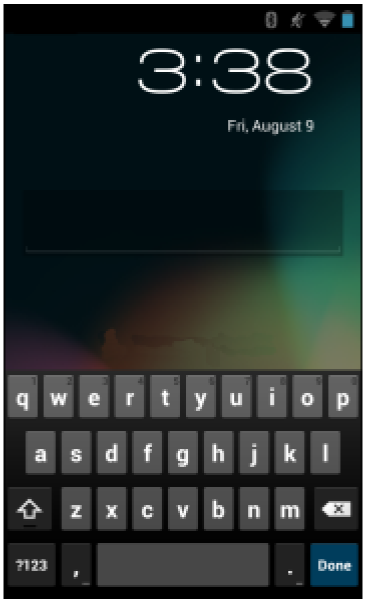


Set Screen Unlock Using Password

Procedure:

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

Figure 83: Password Screen



Set Screen Unlock Using Pattern

Procedure:

1 Touch ⊞.

2 Touch ☰.

3 Touch 🔒 **Security**.

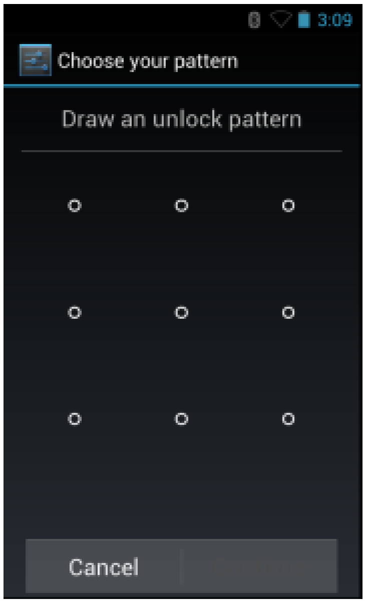
4 Touch **Screen lock**.

5 Touch **Pattern**.

6 Watch pattern example and then touch **Next**.

7 Draw a pattern connecting at least four dots.

Figure 84: Choose Your Pattern Screen



Draw an unlock pattern

8 Touch **Continue**.

9 Re-draw the pattern.

10 Touch **Confirm**.

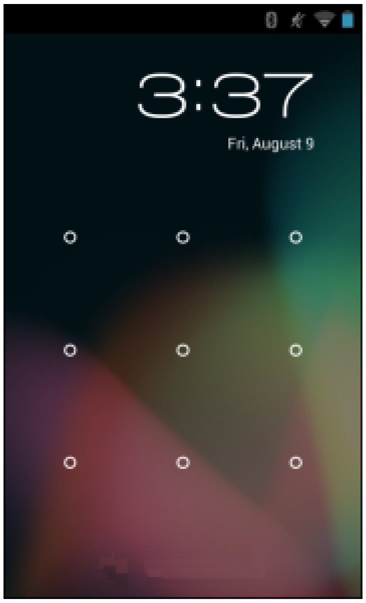
11 On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.

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

13 Touch ⌂.

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

Figure 85: Pattern Screen



Multiple User Mode

For Multi-user Mode configuration, see *Administrator Utilities on page 93*.

Passwords

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

Button Remapping

The MC67's buttons can be programmed to perform different functions or shortcuts to installed applications.

- Trigger 1- Left Scan/Action button
- Trigger 2 - Right Scan/Action button
- Trigger 3 - Volume up button
- Trigger 4 - Volume down button
- Trigger 5 - Action button

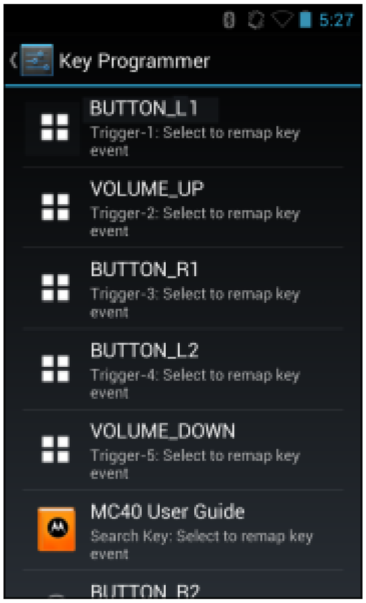
Remapping a Button

Procedure:

1 Touch ⚙.

2 Touch ⊞ **Key Programmer**.

Figure 86: Key Programmer Screen



BUTTON_L1
Trigger-1: Select to remap key event

VOLUME_UP
Trigger-2: Select to remap key event

BUTTON_R1
Trigger-3: Select to remap key event

BUTTON_L2
Trigger-4: Select to remap key event

VOLUME_DOWN
Trigger-5: Select to remap key event

MC40 User Guide
Search Key: Select to remap key event

BUTTON_R2

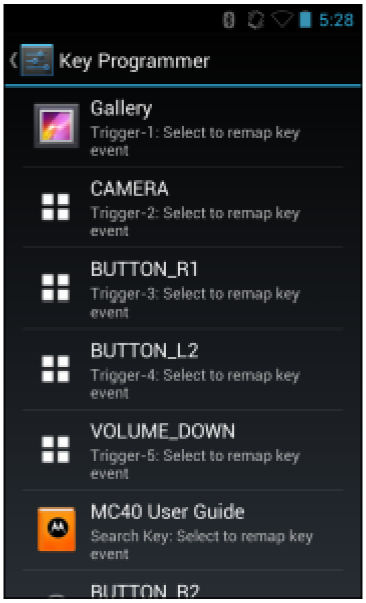
3 Select the button to remap.

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

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

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

Figure 87: Remapped Button



5:28

Key Programmer

Gallery
Trigger-1: Select to remap key event

CAMERA
Trigger-2: Select to remap key event

BUTTON_R1
Trigger-3: Select to remap key event

BUTTON_L2
Trigger-4: Select to remap key event

VOLUME_DOWN
Trigger-5: Select to remap key event

MC40 User Guide
Search Key: Select to remap key event

BUTTON_R2

6 Touch ⌂.

Exporting a Configuration File

The Button Remapping configuration can be exported to an xml file and imported into other MC67 devices.

Procedure:

1 Touch ⊙.

2 Touch ⚙.

3 Touch ⊞ **Key Programmer**.

4 Touch ☰.

5 Touch **Export**.

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

6 Copy the xml file from the folder to a host computer. See *USB Communication on page 61* for more information.

Importing a Configuration File

Procedure:

1 Copy the configuration file (`key-config.xml`) from a host computer to the root of the microSD card. See *USB Communication on page 61* for more information.

2 On the MC67, use **File Browser** to move the file from the root of the microSD card: `/enterprise/usr`.

3 Touch ⚙.

4 Touch ⊞ **Key Programmer**.

5 Touch ☰.

6 Touch **Import**.

Creating a Remap File

The administrator can create an xml configuration file and import it into any MC67 device. Use any text editor to create the xml file with the filename: `key-config.xml`.

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

Replace the options for each trigger. See for a list of available button functions.

Enterprise Reset

To ensure that the configuration persists after an Enterprise Reset:

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

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

Two ways to persist the settings:

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

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

Accounts

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

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

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

Language Usage

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

Changing the Language Setting

Procedure:

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

The operating system text changes to the selected language.

Adding Words to the Dictionary

Procedure:

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

Keyboard Settings

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

- Android Keyboard

- Chinese keyboard

About Phone

Use **About phone** settings to view information about the MC67. Touch ⚙ > **About phone**.

- **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.
  - **Network** - indicates the current network carrier.
  - **Signal strength** - indicates the radio signal strength.
  - **Mobile network type** - indicates the mobile network type.
  - **Service state** - indicates the state of service.
  - **Roaming** - indicates if the device is roaming outside the network.
  - **Mobile network state** - indicates the mobile network state.
  - **My phone number** - displays the phone number associated with the device.
  - **IMEI** - displays the IMEI number for the device.
  - **IMEI SV** - displays the IMEI SV number for the device.
  - **IP address** - Displays the IP address of the device.
  - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
  - **Ethernet address** - Displays the Ethernet driver 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 MC67 has been running since being turned on.
- **Battery information** - Displays information about the battery.
- **Hardware config** - Lists part number for various hardware on the MC67.
- **Legal information** - Opens a screen to view legal information about the software included on the MC67.
- **Model number** - Displays the devices model number.
- **EA Version** - Displays the EA firmware version.
- **SSPAM** - Displays SSPAM firmware version.
- **Serial number** - Displays the device serial number.
- **Build Tag** - Displays the build name.
- **Android version** - Displays the operating system version.
- **Baseband version** - Displays WAN radio firmware version.
- **Kernel version** - Displays the kernel version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

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).

Secure Certificates

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

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

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

Installing a Secure Certificate

Procedure:

1. Copy the certificate from the host computer to the root of the microSD card. See *USB Communication on page 61* for information about connecting the device to a host computer and copying files.
2. Touch ⊞.
3. Touch ☰.
4. Touch 🔒 **Security**.
5. Touch **Install from SD card**.
6. Touch the filename of the certificate to install. Only the names of certificates not already installed are displayed.
7. If prompted, enter the certificate's password and touch **OK**.
8. Enter a name for the certificate and touch **OK**. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

   The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the microSD card.

Configuring Credential Storage Settings

Procedure:

1. Touch ⊞.
2. Touch ⚙.
3. Touch 🔒 **Security**.
    - **Trusted credentials** - Touch to display the trusted system and user credentials.
    - **Install from SD card** - Touch to install a secure certificate from the microSD card.
    - **Clear credentials** - Deletes all secure certificates and related credentials.

Development Tools

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

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

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

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

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

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

On the Home screen, touch ⊞ > ⚙ > { } **Developer options**. Slide the switch to the **ON** position to enable developer options. The following developer options are available:

- **Desktop backup password**
- **Stay awake**
- **Debugging**
    - **USB debugging**

  - **Allow mock locations**
  - **Select debug app**
  - **Wake for debugger**
- **Input**
  - **Show touches**
  - **Pointer location**
- **Drawing**
  - **Show layout bounds**
  - **Show GPU view updates**
  - **Show surface updates**
  - **Window animation scale**
  - **Transition animation scale**
  - **Animator duration scale**
  - **Disable HW overlays**
  - **Force GPU rendering**
- **Monitoring**
  - **Strict mode enabled**
  - **Show CPU usage**
  - **Profile GPU rendering**
  - **Enable traces**
- **Apps**
  - **Don’t keep activities**
  - **Background process limit**
  - **Show all ANRs**

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 Motorola Solutions Support Central web site at *http://www.motorolasolutions.com/support*. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

Application Installation

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

- USB connection, see *Installing Applications Using the USB Connection on page 124*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 124*.
- Mobile device management (MDM) platforms that have application provisioning.

Installing Applications Using the USB Connection

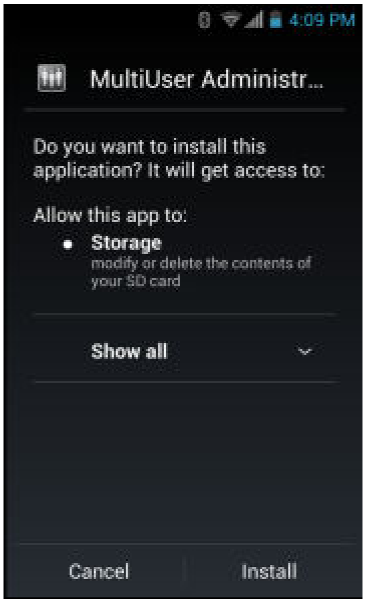
Caution:

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

Procedure:

1. Connect the device to a host computer using USB. See *USB Communication on page 61*.
2. On the host computer, copy the application `.apk` file from the host computer to the device.
3. Disconnect the device from the host computer. See *USB Communication on page 61*.
4. On the device, touch ⊞.
5. Touch 📁 to view files on a microSD card.
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 88: Accept Installation Screen



4:09 PM

MultiUser Administr...

Do you want to install this application? It will get access to:

Allow this app to:

- Storage
  modify or delete the contents of your SD card

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

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

Caution:

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

Prerequisites: Ensure that the ADB drivers are installed on the host computer. See *ADB USB Setup on page 123*.

Procedure:

1. Connect the device to a host computer using USB. See *USB Communication on page 61*.
2. Touch ⊞.

3 Touch ⚙.

4 Touch { } **Developer options**.

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

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

7 Touch **OK**.

8 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.

9 Disconnect the device from the host computer. See *USB Communication on page 61*.

Uninstalling an Application

Procedure:

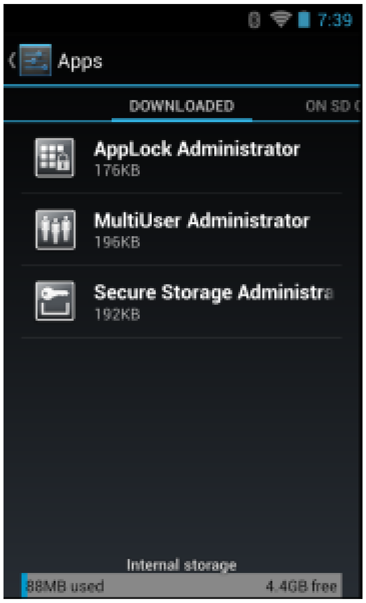
1 Touch ⊞.

2 Touch ⚙.

3 Touch **Apps**.

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

Figure 89: Downloaded Screen



7:39

Apps

DOWNLOADED ON SD C

AppLock Administrator
176KB

MultiUser Administrator
196KB

Secure Storage Administra
192KB

Internal storage
88MB used 4.4GB free

5 Touch the application to uninstall.

6 Touch **Uninstall**.

7 Touch **OK** to confirm.

Updating the System

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

Procedure:

1 Download the system update package:

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

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

2 Locate the System Update package file on the host computer and un-compress the file into a separate directory.

3 Copy the `M67N0JXXVRUxxxxxxx.zip` file to the root directory of the microSD card. See *USB Communication on page 61* for more information.

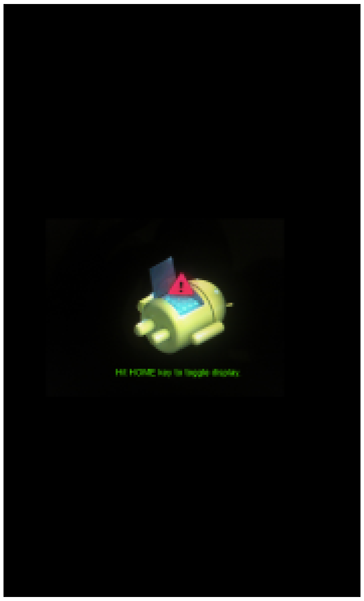
4 Press and hold the Power button until the menu appears.

5 Touch **Reset**.

6 Press and hold the Right Action button.

7 When the Recovery Mode screen appears, release the button.

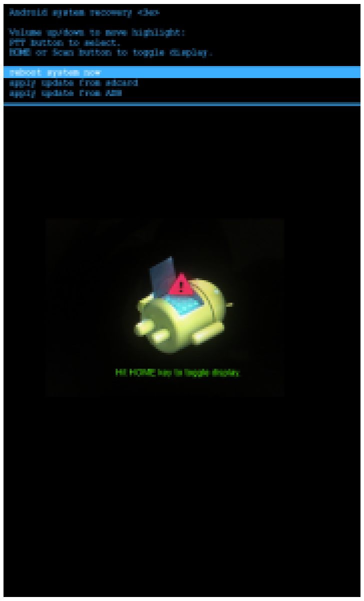
Figure 90: Recovery Mode Screen



Hit HOME key to toggle display

8 Touch ⌂.

Figure 91: System Recovery Screen



```
Android system recovery <3e>

Volume up/down to move highlight;
PTT button to select.
HOME or Scan button to toggle display.

reboot system now
apply update from sdcard
apply update from ADB
```

Hit HOME key to toggle display

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

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

11 Press the Right Action button.

12 Press the Enter button.

13 Press the Volume Up and Volume Down buttons to navigate to the `M67N0JXXVRUxxxxxxx.zip` file.

14 Press the Right Action button. The System Update installs and then the MC67 resets.

Storage

The device contains four types of file storage:

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

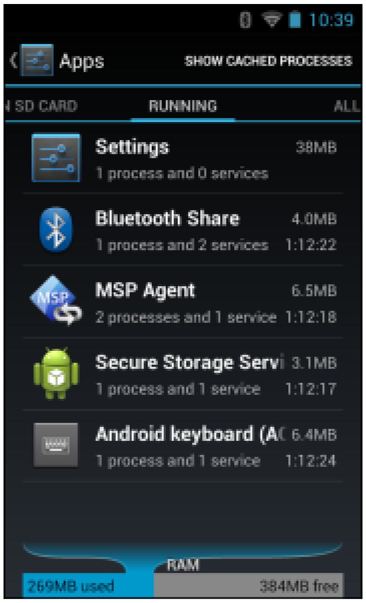
Random Access Memory

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

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

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

Figure 92: Running Screen



Settings 1 process and 0 services	38MB	
Bluetooth Share 1 process and 2 services	4.0MB	1:12:22
MSP Agent 2 processes and 1 service	6.5MB	1:12:18
Secure Storage Servi 1 process and 1 service	3.1MB	1:12:17
Android keyboard (A(1 process and 1 service	6.4MB	1:12:24

269MB used 384MB free

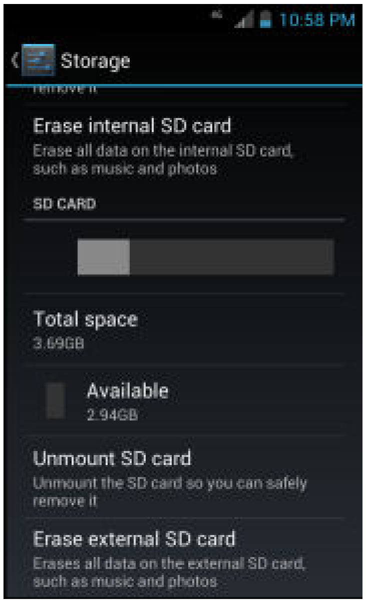
The bar at the bottom of the screen displays the amount of used and free RAM.

External Storage

The MC67 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the MC67 is connected to a host computer. Some applications are designed to be stored on the microSD card rather than in internal memory.

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

Figure 93: Storage Settings



remove it

Erase internal SD card
Erase all data on the internal SD card, such as music and photos

SD CARD

Total space
3.69GB

Available
2.94GB

Unmount SD card
Unmount the SD card so you can safely remove it

Erase external SD card
Erases all data on the external SD card, such as music and photos

- **Total space** - Displays the total amount of space on the installed microSD card.
- **Apps** - Displays the available space used for applications and media content on the installed microSD card.
- **Pictures, videos** - Displays the available space used for pictures and videos on the installed microSD card.

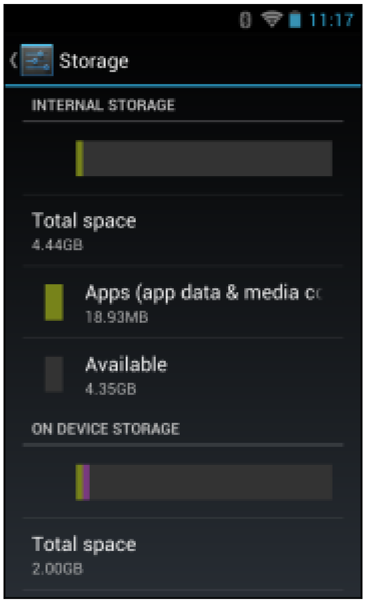
- **Available** - Displays the available space on the installed microSD card.
- **Unmount SD card** - Unmounts the installed microSD card from the MC67 so that it can be safely removed. This setting is dimmed if there is no microSD card installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase external SD card** - Permanently erases everything on the installed microSD card.

Internal Storage

The MC67 has internal storage. The internal storage content can be viewed and files copied to and from when the MC67 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 94: Internal Storage Screen



11:17

Storage

INTERNAL STORAGE

Total space
4.44GB

Apps (app data & media cc
18.93MB

Available
4.35GB

ON DEVICE STORAGE

Total space
2.00GB

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

Enterprise Folder

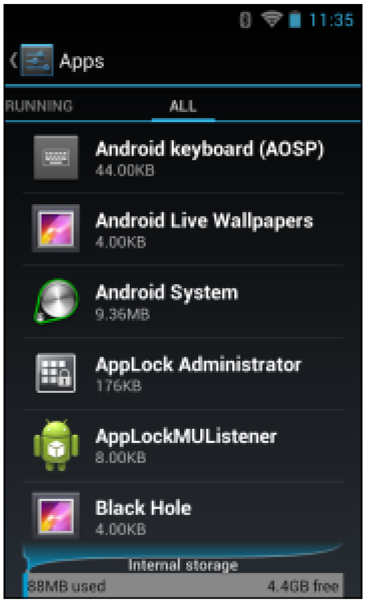
The Enterprise folder (within internal storage) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128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

Application Management

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

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

Figure 95: Manage Applications Screen



11:35

Apps

RUNNING ALL

Android keyboard (AOSP)
44.00KB

Android Live Wallpapers
4.00KB

Android System
9.36MB

AppLock Administrator
176KB

AppLockMUListener
8.00KB

Black Hole
4.00KB

Internal storage

88MB used 4.4GB free

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

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

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

When on the **Downloaded**, **All**, or **On SD card** tab, 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 125* for information about uninstalling applications.
- Touch **Clear data** to delete an application’s settings and associated data.
- Touch **Move to USB storage** or **Move to SD card** to change where some applications are stored.
- Cache If the application stores data in a temporary area, lists how much information is stored, and includes a button for clearing it.
- **Launch by default** clears If you have configured an application to launch certain file types by default, you can clear that setting here.
- **Permissions** lists the areas on the device that the application has access to.

Procedure:

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

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

Stopping an Application

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

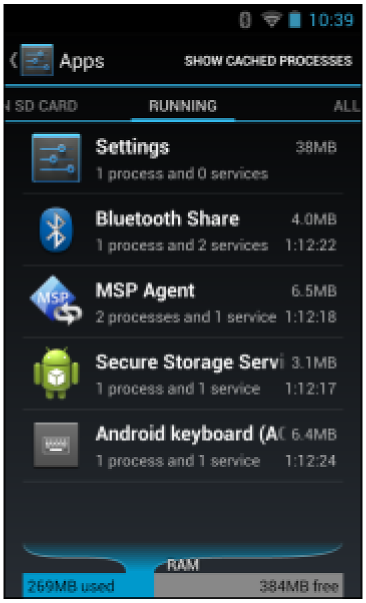
Procedure:

1 Touch ≡ > **Manage apps**.

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

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

Figure 96: Running Applications



Settings	1 process and 0 services	38MB
Bluetooth Share	1 process and 2 services	4.0MB 1:12:22
MSP Agent	2 processes and 1 service	6.5MB 1:12:18
Secure Storage Servi	1 process and 1 service	3.1MB 1:12:17
Android keyboard (A(	1 process and 1 service	6.4MB 1:12:24

269MB used 384MB free

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

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

Touch **Stop**.

Changing Application Location

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

Procedure:

1 Touch ≡ > **Manage apps**.

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

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

Applications that are stored on the microSD card are checked.

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

3 Touch an application in the list.

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

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

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

Managing Downloads

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

Procedure:

1 Touch ⊞.

2 Touch ⬇.

3 Touch an item to open it.

4 Touch headings for earlier downloads to view them.

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

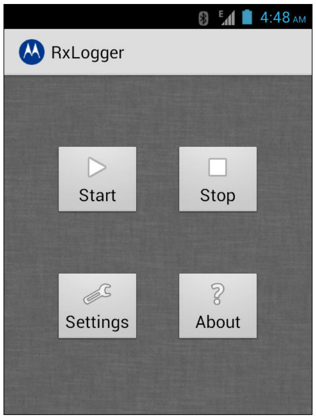
6 Touch **Sort by size** or **Sort by time** to switch back and forth.

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

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).

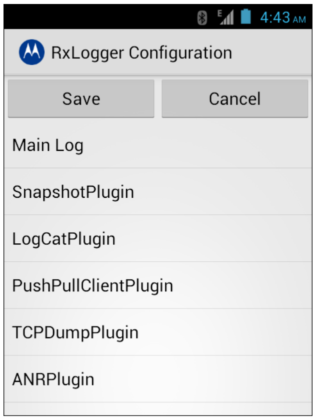
Figure 97: RxLogger



RxLogger Configuration

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

Figure 98: RxLogger Configuration Screen



Main Log Plug-in

The Main log presents a high level timeline 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.

- **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 to use the default external storage directory which is queried from the Android system.
- **Log base filename** - The base filename to use for the CSV file before appending the index number of that particular log file. For example, if the base filename is `Resource` and we are rotating through two log files, the actual filename will be: `Resource0.csv`and `Resource1.csv`.
- **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.
- **Output** - The output is a set of comma separated files containing the requested data. The number of files and the file size is determined by the configuration. These files can be viewed using Microsoft Excel.

Snapshot 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.
- **Log file count** - The number of snapshot files to keep on the filesystem. Once the maximum number of files is reached, the existing files will start to be overwritten.
- **Log CPU usage** - Enables detailed per process CPU logging in the snapshot.
- **Log memory usage** - Enables logging of detailed per process memory usage in the snapshot.
- **Log power info** - Enables logging of detailed power information including battery life, on time, charging, and wake locks.
- **Log processes** - Enables dumping the complete process list in the snapshot.
- **Log threads** - Enables dumping all processes and their threads in the snapshot.
- **Log system properties** - Enables dumping of all system properties on the device. This includes build/version information as well as state information.
- **Log network info** - Enables dumping of all available network interfaces and the routing table.
- **Log filesystem info** - Enables dumping of the available volumes on the file system and the free storage space for each.
- **Log 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.
- **Output** - The snapshot plug-in outputs a series of individual snapshot files. Every snapshot creates a new file and each file is not limited in size. The disk usage is managed by keeping a pool of log files with a configurable size.

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.

- **Log path** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.
- **Enable logcat** - Enables logging for this logcat buffer.
- **Log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
- **Log filename** - Specifies the base log filename for this logcat buffer. The current file count is 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.
- **Max log size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Output** - The logcat plug-in outputs a series of text files in accordance with the configuration. The files contain the output of the logcat buffer flushed at the specified interval.

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.

- **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 push directory** - Specifies the local directory to push files from.
- **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 filed 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.

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.

- **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.
- **Output** - The TCPDump plug-in outputs a set of .cap files according to the configurable options. These are binary files and can be opened with Wireshark tool.

ANR Plugin

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.

- **Log path** - Specifies the default log path to store the ANR log files.
- **Max file size** - Specifies the maximum file size, in killobytes, 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.
- **Output** - The ANR plug-in creates text files in the specified log directory that contain the call stacks of application's that have been shut down by the system due to an ANR event.

Kernal Plug-in

- **Enable Plugin** - Enables logging for this kernal buffer.
- **Log path** - Specifies the high level log path for storage of all kernal logs. This setting applies globally to all kernal buffers.
- **Kernal Log filename** - Specifies the base log filename for this kernal buffer. The current file count is appended to this name.
- **Max Kernal log size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Kernal Log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.
- **Kernal 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.
- **Output** - The kernal plug-in outputs a series of text files in accordance with the configuration. The files contain the output of the kernal buffer flushed at the specified interval.

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 the 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

Procedure:

1. Touch ⊞.
2. Touch Ⓜ.
3. Touch **Start**.
4. Touch ⌂.

Disabling Logging

Procedure:

1. Touch ⊞.
2. Touch Ⓜ.
3. Touch **Stop**.
4. Touch ⌂.

Extracting Log Files

Procedure:

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 MC67

For trouble-free service, observe the following tips when using the MC67:

- Do not scratch the screen of the MC67. When working with the MC67, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the MC67 screen. Motorola recommends using a screen protector, p/n KT-129195-01R.
- The touch-sensitive screen of the MC67 is glass. Do not to drop the MC67 or subject it to strong impact.
- Protect the MC67 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 MC67 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the MC67. If the surface of the MC67 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.
- A screen protector is applied to the MC67. Motorola recommends using this to minimize wear and tear. Screen protectors enhance the usability and durability of touch screen displays. Benefits include:
- Protection from scratches and gouges
- Durable writing and touch surface with tactile feel
- Abrasion and chemical resistance
- Glare reduction
- Keeping the device's screen looking new
- Quick and easy installation.

Battery Safety Guidelines

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Follow battery usage, storage, and charging guidelines found in this guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between +32 ºF and +104 ºF (0 ºC and +40 ºC)
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact Motorola Solutions Global Customer Support Center.

- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- To enable authentication of an approved battery, as required by IEEE1725 clause 10.2.1, all batteries will carry a Motorola hologram. Do not fit any battery without checking it has the Motorola authentication hologram.
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, contact Motorola Solutions Global Customer Support Center to arrange for inspection.

Cleaning Instructions

Caution:

Always wear eye protection.

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

If you have to use any other solution for medical reasons please contact Motorola for more information.

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

Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite, hydrogen peroxide or mild dish soap.

Harmful Ingredients

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

Cleaning Instructions

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

Special Cleaning Notes

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

Cleaning Materials Required

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

Cleaning Frequency

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

Cleaning the MC67

Housing

Using the alcohol wipes, wipe the housing including buttons.

Display

The display can be wiped down with the alcohol wipes, but care should be taken not to allow any pooling of liquid around the edges of the display. Immediately dry the display with a soft, non-abrasive cloth to prevent streaking.

Camera and Exit Window

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

Cleaning Cradle Connectors

To clean the connectors on a cradle:

Procedure:

1. Remove the DC power cable from the cradle.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not leave any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton-tipped applicator.

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

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

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

Troubleshooting

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

MC67

Table 8: Troubleshooting the MC67

Problem	Cause	Solution
When pressing the power button the MC67 does not turn on.	Battery not charged.	Charge or replace the battery in the MC67.
	Battery not installed properly.	Install the battery properly. See *Installing the Battery on page 1-4*.
	System crash.	Perform a reset. See *Resetting the MC67 on page 29*.
When pressing the power button the MC67 does not turn on but two LEDs blink.	Battery charge is at a level where data is maintained but battery should be re-charged.	Charge or replace the battery in the MC67.
Rechargeable battery did not charge.	Battery failed.	Replace battery. If the MC67 still does not operate, perform a reset. See *Resetting the MC67 on page 29*.
	MC67 removed from cradle while battery was charging.	Insert MC67 in cradle. The 3600 mAh battery fully charges in less than six hours.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
Cannot see characters on display.	MC67 not powered on.	Press the **Power** button.
During data communication, no data transmitted, or transmitted data was incomplete.	MC67 removed from cradle or disconnected from host computer during communication.	Replace the MC67 in the cradle, or reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software was incorrectly installed or configured.	Perform setup. Refer to the *MC67 Integrator Guide* for details.
No sound.	Volume setting is low or turned off.	Adjust the volume.
MC67 shuts off.	MC67 is inactive.	The MC67 turns off after a period of inactivity. If the MC67 is running on battery power, set this period from 1 to 5 minutes, in one-minute intervals.
	Battery is depleted.	Replace the battery.
	Battery is not inserted properly.	Insert the battery properly. See *Installing the Battery on page 1-4*.
Tapping the window buttons or icons does not	Screen is not calibrated correctly.	Re-calibrate the screen. Press **Blue** key - **Backspace** key.

Table continued…

Problem	Cause	Solution
activate the corresponding feature.	The device is not responding.	Reset the device. See *Resetting the MC67 on page 29*.
A message appears stating that the MC67 memory is full.	Too many files stored on the MC67.	Delete unused memos and records. If necessary, save these records on the host computer (or use an SD card for additional memory).
	Too many applications installed on the MC67.	Remove user-installed applications on the MC67 to recover memory. Select **Settings**, then select **System** and tap the **Remove Programs** icon. Select the unused program and tap **Remove**.
The Charging/Battery Status LED flashes with the Power button is pressed and the MC67 does not turn on.	The MC67's battery is low.	Recharge the battery.
The MC67 does not decode with reading bar code.	Scanning application is not loaded.	Load a scanning application on the MC67. See your system administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Place the MC67 within proper scanning range.
	MC67 is not programmed for the bar code.	Program the MC67 to accept the type of bar code being scanned.
	MC67 is not programmed to generate a beep.	If the MC67 does not beep on a good decode, set the application to generate a beep on good decode.
	Battery is low.	If the scanner stops emitting a laser beam upon a trigger press, check the battery level. When the battery is low, the scanner shuts off before the MC67 low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or Motorola.
MC67 cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (32.8 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.

Single Slot USB Cradle

Table 9: Troubleshooting the Single Slot USB Cradle

Symptom	Possible Cause	Action
LEDs do not light when MC67 or spare battery is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	MC67 is not seated firmly in the cradle.	Remove and re-insert the MC67 into the cradle, ensuring it is firmly seated.

Table continued…

Symptom	Possible Cause	Action
	Spare battery is not seated firmly in the cradle.	Remove and re-insert the spare battery into the charging slot, ensuring it is firmly seated.
MC67 battery is not charging.	MC67 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure MC67 is seated correctly. Confirm main battery is charging. The 3600 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The MC67 is not fully seated in the cradle.	Remove and re-insert the MC67 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
Spare battery is not charging.	Battery not fully seated in charging slot.	Remove and re-insert the spare battery in the cradle, ensuring it is firmly seated.
	Battery inserted incorrectly.	Re-insert the battery so the charging contacts on the battery align with the contacts on the cradle.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
During data communication, no data transmits, or transmitted data was incomplete.	MC67 removed from cradle during communications.	Replace MC67 in cradle and retransmit.
	Communication software is not installed or configured properly.	Perform setup as described in *Single Slot USB Cradle on page 34*.

Four Slot Ethernet Cradle

Table 10: Troubleshooting the Four Slot Ethernet Cradle

Symptom	Cause	Solution
During communication, no data transmits, or transmitted data was incomplete.	MC67 removed from cradle during communications.	Replace MC67 in cradle and retransmit.
	MC67 has no active connection.	An icon is visible in the status bar if a connection is currently active.
Battery is not charging.	MC67 removed from the cradle too soon.	Replace the MC67 in the cradle. The 3600 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	MC67 is not inserted correctly in the cradle.	Remove the MC67 and reinsert it correctly. Verify charging is active.
	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).

Vehicle Cradle

Table 11: Troubleshooting the Vehicle Cradle

Symptom	Possible Cause	Action
MC67 battery charging LED does not light up.	Cradle is not receiving power.	Ensure the power input cable is securely connected to the cradle's power port.
MC67 battery is not recharging.	MC67 was removed from the cradle too soon.	Replace the MC67 in the cradle. The 3600 mAh battery fully charges in less than six hours.
	Battery is faulty.	Replace the battery.
	MC67 is not placed correctly in the cradle.	Remove the MC67 from the cradle, and re-insert correctly. If the battery still does not charge, contact customer support. The MC67 battery charging LED slowly blinks amber when the MC67 is correctly inserted and charging.
	Ambient temperature of the cradle is too warm.	Move to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).

Four Slot Battery Charger

Table 12: Troubleshooting The Four Slot Battery Charger

Symptom	Possible Cause	Action
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 3600 mAh battery fully charges in less than six 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.

Cables

Table 13: Troubleshooting the Cables

Symptom	Possible Cause	Action
MC67 battery is not charging.	MC67 was disconnected from AC power too soon.	Connect the power cable correctly. Confirm main battery is charging. The 3600 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The MC67 is not fully attached to power.	Detach and re-attach the power cable to the MC67, ensuring it is firmly connected.
During data communication, no data transmits, or transmitted data was incomplete.	Cable was disconnected from MC67 during communications.	Re-attach the cable and retransmit.

Table continued…

Symptom	Possible Cause	Action
	Incorrect cable configuration.	See the system administrator.
	Communication software is not installed or configured properly.	Perform setup as described in *Cables on page 49*.

Magnetic Stripe Reader

Table 14: Troubleshooting the Magnetic Stripe Reader

Symptom	Possible Cause	Action
MSR cannot read card.	MSR removed from MC67 during card swipe.	Reattach MSR to MC67 and reswipe the card.
	Faulty magnetic stripe on card.	See the system administrator.
	MSR application is not installed or configured properly.	Ensure the MSR application is installed on the MC67. Ensure the MSR application is configured correctly.
MC67 battery is not charging.	MC67 was removed from MSR or MSR was unplugged from AC power too soon.	Ensure MSR is receiving power. Ensure MC67 is attached correctly. Confirm main battery is charging. The 3600 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The MC67 is not fully attached to the MSR.	Detach and re-attach the MSR to the MC67, ensuring it is firmly connected.
During data communication, no data transmits, or transmitted data was incomplete.	MC67 detached from MSR during communications.	Reattach MC67 to MSR and retransmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software is not installed or configured properly.	Perform setup as described in the *MC67 Integrator Guide*.

Chapter 9

Technical Specifications

The following sections provide technical specification for the device.

MC67 Technical Specifications

The following tables summarize the EDA's intended operating environment and technical hardware specifications.

MC67

Table 15: MC67 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions	Height: 16.2 cm (6.38 in.) Width: 7.7 cm (3.03 in.) Depth: 3.35 cm (1.32 in.)
Weight	385 g (13.5 oz.)
Display	Color 3.5" video graphics adapter (VGA) with backlight, 65K colors, 480 W x 640 L
Touch Panel	Glass analog resistive touch
Backlight	Light Emitting Diode (LED) backlight
Battery Pack	Rechargeable Lithium Ion 3.7V, 3600 mAh battery
Backup battery	Nickel–metal hydride (Ni-MH) battery (rechargeable) 15 mAh 2.8V (non-user accessible or replaceable)
Expansion Slot	micro Secure Digital (SD) slot (supports up to 32 GB)
Connection Interface	Universal Serial Bus (USB) 2.0 High Speed (host and client)
Notification	Audible tone plus multi-color LEDs
Keypad Options	numeric, QWERTY and Direct Store Delivery (DSD)
Audio	Dual microphone support with noise cancellation; vibrate alert; speaker; Bluetooth headset
Performance Characteristics	
CPU	Dual-core OMAP 4, 1 GHz

Table continued…

Item	Description
Operating System	Android-based AOSP V4.1.1
Memory	1 GB Random Access Memory (RAM)/8 GB Flash
Output Power	USB - 5 VDC @ 300 mA max
User Environment	
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0° C to 40° C (32°F to 104°F)
Humidity	5 to 85% non-condensing
Drop Specification	Multiple 2.4 m (8 ft.) drops per MIL-STD 810G at room temperature. 1.8 m (6 ft.) across operating temperature per MIL-STD 810G
Tumble	1,000 1.6 ft./0.5 meter tumbles at room temperature; per applicable IEC tumble specifications
Electrostatic Discharge (ESD)	+/-15kVdc air discharge, +/-8kVdc direct discharge, +/-8kVdc indirect discharge
Sealing	IP65 and IP67 per IEC specification.
Vibration	4 g's PK Sine (5 Hz to 2 kHz); 0.04g2/Hz Random (20 Hz to 2 kHz); 60 minute duration per axis, 3 axis
Thermal Shock	-40° C to 70° C (-40° F to 158° F) rapid transition
Motorola Interactive Sensor Technology (IST)	
Motion Sensor	3-axis accelerometer provides motion-sensing for dynamic screen orientation and power management
Light Sensor	Ambient light sensor to auto adjust display backlight brightness
Digital Compass	Navigation aid for users
Wireless WAN Data and Voice Communications	
Radio	4G HSPA+
Frequency Band	UMTS/HSDPA and HSUPA: 850, 900, 1900 and 2100 MHz GSM/ EDGE: 850, 900, 1800 and 1900 MHz
Wireless LAN Data and Voice Communications	
Radio	IEEE® 802.11a/b/g/n
Data Rates Supported	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Operating Channels	Chan 36 - 165 (5180 - 5825 MHz) Chan 1 - 13 (2412 - 2472 MHz) Chan 14 (2484 MHz) Japan only Actual operating channels/frequencies depend on regulatory rules and certification agency
Security	**Security Modes:** Legacy, WPA and WPA2

Table continued…

Item	Description
	Encryption: WEP (40 and 128 bit), TKIP and AES **Authentication:** LEAP, EAP-FAST (MS-CHAPv2, GTC), PEAP (MSCHAPv2, EAP-GTC), TLS, TTLS (PAP, MS-CHAP, MS-CHAPv2)
Voice Communications	Voice-over-IP ready, Wi-Fi™-certified, IEEE 802.11a/b/g/n direct sequence wireless LAN, Wi-Fi Multimedia™ (WMM and WMM-PS)
Wireless PAN Data and Voice Communications	
Bluetooth	Class II, v2.1 with Enhanced Data Rate (EDR)
Global Positioning System	
GPS	Integrated stand-alone or Assisted-GPS (A-GPS)
Data Capture Specifications	
2D Imager	SE4500-SR
Data Types	1D and 2D bar codes, photographs, video, signatures and documents.
Voice and Audio	
VoWWAN; VoWLAN; PTT-ready, VoIP-ready; high-quality speakerphone; wireless (Bluetooth) headset support; headset/speakerphone modes	
2D Imager Engine (SE4500-SR) Specifications	
Field of View	Horizontal - 39.6° Vertical - 25.7°
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: 19 cm (7.5 in.)
Aiming Element (VLD)	655 nm +/- 10 nm
Illumination Element (LED)	625 nm +/- 5 nm
Camera Specifications	
Resolution	8 Mega pixel

Table 16: Data Capture Supported Symbologies

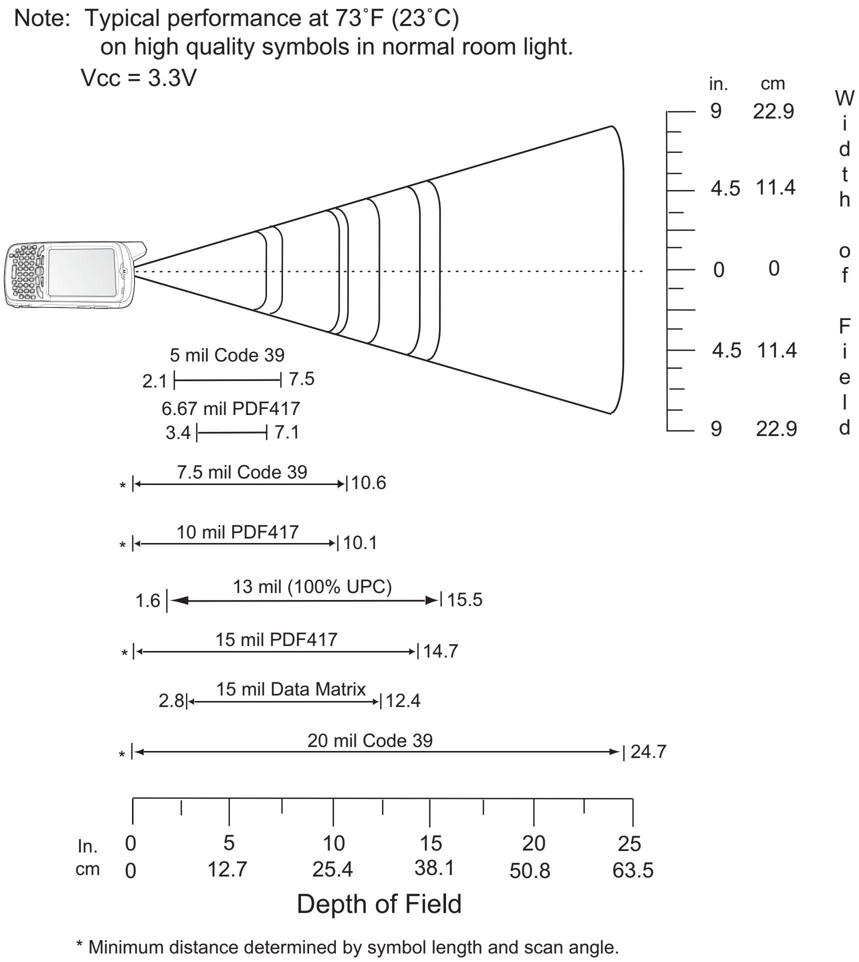
Item	Description
1D Bar Codes	Chinese 2 of 5, Code 128, Coupon Code, EAN-13, GS1 DataBar Expanded, GS1 DataBar Limited, Korean 2 of 5, TLC39, UPCA, UPC/EAN Supplementals, Codabar, Code 39, Discrete 2 of 5, GS1 DataBar, GS1 DataBar Expanded Stacked, Interleaved 2 of 5, Matrix 2 of 5, Trioptic 39, UPCE, Webcode, Code 11, Code 93, EAN-8, GS1 DataBar 14, ISBT 128, MSI, UCC/EAN 128, UPCE1
2D Bar Codes	Australian Postal, Composite AB, Dutch Postal, Maxi Code, PDF-417, UK Postal, Aztec, Composite C, Japanese Postal, Micro PDF-417, QR Code, US Postnet, Canadian Postal, Data Matrix, Linked Aztec, microQR, US Planet, USPS 4-state (US4CB),

SE4500–SR Decode Zone

The figure below shows the decode zone for the SE4500-SR. Typical values appear. *Table 17: SE4500-SR Decode Distances on page 149* 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.

Note: Typical performance at 73°F (23°C) on high quality symbols in normal room light.

Figure 99: SE-4500SR Decode Zone



Note: Typical performance at 73˚F (23˚C) on high quality symbols in normal room light.

Vcc = 3.3V

* Minimum distance determined by symbol length and scan angle.

Table 17: SE4500-SR Decode Distances

Symbol Density/ Bar Code Type	Bar Code Content/ Contrast Note 2	Typical Working Ranges	
		Near	Far
5.0 mil Code 39	ABCDEFGH 80% MRD	2.1 in 5.33 cm	7.5 in 19.05 cm
6.67 mil PDF417	4 Col, 20 Rows 80% MRD	3.4 in 8.64 cm	7.1 in 18.03 cm
7.5 mil Code 39	ABCDEF 80% MRD	Note 1	10.6 in 26.92 cm
10 mil PDF417	3 Col, 17 Rows 80% MRD	Note 1	10.1 in 25.65 cm
13 mil UPC-A	012345678905 80% MRD	1.6 in 5.08 cm	15.5 in 39.37 cm
15 mil PDF417	80% MRD	Note 1	14.7 in 37.34 cm
15 mil Data Matrix	18 x 18 Modules 80% MRD	2.8 in 7.11 cm	12.4 in 31.50 cm
20 mil Code 39	123 80% MRD	Note 1	24.7 in 62.74 cm

Note:

1 Near distances are field-of-view (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.

MC67 External Connector Pin-Outs

Table 18: Table A-6 External Connector Pin-Outs

Pin	Description
1	External Trigger/Cradle Detect
2	USB_ID
3	5.4 VDC
4	USB_VCC
5	USB_D-
6	USB_D+

Table continued…

Pin	Description
7	Ground

MC67 Accessory Specifications

Single Slot USB Cradle

Table 19: Single Slot USB Cradle Technical Specifications

Feature	Description
Dimensions	Height: 7.1 cm (2.80 in.) Width: 11.0 cm (4.33 in.) Depth: 15.0 cm (5.91 in.)
Weight	210 g (7.41 oz)
Input Voltage	12 VDC
Power Consumption	30 watts
Interface	USB
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Four Slot Battery Charger

Table 20: Four Slot Battery Charger Technical Specifications

Feature	Description
Dimensions	Height: 4.7 cm (1.85 in.) Width: 15.5 cm (6.10 in.) Depth: 21.0 cm (8.27 in.)
Weight	384 g (13.55 oz)
Input Voltage	12 VDC
Power Consumption	30 watts
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)

Table continued…

Feature	Description
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Four Slot Charge Only Cradle

Table 21: Four Slot Charge Only Cradle Technical Specifications

Feature	Description
Dimensions	Height: 13.7 cm (5.39 in.) Width: 46.8 cm (18.43 in.) Depth: 9.9 cm (3.90 in.)
Weight	1115 g (39.33 oz)
Input Voltage	12 VDC
Power Consumption	100 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Four Slot Ethernet Cradle

Table 22: Four Slot Ethernet Cradle Technical Specifications

Feature	Description
Dimensions	Height: 13.7 cm (5.39 in.) Width: 46.8 cm (18.43 in.) Depth: 9.9 cm (3.90 in.)
Weight	1115 g (39.33 oz)
Power	12 VDC
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)

Table continued…

Feature	Description
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Magstripe Reader

Table 23: Magstripe Reader (MSR) Technical Specifications

Feature	Description
Dimensions	8.4 cm x 9.4 cm (3.3 in. x 3.7 in.)
Weight	79.4 g (2.8 oz)
Interface	Serial with baud rate up to 19,200
Format	ANSI, ISO, AAMVA, CA DMV, user-configurable generic format
Swipe Speed	5 to 50 in. (127 to 1270 mm) /sec, bi-directional
Decoders	Generic, Raw Data
Mode	Buffered, unbuffered
Track Reading Capabilities	Tracks 1 and 3: 210 bpi Track 2: 75 and 210 bpi, autodetect
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	5% to 95% non-condensing
Drop	4 ft. (1.22 m) drops to concrete
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Vehicle Cradle

Table 24: Vehicle Cradle Technical Specifications

Feature	Description
Dimensions	Height: 10.4 cm (4.09 in.) Width: 11.1 cm (4.37 in.) Depth: 6.9 cm (2.72 in.)
Weight	240 g (8.47 oz)

Table continued…

Feature	Description
Power	9- 32 VDC
Operating Temperature	-20 °C to 50 °C (-4 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °FC to 104 °F)
Humidity	10% 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

Cables

Table 25: USB Charging Cable Technical Specifications

Feature	Description
Length	161.9 cm (63.74 in.)
Operating Temperature	-10 °C to 50 °C (14 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Table 26: Charge Only Cable Technical Specifications

Feature	Description
Length	28.0 cm (11.00 in.)
Operating Temperature	-10 °C to 50 °C (14 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Table 27: Auto Charge Cable Technical Specifications

Feature	Description
Length	169.0 cm (66.54 in.)
Input Voltage	12 - 24 VDC
Operating Temperature	-10 °C to 50 °C (14 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)

Table continued…

Feature	Description
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Index