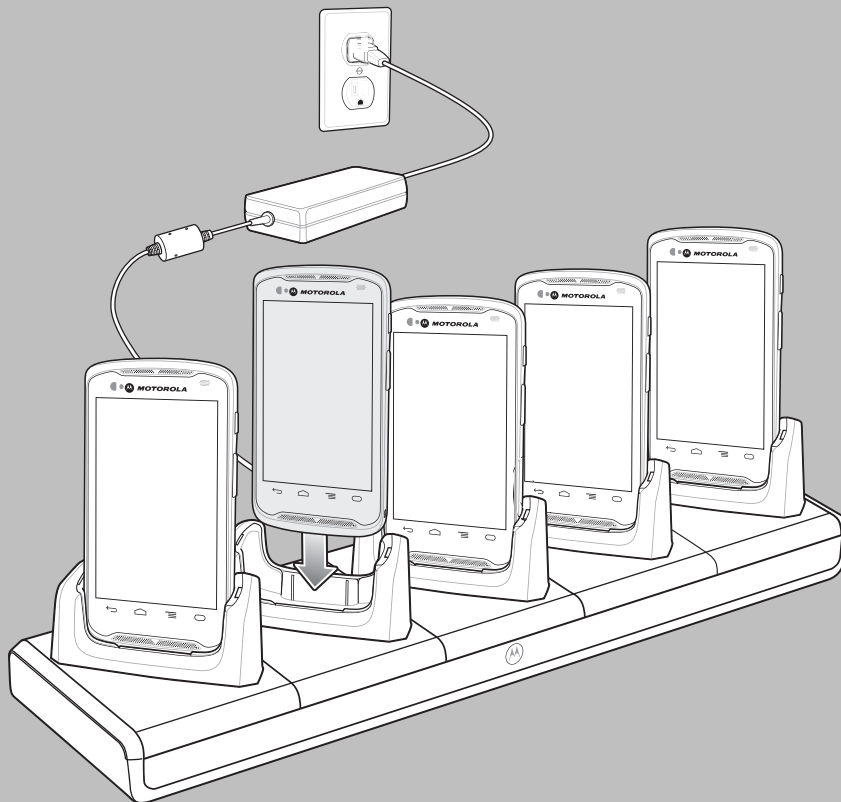


# TC55 INTEGRATOR GUIDE





# 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.

© 2013 Motorola Solutions, Inc. All Rights Reserved

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	10/15/2013	Initial release.



# Contents

<b>Copyrights</b> .....	<b>3</b>
<b>Revision History</b> .....	<b>5</b>
<b>List of Tables</b> .....	<b>11</b>
<b>List of Figures</b> .....	<b>13</b>
<b>About This Guide</b> .....	<b>17</b>
Documentation Set.....	17
Configurations.....	17
Chapter Descriptions.....	18
Notational Conventions.....	18
Icon Conventions.....	18
Service Information.....	19
<b>Chapter 1: Getting Started</b> .....	<b>21</b>
Unpacking.....	21
Setup.....	21
Installing the SIM Card.....	21
Installing an Optional microSD Card.....	24
Installing the Battery.....	26
Charging the Battery.....	28
Charging the Main Battery.....	28
Charging LED Status.....	29
Charging Temperature.....	29
Powering On the TC55.....	30
Replacing the 2,940 mAh Battery.....	30
Replacing the 4,410 mAh Battery.....	32
Replacing the microSD Card.....	34
Resetting the Device.....	36
Performing a Soft Reset.....	36
Performing a Hard Reset.....	36
Performing an Enterprise Reset.....	37
Performing a Factory Reset.....	38
<b>Chapter 2: Accessories</b> .....	<b>39</b>
TC55 Accessories.....	39
Five Slot Charge Only Cradle.....	40
Installing a Cup.....	41
<b>Chapter 3: USB Communication</b> .....	<b>45</b>
Connecting to a Host Computer via USB.....	45
Connecting to the TC55 as a Media Device.....	45
Connecting to the TC55 as an Installer.....	45
Disconnect from the Host Computer.....	46
<b>Chapter 4: DataWedge Configuration</b> .....	<b>47</b>
Basic Scanning.....	47
Using the Camera.....	47

Using the Imager.....	48
Profiles.....	49
Plug-ins.....	49
Profiles Screen.....	50
Disabling DataWedge.....	52
Creating a New Profile.....	52
Profile Configuration.....	53
Bar Code Input.....	53
Keystroke Output.....	60
Intent Output.....	61
Intent Overview.....	62
IP Output.....	63
Generating Advanced Data Formatting Rules.....	64
Configuring ADF Plug-in.....	64
Creating a Rule.....	65
Defining a Rule.....	65
Defining Criteria.....	66
Defining an Action.....	67
Deleting a Rule.....	68
Order Rules List.....	68
Deleting an Action.....	69
ADF Example.....	69
DataWedge Settings.....	72
Importing a Configuration File.....	73
Exporting a Configuration File.....	73
Importing a Profile File.....	73
Exporting a Profile.....	73
Restoring DataWedge.....	74
Configuration and Profile File Management.....	74
Programming Notes.....	75
Overriding Trigger Key in an Application.....	75
Capture Data and Taking a Photo in the Same Application.....	75
Disable DataWedge on TC55 and Mass Deploy.....	75
<b>Chapter 5: Administrator Utilities.....</b>	<b>77</b>
Required Software.....	77
On-device Application Installation.....	77
Multi-user/AppLock Configuration.....	77
Enterprise Administrator Application.....	78
Creating Users.....	78
Adding Packages.....	79
Creating Groups.....	80
Creating Remote Authentication.....	80
Save Data.....	81
Exporting File.....	81
Importing User List.....	81
Importing Group List.....	82
Importing Package List.....	82
Editing a User.....	82
Deleting a User.....	82
Editing a Group.....	82
Deleting a Group.....	82
Editing a Package.....	83
Deleting a Package.....	83
MultiUser Administrator.....	83

Importing a Password.....	83
Disabling the Multi-user Feature.....	84
Enabling Remote Authentication.....	84
Disabling Remote Authentication.....	85
Enabling Data Separation.....	85
Disabling Data Separation.....	85
Delete User Data.....	86
Capturing a Log File.....	86
AppLock Administrator.....	86
Installing Groups and White Lists.....	86
Enabling Application Lock.....	87
Disabling Application Lock.....	87
Manual File Configuration.....	88
Determining Applications Installed on the Device.....	89
Secure Storage.....	89
Installing a Key.....	90
Viewing Key List.....	90
Deleting a Key.....	90
Volumes.....	91
Creating Volume Using EFS File.....	91
Creating a Volume Manually.....	91
Mounting a Volume.....	92
Listing Volumes.....	92
Unmounting a Volume.....	92
Deleting a Volume.....	93
Encrypting an SD Card.....	93
Creating an EFS File.....	93
Off-line Extraction Tool.....	93
Creating an Image.....	94
Mounting an Image.....	94
Unmounting an Image.....	95

## **Chapter 6: MLog Manager..... 97**

Exporting QXDM Logs.....	98
--------------------------	----

## **Chapter 7: Settings..... 99**

Location Settings.....	99
Screen Unlock Settings.....	100
Single User Mode.....	100
Set Screen Unlock Using PIN.....	100
Set Screen Unlock Using Password.....	101
Set Screen Unlock Using Pattern.....	102
Multiple User Mode.....	103
Passwords.....	104
Button Programming.....	104
Programming a Button.....	104
Exporting a Programmable Key Configuration File.....	105
Importing a Programmable Key Configuration File.....	105
Language Usage.....	106
Changing the Language Setting.....	106
Adding Words to the Dictionary.....	106
Keyboard Settings.....	106
About Phone.....	106

<b>Chapter 8: Application Deployment.....</b>	<b>109</b>
Security.....	109
Secure Certificates.....	109
Installing a Secure Certificate.....	109
Configuring Credential Storage Settings.....	110
Development Tools.....	110
ADB USB Setup.....	111
Application Installation.....	111
Installing Applications Using the USB Connection.....	112
Installing Applications Using the Android Debug Bridge.....	112
Uninstalling an Application.....	113
Mobility Services Platform.....	113
Updating the System.....	114
Storage.....	115
Random Access Memory.....	115
Internal Storage.....	115
External Storage.....	117
Enterprise Folder.....	117
Application Management.....	117
Viewing Application Details.....	118
Stopping an Application.....	119
Changing Application Location.....	119
Managing Downloads.....	120
<b>Chapter 9: Maintenance and Troubleshooting.....</b>	<b>121</b>
Maintaining the TC55.....	121
Battery Safety Guidelines.....	121
Cleaning Instructions.....	122
Cleaning the TC55.....	123
Connector Cleaning.....	123
Cleaning Cradle Connectors.....	123
Troubleshooting.....	124
Troubleshooting the TC55.....	124
Five-Slot Charge Only Cradle CRDUNIV-55-5000R Troubleshooting.....	126
<b>Chapter 10: Technical Specifications.....</b>	<b>127</b>
TC55 Technical Specifications.....	127
TC55 Decode Zone.....	130
SE-655 Decode Distances.....	131
TC55 Connector Pin-Outs.....	132
Five-Slot Charge Only Cradle CRDUNIV-55-5000R Technical Specifications.....	134
<b>Chapter 11: Keypad Remap Strings.....</b>	<b>135</b>

## List of Tables

Table 1: Charging LED Status .....	29
Table 2: TC55 Accessories .....	39
Table 3: ADF Supported Actions .....	68
Table 4: Troubleshooting the TC55 .....	124
Table 5: Troubleshooting the Five-Slot Charge Only Cradle .....	126
Table 6: TC55 Technical Specifications .....	127
Table 7: SE-655 Decode Distances .....	131
Table 8: Headset Connector Pin-Outs .....	133
Table 9: Power Connector Pin-Outs .....	133
Table 10: micro-B USB Connector Pin-Outs .....	133
Table 11: Five-Slot Charge Only Cradle Technical Specifications .....	134
Table 12: Remap Key Event/Scancodes .....	135



## List of Figures

Figure 1: Manufacturing Label Location .....	19
Figure 2: Unlock SIM Card Holder .....	22
Figure 3: Install SIM Card .....	23
Figure 4: Close SIM Card Holder .....	23
Figure 5: Lock SIM Card Holder .....	24
Figure 6: Unlock microSD Card Door .....	25
Figure 7: Insert microSD Card .....	25
Figure 8: Lock SD Card Door .....	26
Figure 9: Inserting the 2,940 mAh Battery .....	26
Figure 10: Inserting the 4,410 mAh Battery .....	27
Figure 11: Install the Battery Cover .....	27
Figure 12: Secure Cover .....	28
Figure 13: Connect the Rugged Charge Cable .....	29
Figure 14: Remove the Battery Cover .....	30
Figure 15: Remove 2,940 mAh Battery .....	31
Figure 16: Inserting the 2,940 mAh Battery .....	31
Figure 17: Align the Battery Cover .....	31
Figure 18: Secure the Battery Cover .....	32
Figure 19: Remove the Battery Door .....	32
Figure 20: Remove 4,410 mAh Battery .....	33
Figure 21: Inserting the 4,410 mAh Battery .....	33
Figure 22: Align the Battery Cover .....	33
Figure 23: Secure the Battery Cover .....	34
Figure 24: Unlock microSD Card Door .....	35
Figure 25: Insert microSD Card .....	35
Figure 26: Lock microSD Card Cover .....	36
Figure 27: Three Button Reset .....	37
Figure 28: System Recovery Screen .....	37
Figure 29: System Recovery Screen .....	38
Figure 30: Five Slot Charge Only Cradle .....	40
Figure 31: Five Slot Charge Only Cradle Power Connections .....	41
Figure 32: Remove Cup Insert .....	41

Figure 33: Five Slot Charge Only Cradle Cup Installation .....	42
Figure 34: Securing Cup to Base .....	42
Figure 35: Data Capture with Camera .....	48
Figure 36: Data Capture .....	48
Figure 37: DataWedge Profiles Screen .....	51
Figure 38: Profile Context Menu .....	51
Figure 39: DataWedge Options Menu .....	52
Figure 40: New Profile Name Dialog Box .....	53
Figure 41: Profile Configuration Screen .....	53
Figure 42: IP Output Screen .....	64
Figure 43: Advanced Data Formatting Screen .....	65
Figure 44: Rule List Screen .....	66
Figure 45: Criteria Screen .....	66
Figure 46: Barcode Input Screen .....	67
Figure 47: ADF Sample Screen .....	71
Figure 48: Sample Bar Code .....	71
Figure 49: Formatted Data .....	72
Figure 50: DataWedge Settings Window .....	72
Figure 51: Enterprise Administrator Window .....	78
Figure 52: User Manager Window .....	79
Figure 53: Package Information Window .....	79
Figure 54: Group Manager Window .....	80
Figure 55: Authentication Window .....	81
Figure 56: MultiUser Administrator Screen .....	83
Figure 57: MultiUser Login Screen .....	84
Figure 58: AppLock Administrator Screen .....	87
Figure 59: Enter Key Dialog Box .....	90
Figure 60: List of Keys .....	90
Figure 61: Enter Parameter To Create Volume Dialog Box .....	92
Figure 62: Location Access Screen .....	99
Figure 63: PIN Screen .....	101
Figure 64: Password Screen .....	102
Figure 65: Choose Your Pattern Screen .....	103
Figure 66: Pattern Screen .....	103
Figure 67: Programmable Keys Screen .....	104

Figure 68: Remapped Button .....	105
Figure 69: Accept Installation Screen .....	112
Figure 70: Downloaded Screen .....	113
Figure 71: System Recovery Screen .....	114
Figure 72: Running Screen .....	115
Figure 73: Storage Settings - Internal Storage .....	116
Figure 74: Storage Settings - Internal Storage .....	116
Figure 75: Storage Settings .....	117
Figure 76: Manage Applications Screen .....	118
Figure 77: Running Applications .....	119
Figure 78: SE-655 Decode Zone .....	131
Figure 79: Headset Connector .....	132
Figure 80: Power Connector .....	133
Figure 81: micro-B USB Connector .....	133



# About This Guide

This guide provides information about setting up and configuring the TC55 and its accessories.



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

## Documentation Set

---

The documentation set for the TC55 provides information for specific user needs, and includes:

- *TC55 Quick Start Guide* - describes how to get the device up and running.
- *TC55 User Guide* - describes how to use the device.
- *TC55 Integrator Guide* - describes how to set up the device and accessories.

## Configurations

---

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
TC55AH	WLAN: 802.11a/b/g/n  WPAN: Bluetooth v4.0 and NFC  WWAN: LTE	4.3" color WVGA	1 GB RAM / 8 GB Flash	Linear imager and camera or camera	Android-based, Android Open- Source Project 4.1.2
TC55BH	WLAN: 802.11a/b/g/n  WPAN: Bluetooth v4.0 and NFC  WWAN: HSPA+	4.3" color WVGA	1 GB RAM / 8 GB Flash	Linear imager and camera or camera	Android-based, Android Open- Source Project 4.1.2

---

## 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.

## Chapter Descriptions

---

Topics covered in this guide are as follows:

- *Getting Started on page 21* provides information on getting the TC55 up and running for the first time.
- *Accessories on page 39* describes the available accessories and how to use them with the TC55.
- *USB Communication on page 45* describes how to connect the TC55 to a host computer using USB.
- *DataWedge Configuration on page 47* describes how to use and configure the DataWedge application.
- *Administrator Utilities on page 77* provides information for using the suite of administrative tools for configuring the TC55.
- *MLog Manager on page 97* provides information for using the MLog application.
- *Settings on page 99* provides the settings for configuring the TC55.
- *Application Deployment on page 109* provides information for developing and managing applications.
- *Maintenance and Troubleshooting on page 121* includes instructions on cleaning and storing the TC55, and provides troubleshooting solutions for potential problems during TC55 operation.
- *Technical Specifications on page 127* provides the technical specifications for the TC55.
- *Keypad Remap Strings on page 135* provides a list of remap strings used when remapping keys.

## Notational Conventions

---

The following conventions are used in this document:

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

## Icon Conventions

---

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



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



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



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

## Service Information

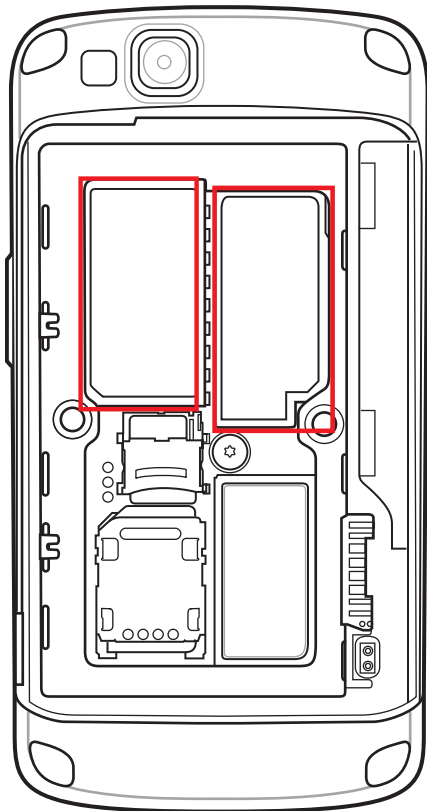
---

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

When contacting Motorola Solutions Global Customer Support Center, please have the following information available:

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

**Figure 1: Manufacturing Label Location**



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

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

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



# Chapter 1

## Getting Started

This chapter provides the features of the TC55 and explains how to set it up for the first time.

### Unpacking

---

Carefully remove all protective material from the TC55 and save the shipping container for later storage and shipping.

Verify the following items are in the box:

- TC55
- Lithium-ion battery (2,940 mAh or 4,410 mAh)
- Charge Cable
- Quick Start Guide
- Regulatory Guide.



**Note:** Power Supply, p/n PWRS-124306–01R, is required and must be purchased separately.

Inspect the equipment for damage. If any equipment is missing or damaged, contact the Motorola Solutions Global Customer Support Center immediately. See [Service Information on page 19](#) for contact information.

### Setup

---

To start using the TC55 for the first time:

- Install the SIM Card
- Install microSD card (optional)
- Install the battery
- Charge the TC55
- Power on the TC55.

### Installing the SIM Card



**Caution:**

For proper electrostatic discharge (ESD) precautions to avoid damaging the SIM card. Proper ESD precautions include, but not limited to, working on an ESD mat and ensuring that the user is properly grounded.



**Note:**

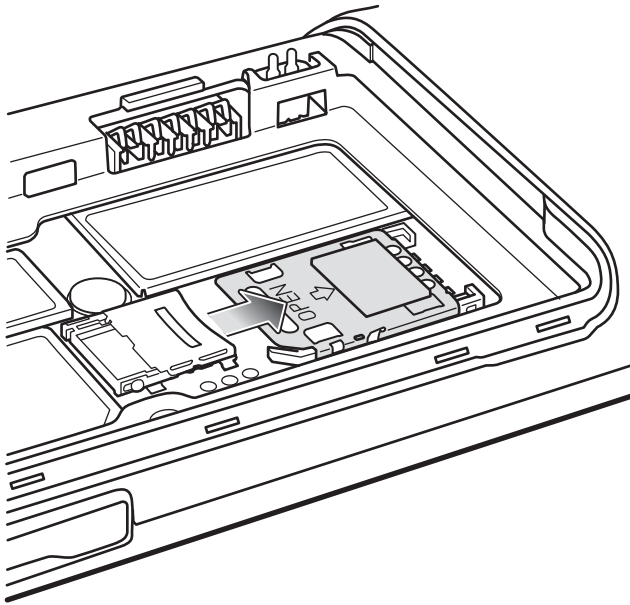
The TC55 accepts a full size SIM card. If using a micro or nano SIM card, a third-party SIM adapter is required.

The TC55 requires an activated SIM card. Obtain the card from a service provider.

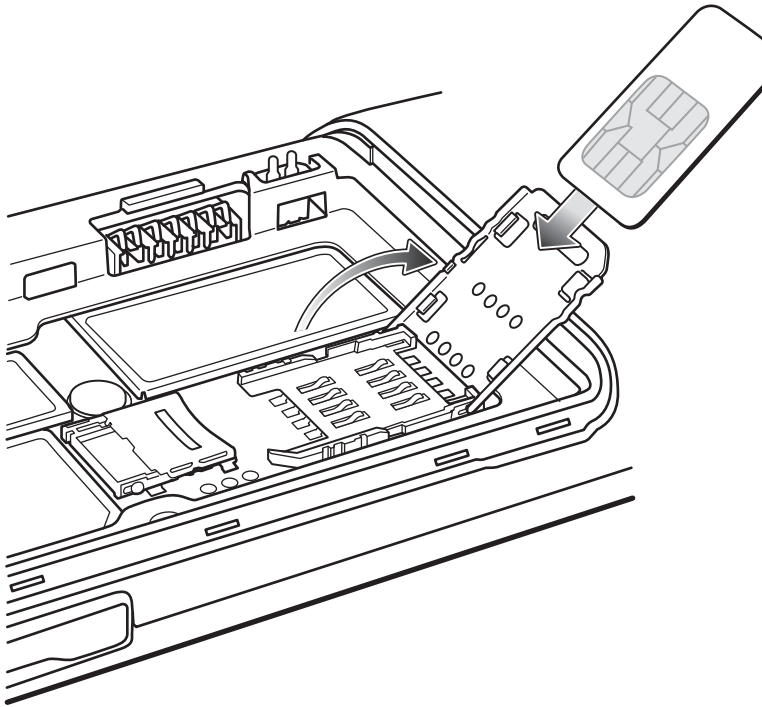
**Procedure:**

- 1 Slide the SIM card holder toward the bottom of the TC55 to unlock.

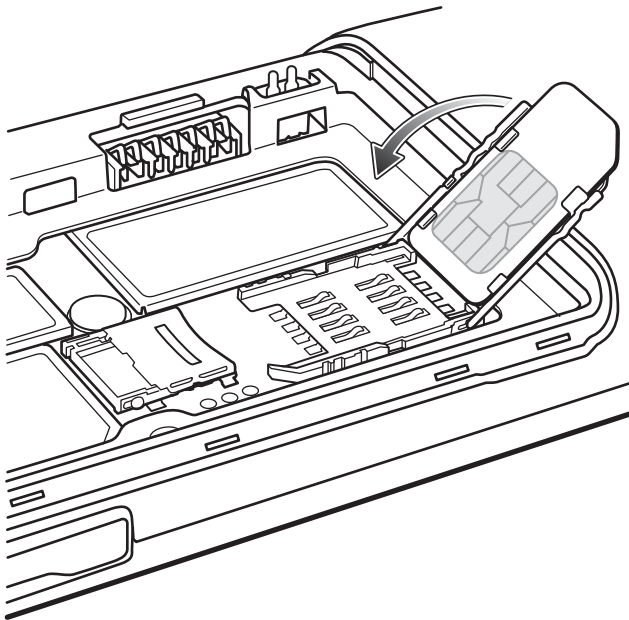
**Figure 2: Unlock SIM Card Holder**



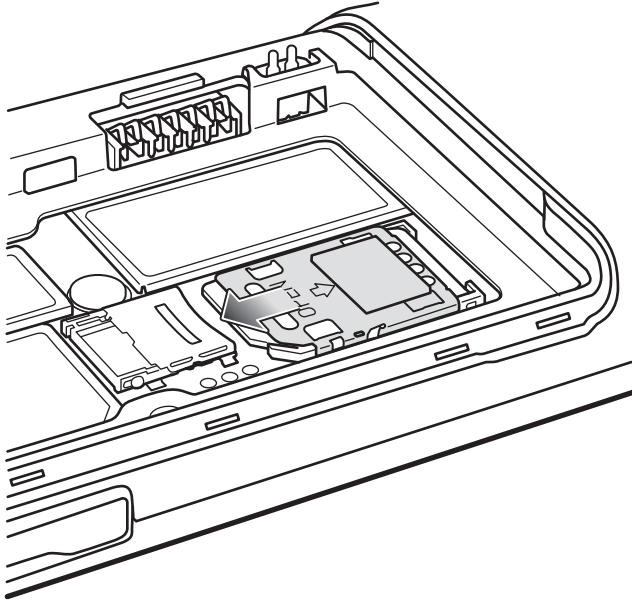
- 2 Lift the SIM door.
- 3 Insert the SIM card with the cut edge and the contacts facing up.

**Figure 3: Install SIM Card**

- 4 Close the SIM card holder.

**Figure 4: Close SIM Card Holder**

- 5 Slide the SIM card holder toward the top of the TC55 to lock into place.

**Figure 5: Lock SIM Card Holder**

## Installing an Optional microSD Card

**Caution:**

For proper electrostatic discharge (ESD) precautions to avoid damaging the SD card. Proper ESD precautions include, but not limited to, working on an ESD mat and ensuring that the user is properly grounded.

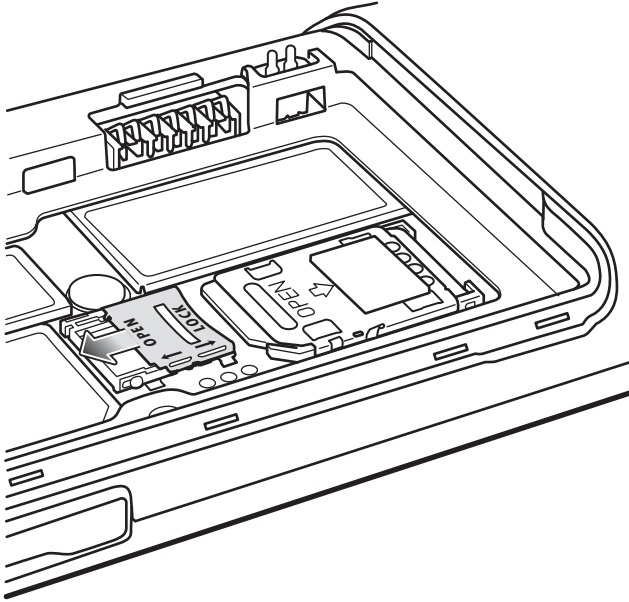
Changing the microSD card can change the functionality of the TC55.



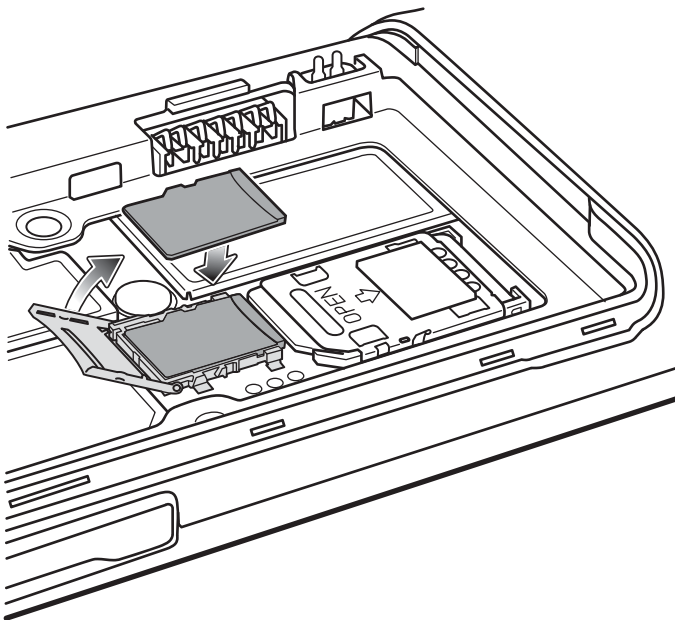
**Note:** The TC55 supports microSD cards up to 32 GB.

**Procedure:**

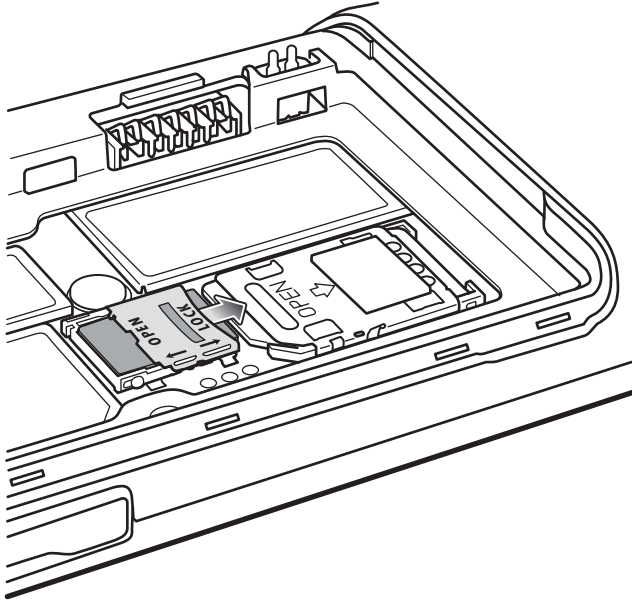
- 1 Slide the microSD card door toward the top of the TC55 to unlock.

**Figure 6: Unlock microSD Card Door**

- 2 Lift the SD card door.
- 3 Align the microSD card with the card holder. Ensure that the contacts on the card are facing down and toward the card holder.
- 4 Insert the microSD card into the card holder.

**Figure 7: Insert microSD Card**

- 5 Close the SD card door.
- 6 Slide the SD card door toward the bottom of the TC55 to lock into place.

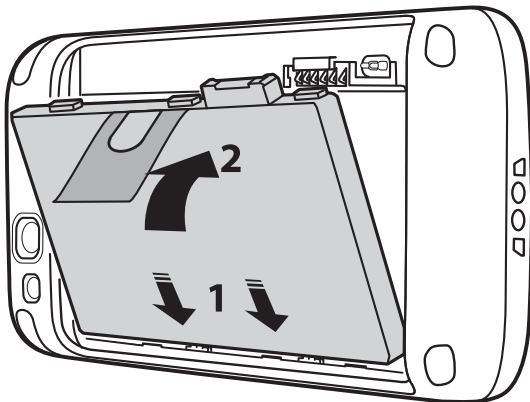
**Figure 8: Lock SD Card Door**

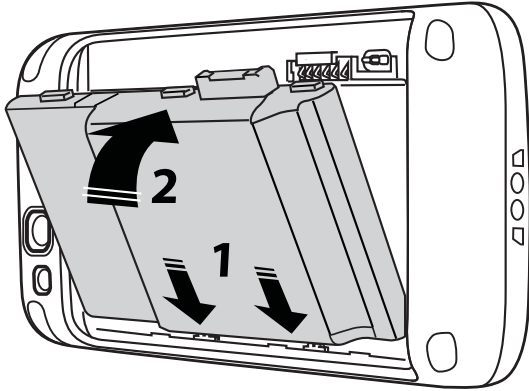
## Installing the Battery

There are two sizes of batteries available for the TC55; a 2,940 mAh battery and a 4,410 mAh battery.

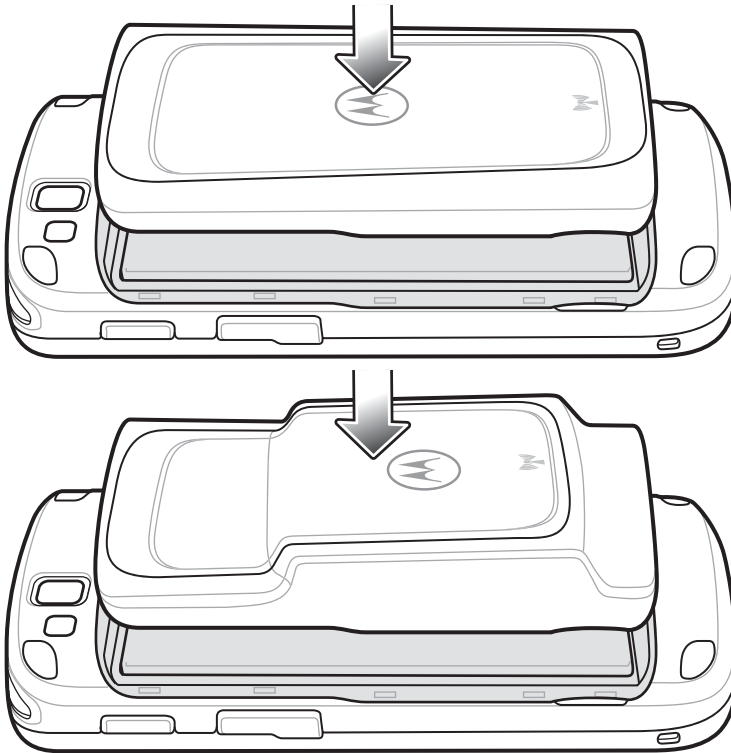
### Procedure:

- 1 Align the three tabs on the bottom of the battery with the three slots in the battery compartment.
- 2 Press the battery down and then rotate until it locks into place.

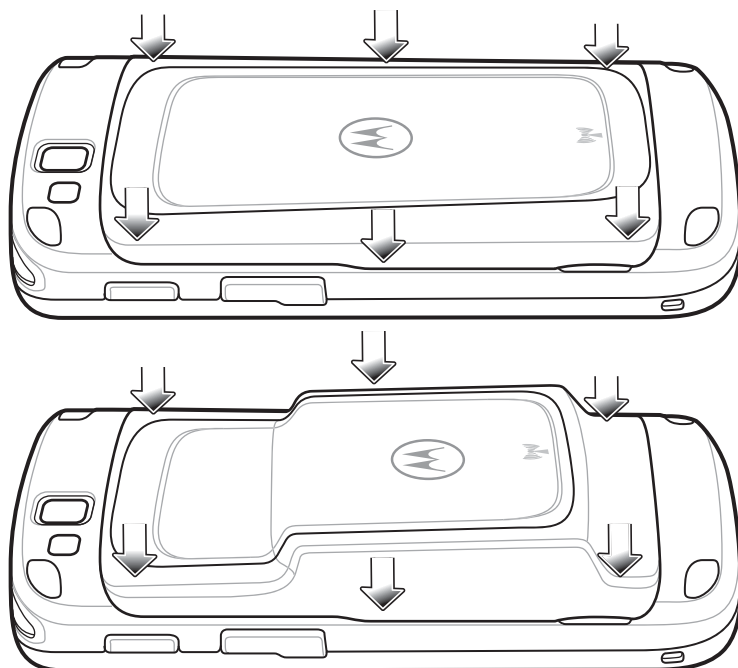
**Figure 9: Inserting the 2,940 mAh Battery**

**Figure 10: Inserting the 4,410 mAh Battery**

- 3 Align the battery door with the back of the device and press the battery door down until it snaps into place.

**Figure 11: Install the Battery Cover**

- 4 Press around the edge of the cover to ensure that the battery door is seated properly.

**Figure 12: Secure Cover**

## Charging the Battery



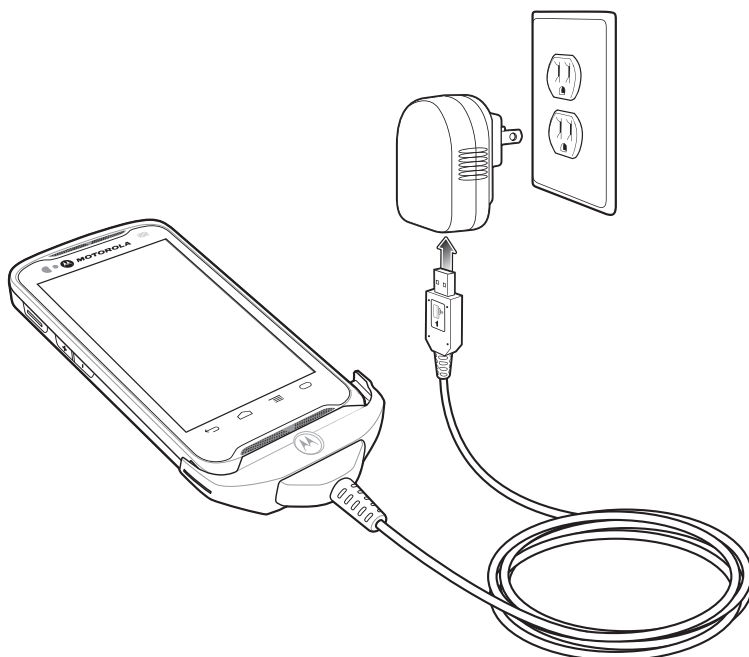
**Caution:** Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 121](#).

## Charging the Main Battery

Before using the TC55 for the first time, charge the main battery until the light emitting diode (LED) turns solid green (see [Charging LED Status on page 29](#) for charge status indications). To charge the TC55, use the Rugged Charge Cable with the optional power supply.



**Note:** Only connect the Rugged Charge Cable to the optional power supply. Do not connect the Rugged Charge Cable to a host computer for charging.

**Figure 13: Connect the Rugged Charge Cable**

The TC55 begins charging. The LED blinks green while charging, then turns solid green when fully charged. The 2,940 mAh battery charges in approximately three hours and the 4,410 mAh battery charges in approximately 4.5 hours.

## Charging LED Status

**Table 1: Charging LED Status**

Status	Indications
Off	TC55 is not inserted correctly in the cradle. TC55 is not connected to a power source. Cable or cradle is not powered.
Slow blinking green (1 blink every two seconds)	TC55 is charging.
Solid green	Charging complete.
Slow blinking red (1 blink every two seconds)	Battery is in an extremely low power state (normal slow charging mode).
Fast blinking red (2 blinks / per second)	Charging error: <ul style="list-style-type: none"> <li>• Temperature is too low or too high.</li> <li>• Charging has gone on too long without completion (typically eight hours).</li> </ul>

## Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Note that charging is intelligently controlled by the TC55. To accomplish this, for small periods of time, the TC55 or accessory alternately enables and disables

battery charging to keep the battery at acceptable temperatures. The TC55 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

## Powering On the TC55



**Note:** Ensure that the battery cover is properly installed. Otherwise, the TC55 will not power on.

If the TC55 did not turn on when the battery was installed, press the Power button. The LED flashes green and the device vibrates. The splash screen displays for about a minute as the TC55 boots.

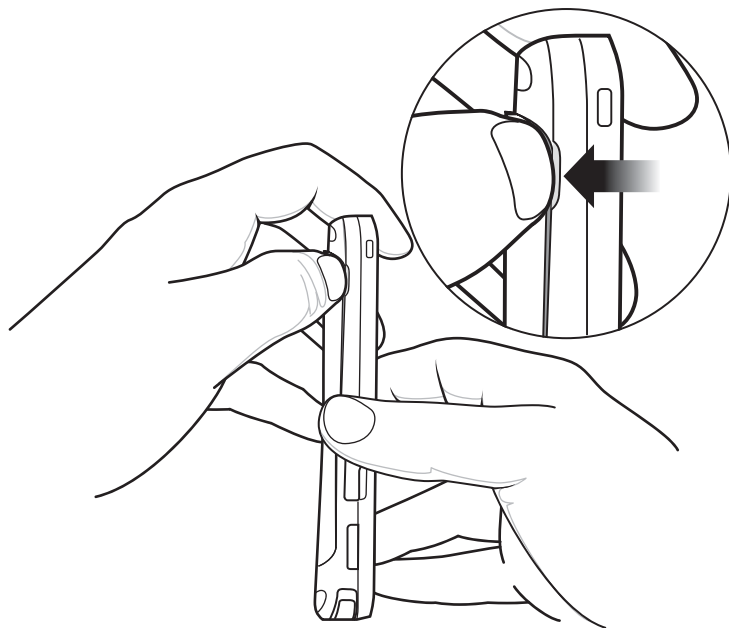
## Replacing the 2,940 mAh Battery

---

### Procedure:

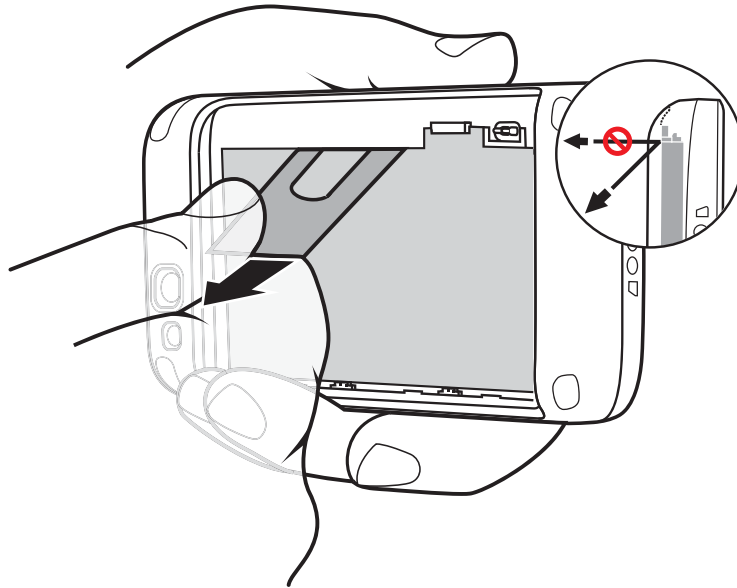
- 1 Press the Power button until the menu displays.
- 2 Touch **Power off**.
- 3 Touch **OK**.
- 4 Place thumbnail at notch and lift the battery cover.

**Figure 14: Remove the Battery Cover**

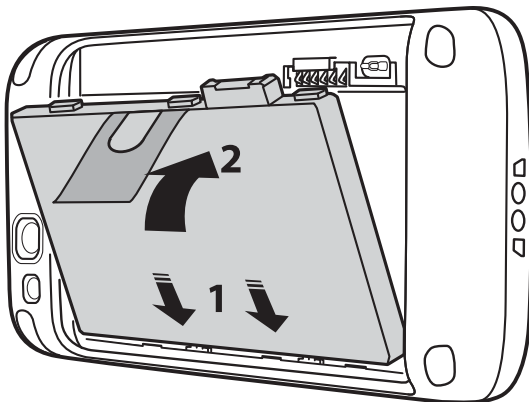


**Note:** Do not pull the battery tab straight out. Pull at a 45 degree angle.

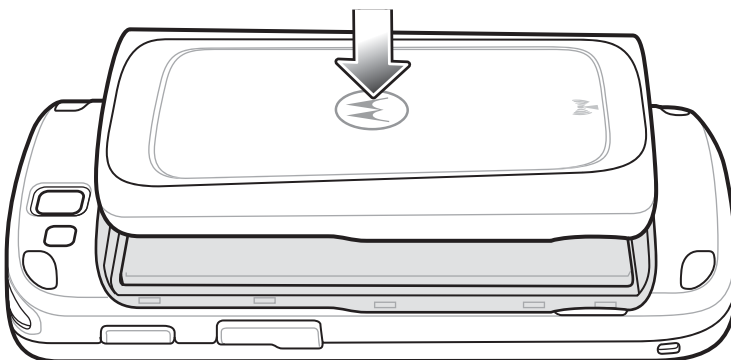
Pull the battery tab down at a 45 degree angle.

**Figure 15: Remove 2,940 mAh Battery**

- 6 Remove the battery from the battery compartment.
- 7 Align the three tabs on the bottom of the replacement battery with the three slots in the battery compartment.
- 8 Press the battery down and rotate until it locks into place.

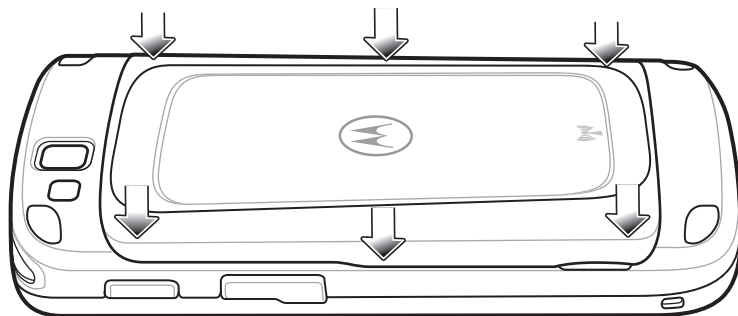
**Figure 16: Inserting the 2,940 mAh Battery**

- 9 Align the battery door with the back of the device.

**Figure 17: Align the Battery Cover**

- 10 Press around the edge of the cover to ensure that the battery door is seated properly.

**Figure 18: Secure the Battery Cover**



11 Press the Power button to turn on the TC55.

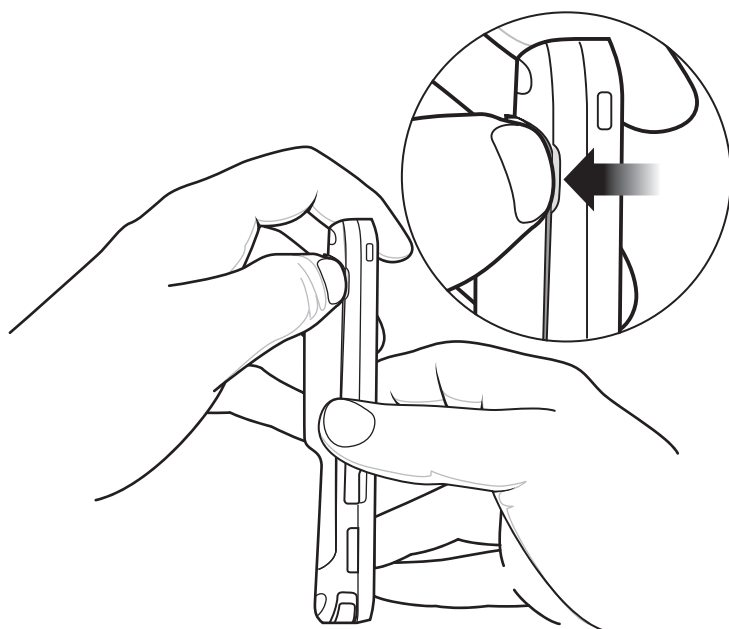
## Replacing the 4,410 mAh Battery

---

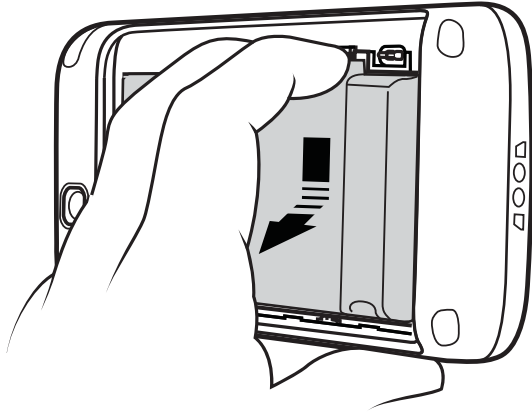
### Procedure:

- 1 Press the Power button until the menu displays.
- 2 Touch **Power off**.
- 3 Touch **OK**.
- 4 Place thumbnail at notch and lift the battery cover.

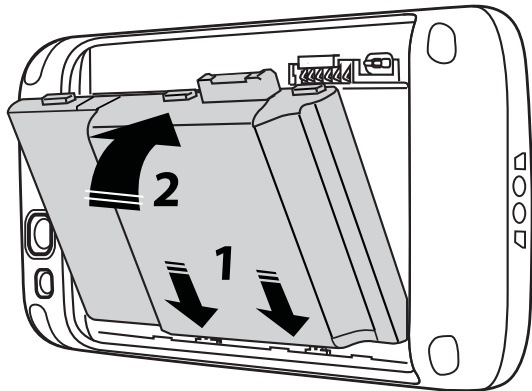
**Figure 19: Remove the Battery Door**



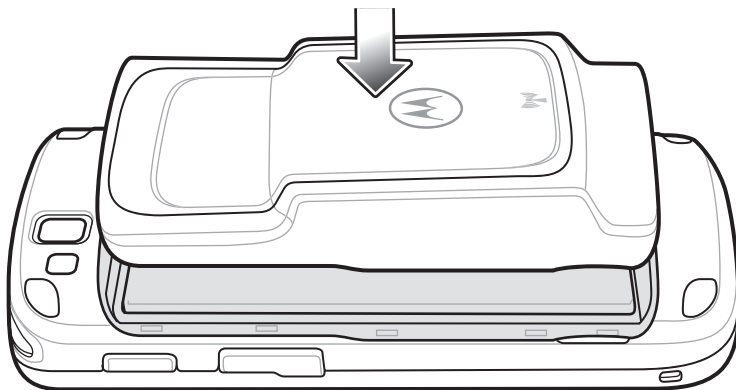
5 With two fingers, press the battery down.

**Figure 20: Remove 4,410 mAh Battery**

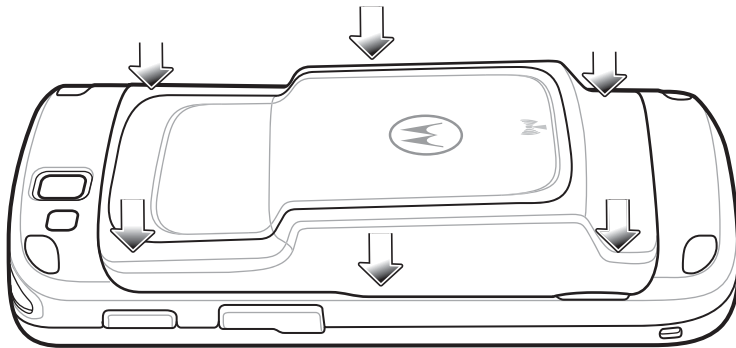
- 6 Rotate the battery out of the compartment.
- 7 Align the three tabs on the bottom of the replacement battery with the three slots in the battery compartment.
- 8 Press the battery down and rotate until it locks into place.

**Figure 21: Inserting the 4,410 mAh Battery**

- 9 Align the battery door with the back of the device.

**Figure 22: Align the Battery Cover**

- 10 Press around the edge of the cover to ensure that the battery door is seated properly.

**Figure 23: Secure the Battery Cover**

11 Press the Power button to turn on the TC55.

## Replacing the microSD Card

---



**Caution:**

For proper electrostatic discharge (ESD) precautions to avoid damaging the SD card. Proper ESD precautions include, but not limited to, working on an ESD mat and ensuring that the user is properly grounded.

Changing the microSD card can change the functionality of the TC55.

Ensure that you follow the procedures to shut down the TC55 before replacing the microSD card. Data corruption can occur if reading or writing to the microSD card and power is removed.

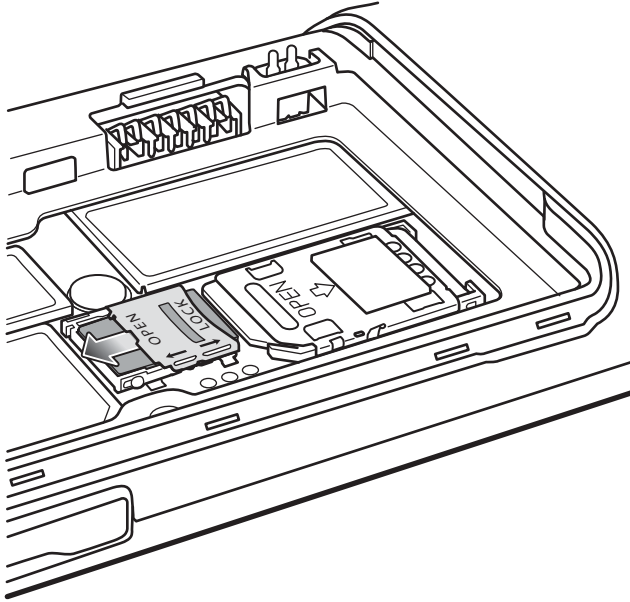


**Note:** The TC55 supports microSD cards up to 32 GB.

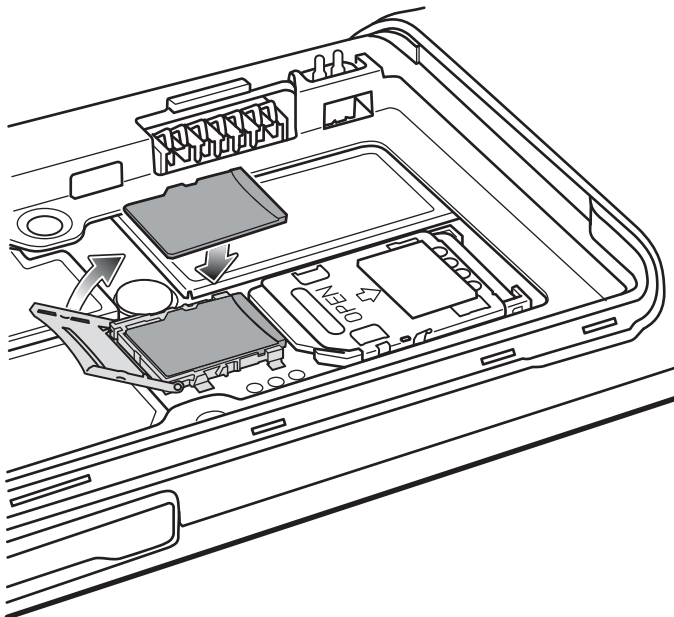
To replace the microSD card:

**Procedure:**

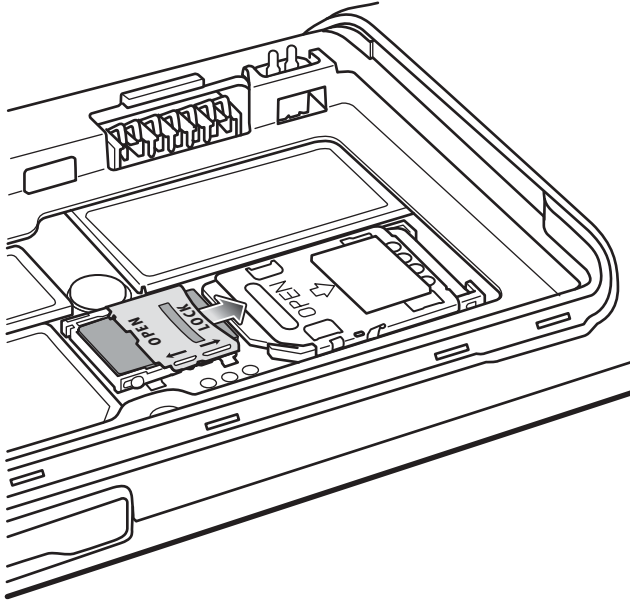
- 1 Press the Power button until the menu displays.
- 2 Touch **Power off**.
- 3 Touch **OK**.
- 4 Wait for the device to power off completely.
- 5 Remove the battery cover.
- 6 Remove the battery.
- 7 Slide the microSD card door up to unlock.

**Figure 24: Unlock microSD Card Door**

- 8 Lift the microSD card door.
- 9 Remove the microSD card from the card holder.
- 10 Align the replacement microSD card with the card holder. Ensure that the contacts on the card are facing down and toward the card holder.
- 11 Insert the microSD card into the card holder.

**Figure 25: Insert microSD Card**

- 12 Close the microSD card door.
- 13 Slide the microSD card door down to lock into place.

**Figure 26: Lock microSD Card Cover**

14 Replace the battery.

15 Align the battery door with the back of the device and press the battery door down until it snaps into place.

16 Press the Power button to turn on the device.

## Resetting the Device

---

There are four reset functions:

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

### Performing a Soft Reset

Perform a soft reset if applications stop responding.

**Procedure:**

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

### Performing a Hard Reset



**Caution:** Performing a hard reset with a SD card installed in the TC55 may cause damage or data corruption to the SD card.

Perform a hard reset if the TC55 stops responding.

**Procedure:**

- 1 Simultaneously press the Power, Programmable and Volume Up buttons.

**Figure 27: Three Button Reset**

- 2 The TC55 reboots.

## Performing an Enterprise Reset

An Enterprise Reset erases all data in the /cache and /data partitions and clears all TC55 settings, except those in the /enterprise partition.

### Procedure:

- 1 Download the Enterprise Reset file from Motorola Support Central web site.
- 2 Copy the TC55N×GenER0000002.zip file to the root directory of the microSD card. See [USB Communication on page 45](#).
- 3 Press and hold the Power button until the **Device options** menu appears.
- 4 Touch **Reset**.
- 5 Touch **OK**. The TC55 resets.
- 6 Press and hold the Volume Up button.
- 7 When the System Recovery screen appears release the Volume Up button.

**Figure 28: System Recovery Screen**

- 8 Use the Volume Up and Down buttons to navigate to **Apply update from SD card** or **apply from internal**.
- 9 Press the Scan button.

10 Use the Volume Up and Down keys to navigate to the TC55N×GenER0000002.zip file.

11 Press the Scan button. The Enterprise Reset occurs and then the TC55 resets.

## Performing a Factory Reset

A Factory Reset erases all data in the /cache, /data and /enterprise partitions in internal storage and clears all TC55 device settings. A Factory Reset returns the TC55 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 114](#) for more information.

### Procedure:

- 1 Download the Enterprise Reset file from Motorola Support Central web site.
- 2 Copy the TC55N×GenFR0000002.zip file to the root directory of the microSD card or to Internal Storage. See [USB Communication on page 45](#).
- 3 Press and hold the Power button until the menu appears.
- 4 Touch **Reset**.
- 5 Touch **OK**. The TC55 resets.
- 6 Press and hold the Volume Up button.
- 7 When the System Recovery screen appears release the Volume Up button.

**Figure 29: System Recovery Screen**



8 Use the Volume Up and Down buttons to navigate to **Apply update from SD card** or **apply from internal**.

9 Press the Scan button.

10 Use the Volume Up and Down keys to navigate to the TC55N×GenFR0000002.zip file.

11 Press the Scan button. The Factory Reset occurs and then the TC55 resets.

# Chapter 2

## Accessories

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

### TC55 Accessories

---

The table below lists the accessories available for the TC55.

**Table 2: TC55 Accessories**

Accessory	Part Number	Description
<b>Cradles</b>		
Five Slot Charge Only Cradle	CRDUNIV-55-5000R	Provides charging for up to five TC55 devices. Requires additional power supply.
Five Slot Charge Only Cradle Base	CRDUNIV-XX-5000R	Provides charging for up to five TC55 devices. Requires charging cups and additional power supply.
Vehicle Cradle	CRD-TC55-VCD1-01	Provides mounting of the TC55 in a vehicle.
<b>Chargers</b>		
Power Supply (12 VDC, 4.16 A.)	PWRS-14000-148R	Provides power to the Five Slot Charge Only Cradle.
Power Supply (5 VDC, 1.2 A)	PWRS-124306-01R	Provides power to the TC55.
<b>Cables</b>		
Rugged Charge Cable	CBL-TC55-CHG1-01	Provides power to the TC55.
Micro USB Cable	25-MCXUSB-01R	Provides USB communication with a host computer.
Auto Charge Cable	VCA400-01R	Charges the TC55 in a Vehicle Cradle using a vehicle's cigarette lighter.
US AC Line Cord (3-wire)	50-16000-221R	Provides power to the power supplies.
International AC line Cord	-	Provides power to the power supplies. Purchase separately.
<b>Miscellaneous</b>		
Spare 2940 mAh lithium-ion battery	BTRY-TC55-29MA1-01	Replacement 2940 mAh battery.

*Table continued...*

Accessory	Part Number	Description
Spare 4410 mAh lithium-ion battery	BTRY-TC55-44MA1-01	Replacement 4410 mAh battery.
2940 mAh Battery Door	KT-TC55-29BTYD1-01	Replacement battery door for 2940 mAh battery.
4410 mAh Battery Door	KT-TC55-44BTYD1-01	Replacement battery door for 4410 mAh battery.
Charging Cup	CUPTC55XX-1000R	Mounts onto the Multi Slot Charge Only Cradle Base and provides TC55 charging slot.
Blank Slot Cover	CUPUNICVR-5000R	Mounts on the Five Slot Charge Only Cradle and covers a slot when a cup is not required (5-pack).
Protective Boot (Blue/Black)	SG-TC55-BOOT1-01	Provides additional protection for the TC55.
Protective Boot (Grey/Black)	SG-TC55-BOOT2-01	Provides additional protection for the TC55.
Stylus for Protective Boot	KT-TC55-STYLUS1-01 KT-TC55-STYLUS1-03	Single stylus for Protective Boot with tether. Stylus for Protective Boot with tether (3-pack).
Holster	SG-TC55-HLSTR1-01	Mounts on belt and provides storage for the TC55.

## Five Slot Charge Only Cradle

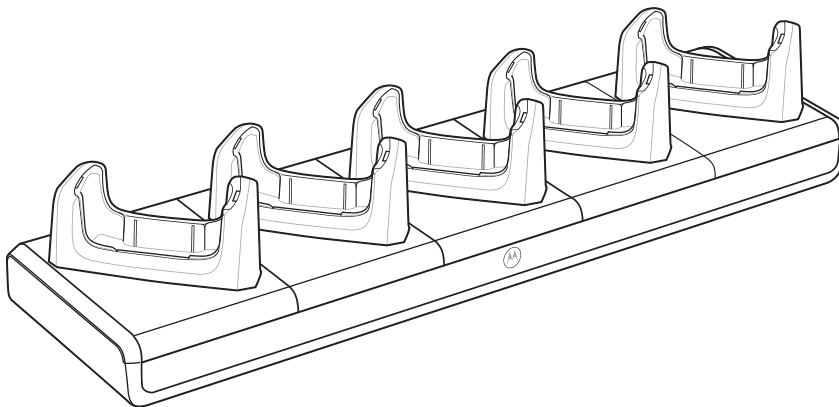
The Five Slot Charge Only cradle:

- Provides 5 VDC power for operating the TC55.
- Simultaneously charges up to five TC55s.
- Contains five removal cups.

### Charging the TC55

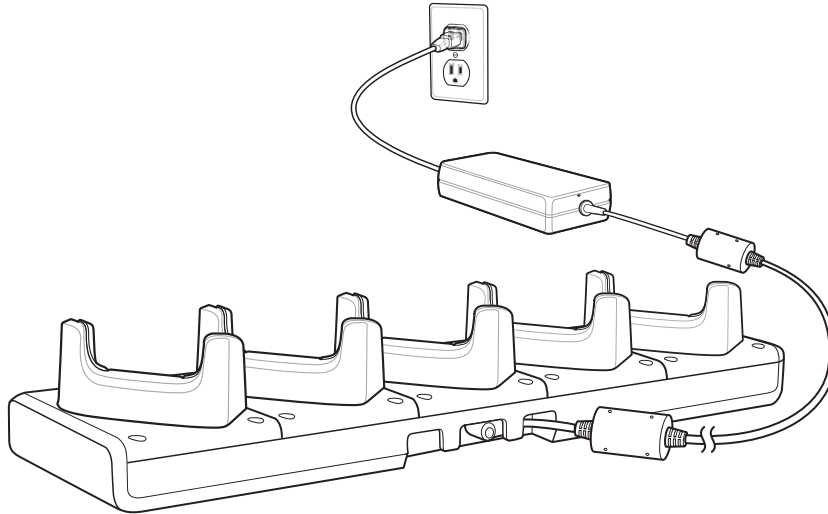
To charge the TC55, insert the TC55 into an open slot.

**Figure 30: Five Slot Charge Only Cradle**



## Power Setup

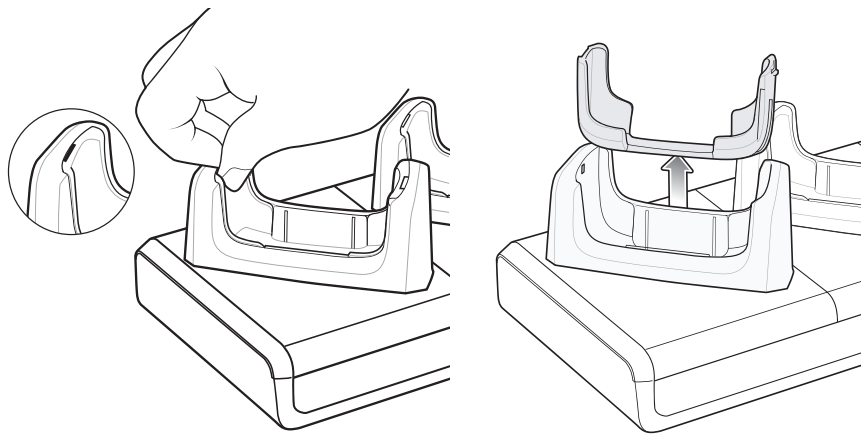
**Figure 31: Five Slot Charge Only Cradle Power Connections**



## Inserting a TC55 with Boot into Cradle

Each cradle cup has an insert that must be removed prior to inserting the TC55 with Protective Boot. Remove the insert and then insert the TC55 into the cup.

**Figure 32: Remove Cup Insert**



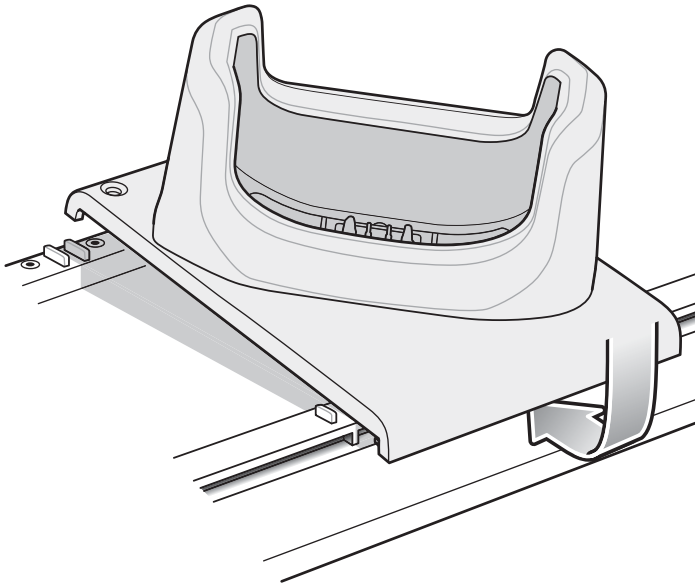
## Installing a Cup

Cups on the Five Slot Charge Only Cradle can be removed and replaced with new cups or blank cups. To install the cradle cups:

### Procedure:

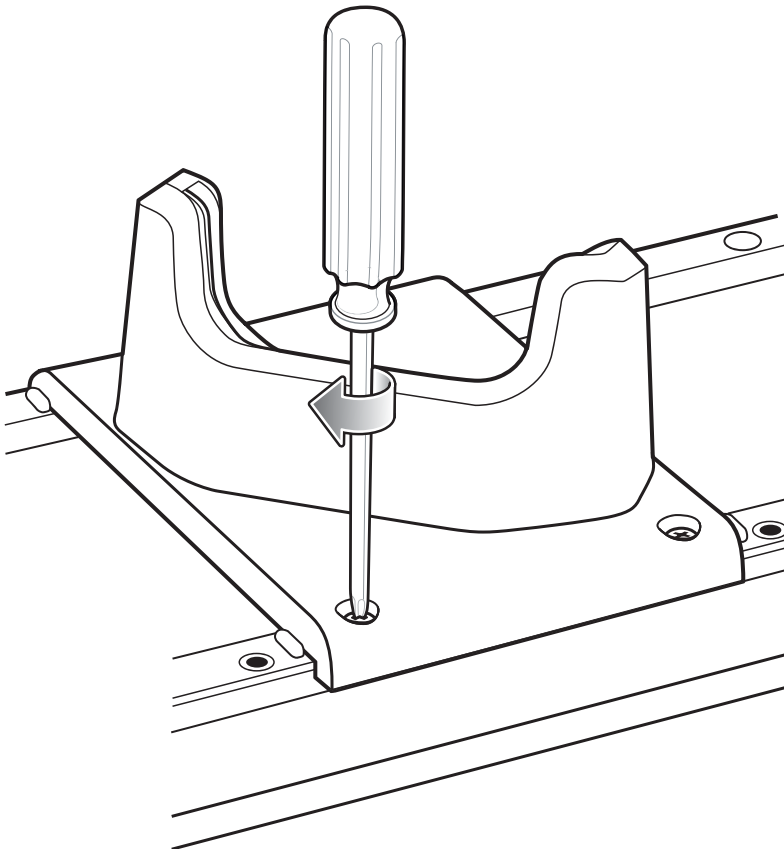
- 1 Remove power from the cradle base before installing cups.
- 2 Using a Phillips screwdriver, remove the two screws securing the cup to the base.
- 3 Lift the front of the cup and then slide off the back of the base.
- 4 Align the lip of the cup with the slot on the front of the cradle. Ensure that the cup is positioned within the Slot Alignment Tabs.

**Figure 33: Five Slot Charge Only Cradle Cup Installation**



- 5 Slide the lip into the slot and rotate the cup until it is flat on the cradle base.
- 6 Using a Phillips screwdriver, secure the cup to the charger base using the two screws provided with the cup.

**Figure 34: Securing Cup to Base**



- 7 Each slot on the Cradle Base must have a cup installed.
- 8 Repeat for each additional cup.



# 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 TC55 to a host computer using the micro USB cable to transfer files between the TC55 and the host computer.



**Caution:**

When connecting the TC55 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

### Connecting to the TC55 as a Media Device

**Procedure:**

- 1 Connect the micro USB cable to the TC55 and then to the host computer.

**Step result:** **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 TC55 as a portable device.  
If an external microSD card is installed, it displays as **SD card**. The internal memory appears as **Internal Storage**.
- 5 Open either **SD card** or **Internal Storage**.
- 6 Copy or delete files as required.

### Connecting to the TC55 as an Installer

**Procedure:**

- 1 Connect the micro USB cable to the TC55 and then to the host computer.

**Step result:** **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 On the host computer, open a file explorer application.  
The TC55 storage appears as Removable Disks.
- 4 On the TC55, pull down the Notification shade and touch **USB Connected**.
- 5 On the **USB mass storage** screen, touch **Turn on USB storage**.

On the host computer, the TC55 Internal Storage appears as **INTERNAL** and the microSD card appears as **Removable Disk**.

- 6 Locate the TC55 as a devices within Removable Storage.
- 7 Open either **INTERNAL** or **Removable Disk**.
- 8 Copy or delete files as required.
- 9 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 microSD card.
- 2 Remove the micro USB cable from the TC55.

# Chapter 4

## DataWedge Configuration

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

### Basic Scanning

---

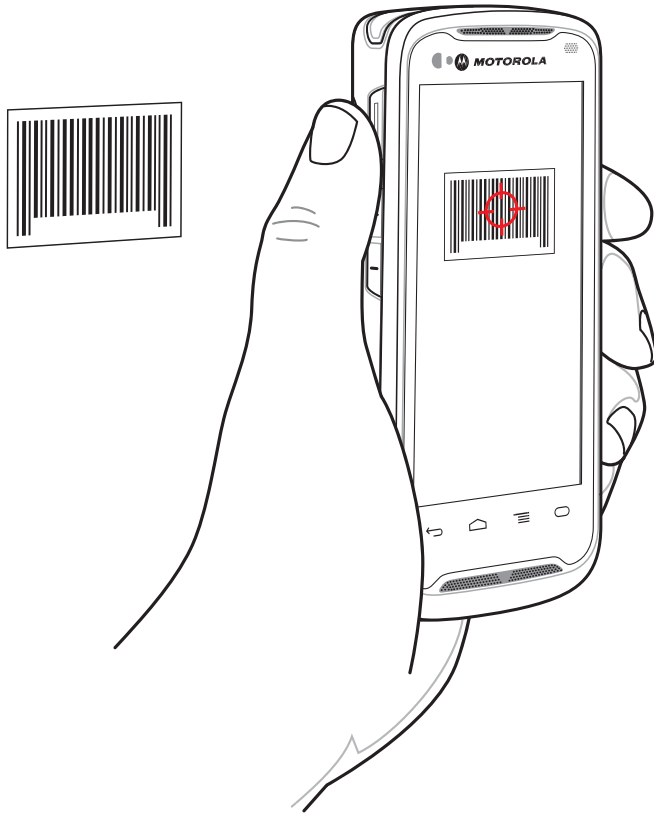
Scanning can be performed using either the linear imager or the rear-facing camera.

### Using the Camera

To capture bar code data:

**Procedure:**

- 1 Ensure that an application is open on the TC55 and a text field is in focus (text cursor in text field).
- 2 Aim the rear-facing camera at a bar code.
- 3 Press and hold the Programmable button. By default, a preview window appears on the screen. The LED light red to indicate that data capture is in process.

**Figure 35: Data Capture with Camera**

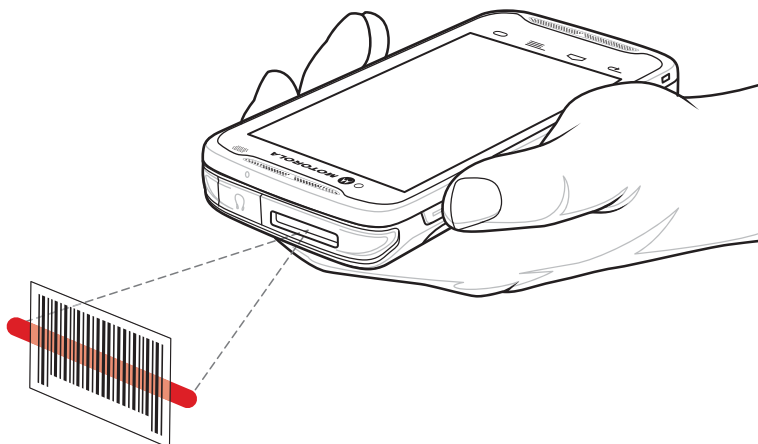
- 4 Move the TC55 until the bar code is centered under the red target.
- 5 The LED light green, a beep sounds and the TC55 vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

## Using the Imager

To capture bar code data:

### Procedure:

- 1 Ensure that an application is open on the TC55 and a text field is in focus (text cursor in text field).
- 2 Point the top of the TC55 at a bar code.

**Figure 36: Data Capture**

- 3 Press and hold the Programmable button. The LED lights red to indicate that data capture is in process.
- 4 Place the red aiming pattern across the bar code. The LED lights green and a beep sounds, by default, to indicate the bar code was decoded successfully.
- 5 The captured data appears in the text field.

## Profiles

---

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

Profile information consists of:

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

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

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

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

### Profile0

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

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

## Plug-ins

---

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

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

## Input Plug-ins

An Input Plug-in supports an input device, such as a bar code scanner contained in, or attached to the device.

**DataWedge** contains base plug-ins for these input devices.

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

## Process Plug-ins

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

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

## Output Plug-ins

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

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

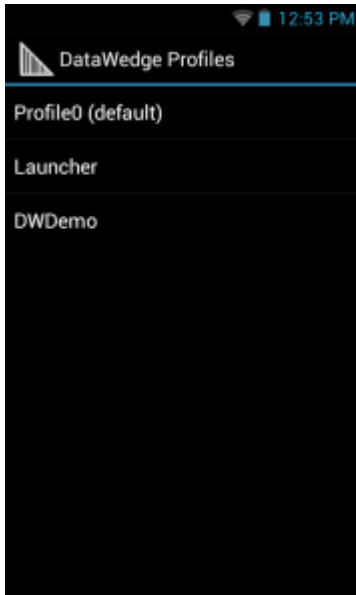
## Profiles Screen

---

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

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

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

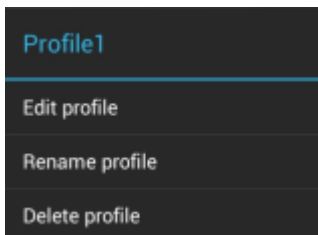
**Figure 37: DataWedge Profiles Screen**

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

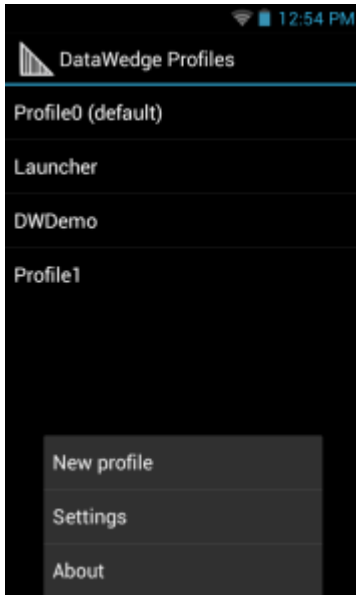
Touch and hold a profile to open a context menu that allows additional actions to be performed on the selected profile.

**Figure 38: Profile Context Menu**

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

### Options Menu




Touch  to open the options menu.

**Figure 39: 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**.

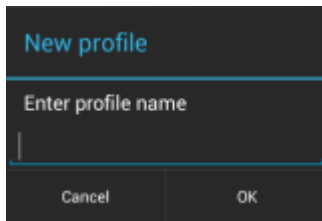
**Step result:** The blue check disappears from the checkbox indicating that DataWedge is disabled.

## 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 40: New Profile Name Dialog Box**

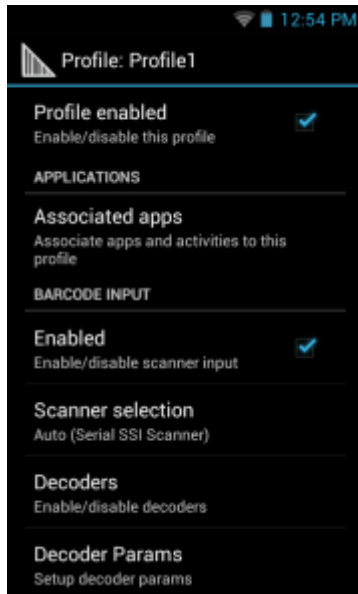
6 Touch **OK**.

**Step result:** 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 41: Profile Configuration Screen**

The configuration screen lists the following sections:

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

## Bar Code Input

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

### Enabled

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

## Scanner Selection

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


- **Auto** - The software automatically determines the best scanning device. If the linear imager is installed, then the **Serial SSI Scanner** is selected. Otherwise the **Camera Scanner** is selected.
- **Camera scanner** - Scanning is performed with the rear-facing camera.
- **Serial SSI Scanner** - Scanning is performed using the Linear 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 58](#) for more information.
    - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
    - **Length2** - Use to set decode lengths 4 (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 10). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length 2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 14). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 58](#) 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 58](#) for more information.
  - **Length2** - Use to set decode lengths (default - 0). See [Decode Lengths on page 58](#) 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.

- **Supplementals Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
- **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN 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).
- **Power Mode** - Set the linear imager power mode:
  - **Low Power Mode** - Imager power is enabled only when scanning.
  - **Optimized Power Mode** - Imager power remains enabled after scanning and turns off after a timeout value. (default)
  - **High Power Mode** - Imager power is enabled when scanning is enabled.
  - **Always On** - Imager power is enabled when the scanner object is opened.
- **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).
- **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).

## Keystroke Output

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

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

- **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 64](#) 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
  - 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 64](#) for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

- **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

## Intent Overview

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

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

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

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

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

and the Intent category would be:

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

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

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

- String LABEL\_TYPE\_TAG = "com.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.

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.

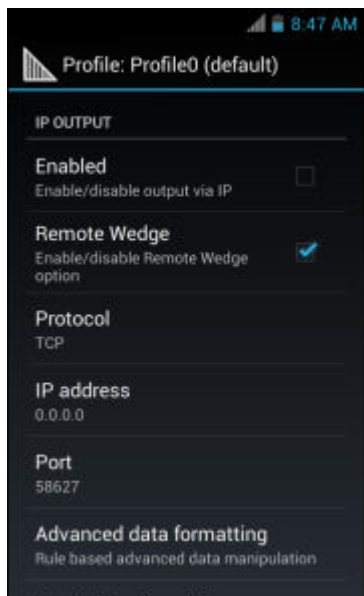
## IP Output

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 64](#) 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 42: IP Output Screen**

## 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:



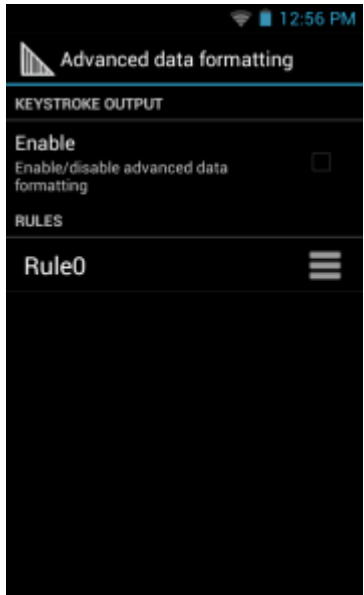
- 1 Touch .
- 2 Touch .
- 3 Touch a DataWedge profile.
- 4 In **Keystroke Output**, touch **Advanced data formatting**.

Figure 43: Advanced Data Formatting Screen



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

## Creating a Rule



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

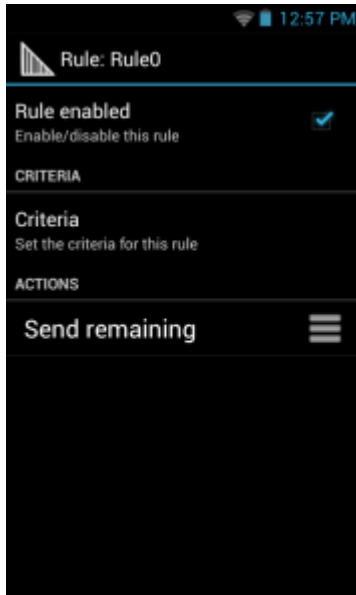
### Procedure:

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

## Defining a Rule

### Procedure:

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

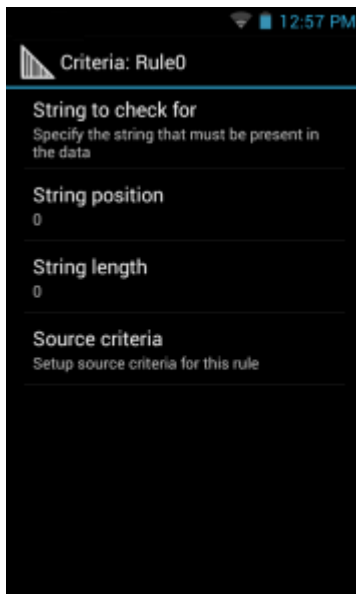
**Figure 44: Rule List Screen**

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

## Defining Criteria

### Procedure:

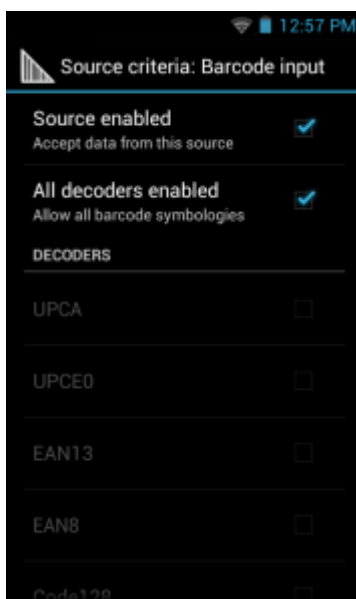
- 1 Touch **Criteria**.



**Figure 45: Criteria Screen**

- 2 Touch **String to check for** option to specify the string that must be present in the data.
- 3 In the **Enter the string to check for** dialog box, enter the string
- 4 Touch **Done**.
- 5 Touch **OK**.

- 6 Touch **String position** option to specify the position of the string specified in the **String to check for** option. The ADF rule is only applied if the specific string in **String to check for** is found at the specified **String position** location (zero for the start of the string).
- 7 Touch the + or - to change the value.
- 8 Touch **OK**.
- 9 Touch **String length option** to specify a length for the received data. The ADF rule only applies to the bar code data with that specified length.
- 10 Touch the + or - to change the value.
- 11 Touch **OK**.
- 12 Touch **Source criteria** option to associate an input device to an ADF rule. The ADF rule only applies to data received from associated input devices.
- 13 Touch **Barcode input**.
- 14 Touch the **Source enabled** checkbox to accept data from this source.

**Figure 46: Barcode Input Screen**




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



## 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 3: ADF Supported Actions on page 68](#) 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 3: 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 <b>Crunch spaces</b> action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last <b>Remove all spaces</b> action.
	Remove leading zeros	Remove all zeros at the beginning of data.
	Stop zero removal	Stop removing zeros at the beginning of data. This disables the previous <b>Remove leading zeros</b> action.
	Pad with zeros	Left pad data with zeros to meet the specified length. Enter the number zeros to pad.
	Stop pad zeros	Stop padding with zeros. This disables the previous <b>Pad with zeros</b> action.

*Table continued...*

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

## Deleting an Action

### 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:

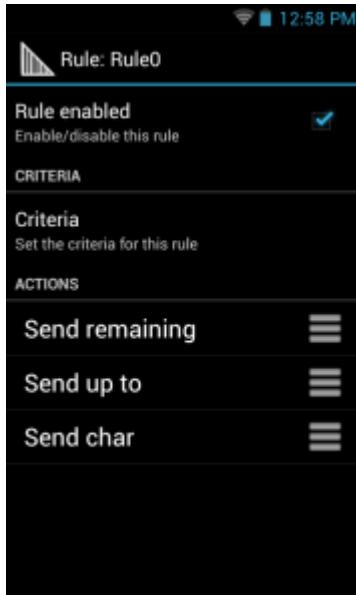
- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

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 .

**Figure 47: ADF Sample Screen**

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


**Figure 48: Sample Bar Code**

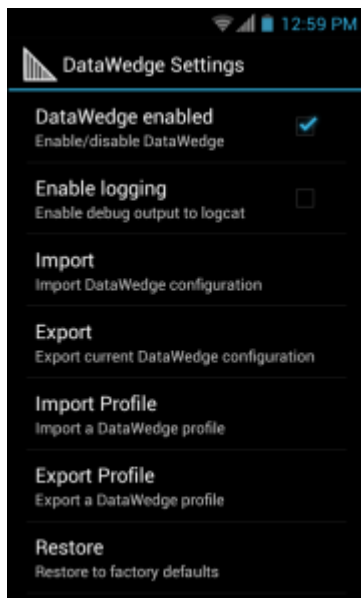
- 48 Press and hold the scan button.  
The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern. The LED light red to indicate that data capture is in process.
- 49 The LED light green, a beep sounds and the device vibrates, by 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 49: Formatted Data**

## DataWedge Settings

---

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




**Figure 50: DataWedge Settings Window**

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

- **Restore** - return the current configuration back to factory defaults.




## Importing a Configuration File

### Procedure:

- 1 Copy the configuration file to the root of the microSD card.
- 2 Touch .
- 3 Touch .
- 4 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 be copied to the microSD card of other devices and imported into DataWedge on those devices. Importing a configuration or profile replaces the existing settings.

### 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 TC55 and Mass Deploy

To disable DataWedge and deploy onto multiple TC55 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 73](#) for instructions. See [Configuration and Profile File Management on page 74](#) for instructions for using the auto import feature.



# 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 111](#) 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 88](#) for more information.

## Enterprise Administrator Application

---

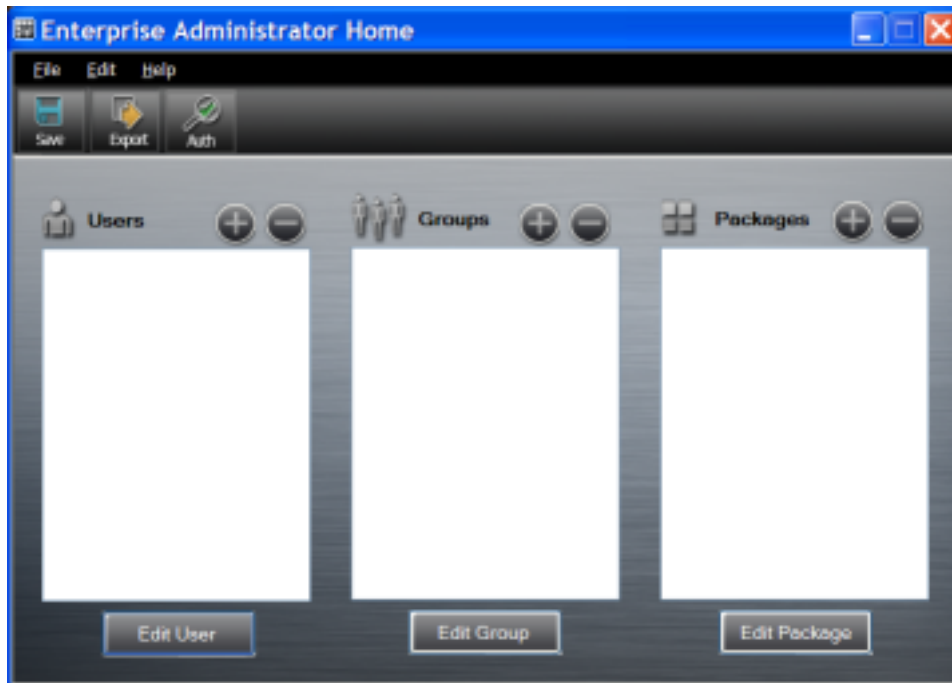


**Note:** .Net Compact Framework 4 or later is required to run the Enterprise Administrator. To download, go to [www.microsoft.com](http://www.microsoft.com).

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 51: 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 52: User Manager Window**

The screenshot shows a window titled "User Manager" with a sub-header "User Information". Below the header, there is a note: "Fields marked with a \* are required". The form contains three text input fields: "Username:" (with an asterisk), "Password:", and "Retype Password:". At the bottom, there are two checkboxes: "Admin:" (unchecked) and "Enabled:" (checked). Below the checkboxes are "OK" and "Cancel" buttons.

- 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 89](#).

**Figure 53: Package Information Window**

The screenshot shows a window titled "Manage Application" with a sub-header "Package Information". Below the header, there is a text input field labeled "Package name:". At the bottom, there are "OK" and "Cancel" buttons.

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

- Repeat steps 1 through 3 for each additional package.

## Creating Groups

Create groups of users that have access to specific applications.

### Procedure:

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

**Figure 54: Group Manager Window**



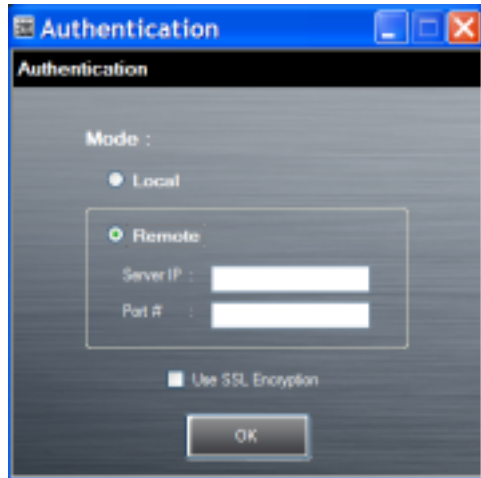
- In the **Group name** text box, enter a name for the group. This field is required.
- Select a user in the **Available Users** list box and then click the **Add** button to add the user to the **Users in Group** list box or click the **Add All** button to add all the users in the **Available Users** list box to the **Users in Group** list box.
- 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.
- Click **OK**.
- Click **Save**.

## Creating Remote Authentication

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

### Procedure:

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

**Figure 55: 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**.

**Step result:** 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 45](#) 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**.

**Step result:** 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**.

**Step result:** 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 89* 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**.

**Step result:** 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.

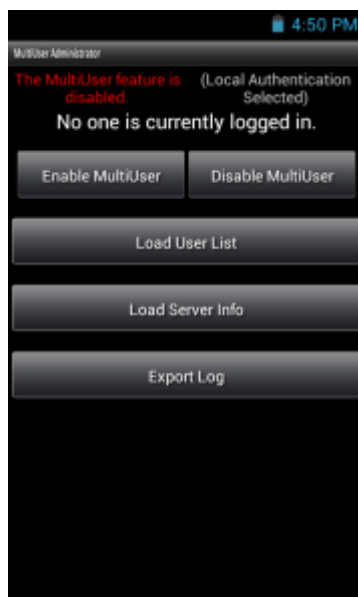
## Importing a Password

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

### Procedure:

- 1 Touch .
- 2 Touch .

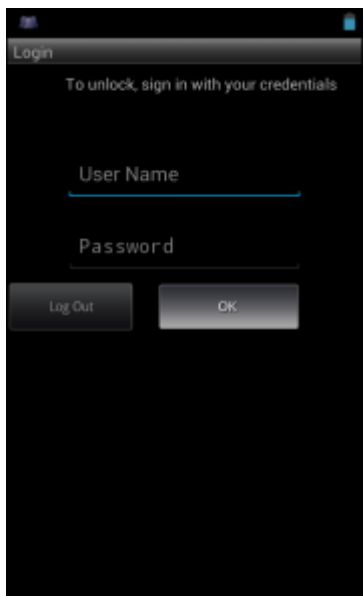
**Figure 56: MultiUser Administrator Screen**



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

- 4 Touch **Enable Multiuser** to enable the feature.

**Figure 57: MultiUser Login Screen**



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

## Disabling the Multi-user Feature



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

### Procedure:

- 1 Touch .
- 2 Touch .
- 3 Touch **Disable MultiUser**.




**Step result:** 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**.

**Step result:** 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**.

**Step result:** 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.

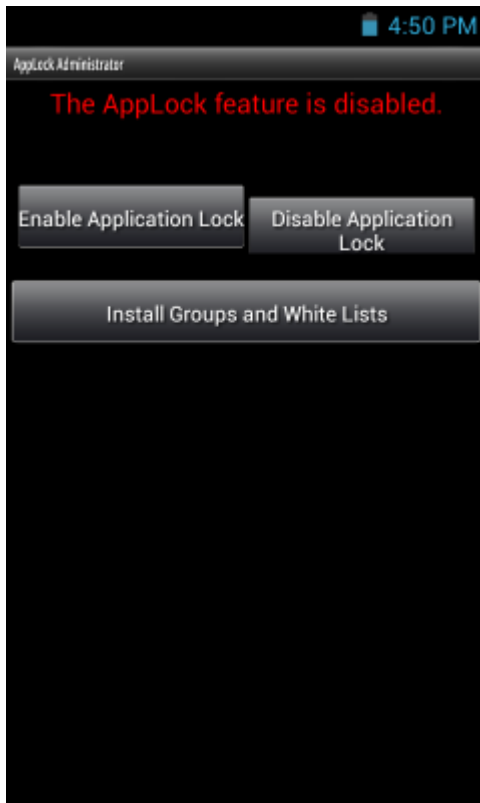


**Note:** To use the AppLock Administrator application, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

## Installing Groups and White Lists

### Procedure:

- 1 Touch .
- 2 Touch .

**Figure 58: AppLock Administrator Screen****Note:**

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

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

- 3 Touch **Install Groups and White Lists** to read the contents of the Groups and White List files from the root of the microSD card and push its contents into the AppLock framework.

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

## 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 83](#) 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 is 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 110](#) 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:

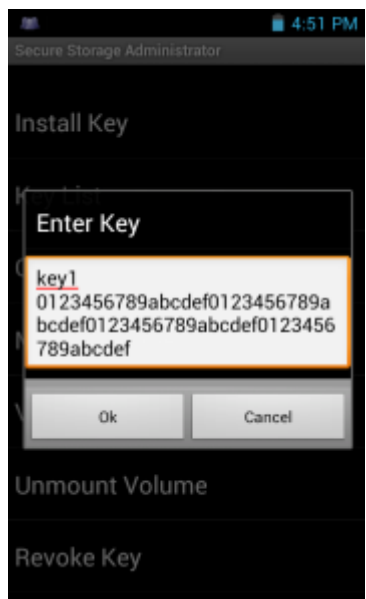
- installation and deletion of encrypted keys
- creation, mounting, un-mounting and deletion of the encrypted file systems.

## Installing a Key

### Procedure:

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

**Figure 59: Enter Key Dialog Box**



- 6 In the **Enter key** text box, enter the key name followed by the key value obtained in step 1, using the following format:  
 <Key Name> <Key value in Hex String>  
 Example: key2 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef  
 The key value must be a 64 hexadecimal character string.
- 7 Touch **OK**. The key is imported into the device. The message **successfully installed the key** appears on the screen.

## Viewing Key List

### Procedure:

- 1 Touch **Key List**.

**Figure 60: List of Keys**

- 2 Touch **OK**.

## Deleting a Key

### Procedure:

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



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

## Volumes

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

### Creating Volume Using EFS File

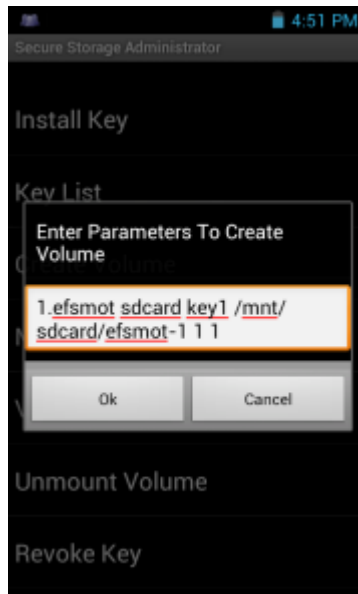
**Procedure:**

- 1 Create an efs file. See *Creating an EFS File on page 93* 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 45*.
- 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 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.

**Figure 61: Enter Parameter To Create Volume Dialog Box**

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

## Mounting a Volume

### Procedure:

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

## Listing Volumes

### Procedure:

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

## Unmounting a Volume

### Procedure:

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

## Deleting a Volume

### Procedure:

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

## Encrypting an SD Card



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

### Procedure:

- 1 Touch **Encrypt SD card**. A warning message appears.
- 2 Touch **Yes**. The Key List dialog box appears.
- 3 Select a key from the list and then touch **Ok**.  
The encryption process begins and when completed, displays a successfully completed message.

## Creating an EFS File

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

### Procedure:

- 1 On a host computer, create a text file.
- 2 In the text file enter the following:  
<Volume Name> <Volume Storage Type> <Key Name> <Mount Path> <Auto Mount> <Volume size>  
where:  
<Volume Name> = name of the volume  
<Volume Storage Type> = storage location. Options: internal or sdcard.  
<Key Name> = name of the key to use when creating the volume.  
<Mount Path> = path where the volume will be located.  
<Auto Mount> = Options: 1 = yes, 0 = no.  
<Volume size> = size of the volume in Megabytes.  
Example:  
MyVolume sdcard key1 /mnt/sdcard/efsfolder 1 1
- 3 Save the text file as `efsfile`.

## Off-line Extraction Tool

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

Connect the device to the host computer.

## Usage

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

The following Main Menu appears:

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

## Creating an Image

### Procedure:

- 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
```
- 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**.
- 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**.
- 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.
- 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
```
- 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.
- If the volume is mounted on the desktop, then that volume can be provisioned with files for deployment.
- 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:

- 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
```
- Enter the name of the volume and then press **Enter**.
- 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

## MLog Manager

The **MLog Manager** allows the user to export operating system and modem logs. Analyzing the exported logs can provide visibility into the system internal behavior and may help determining root causes of the system faults and issues.

### Sub-systems

- **MLog Manager**
  - Built-in user interface (UI) application for users.
  - Exports logs using UI button requests.
  - Supports B2M **Elemex** client requests.
  - Sets MLog parameters (e.g. Persisting-Logs and Export-Logs-Upon-Boot).
- **MLog Services**
  - Built-in daemon service.
  - Synchronizes access to the MLog service functions.
  - Reads incoming logs messages from the Android (kernel/firmware) drivers and the modem sub-system.
  - Writes the Android logs circularly into a secured 'logs' partition (only when the 'Persisting Logs' mode is active).
  - Exports logs data automatically to a microSD card (only when **Export Logs upon Boot** mode is active).

### Log Descriptions



The MLog system provides the ability to export Android and modem logs using the **MLog Manager**

- **Android**
  - **Framework/Kernel Logs** - captures standard Android system messages, including errors, warnings and informational messages that have been written from Android applications, services and drivers.
  - **TombStones/ANRs Logs** - captures important information of native crashed process, which include terminated signal and fault address, CPU registers, and the crashed process call-stack.
  - **AbnormalResets/Recovery/FWL Logs**
    - + captures all the abnormal resets that occur on the TC55, e.g. reset that occur to the TC55 as result of battery replacement.
    - + captures all the upgrades and downgrades that are done to the TC55 via the recovery mechanism.
    - + captures the Flash health values any time it changes.
  - **AppNoRespond Logs** - captures Java level stack traces of an Android crashed application.
  - **Export All Logs** - captures all of the above logs at once.
- **QXDM**
  - captures baseband system messages, which include errors, warnings and informational messages. Choose the filter by what you did on the WAN function. The filter are voice call (CS), data call (PS), GPS (GNSS), network (NW), SIM card, SMS and STK issue. If you cannot recognize where the issue is, use 234G filter to capture the log before your testing.

## Exporting QXDM Logs

---

### Procedure:

- 1 Touch .
- 2 Touch .
- 3 On the QXDM tab, touch **Start Qxdm Logging**.
- 4 On the **Choose log filter** dialog box, select one of the options:
  - 234G
  - CS (Voice call)
  - GNSS (GPS)
  - NW (network)
  - PS (Data call)
  - SIM (SIM card)
  - SMS
  - STK
  - User Defined
- 5 Select a filter.

**Step result:** The TC55 starts collecting the select data.



# Chapter 7

## Settings

This chapter describes settings available for configuring the device.

### Location Settings

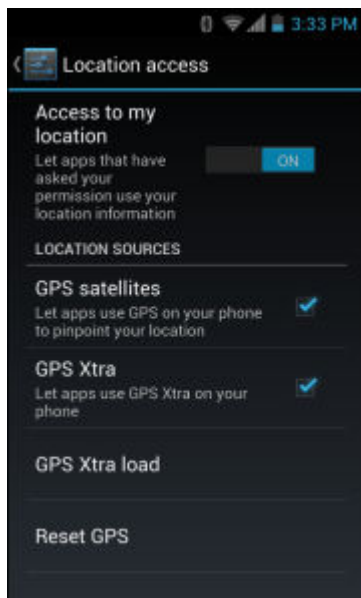
---

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



**Location access.**

**Figure 62: Location Access Screen**



- **Access to my location** - Set to **ON** to ensure that applications request access to your location information.
- **Location Sources**
  - **GPS satellites** - Check to allow application to use the TC55 to pinpoint your location.
  - **GPS Xtra** - Check to allow applications to use GPS Xtra on the TC55.





**Note:** The TC55 can access GPS information from an eXTended Receiver Assistance (Xtra) server using an Internet connection. This technology provides enhanced operation for Stand-alone GPS operation.

- **GPS Xtra load** - Select to load GPS Xtra data to the TC55.
- **Reset GPS** - Touch to reset the GPS data to factory default settings.

## 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 102](#) for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See [Set Screen Unlock Using PIN on page 100](#) for more information.
  - **Password** - Enter a password to unlock screen. See [Set Screen Unlock Using Password on page 101](#) 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:





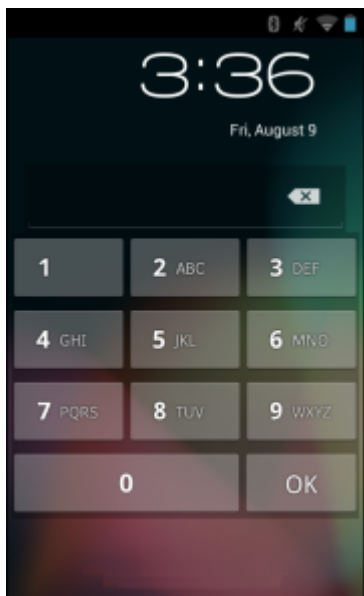
- 1 Touch .
- 2 Touch .
- 3 Touch  **Security**.
- 4 Touch **Screen lock**.
- 5 Touch **PIN**.
- 6 Touch in the text field.
- 7 Enter a PIN (between 4 and 16 characters) then touch **Next**.
- 8 Re-enter PIN and then touch **Next**.
- 9 On the **Security** screen, touch **Vibrate on touch** to enable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

Figure 63: PIN Screen



## Set Screen Unlock Using Password

### Procedure:





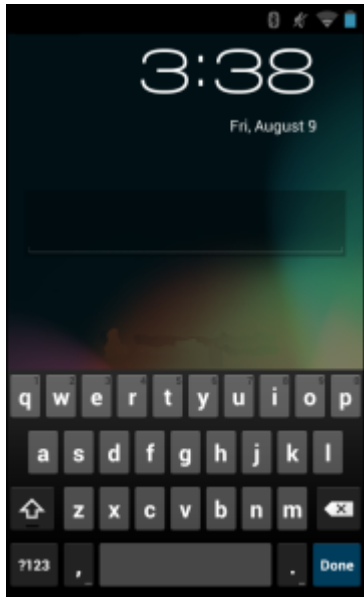



- 1 Touch .
- 2 Touch .
- 3 Touch  **Security**.
- 4 Touch **Screen lock**.
- 5 Touch **Password**.
- 6 Touch in the text field.
- 7 Enter a password (between 4 and 16 characters) then touch **Next**.
- 8 Re-enter the password and then touch **Next**.
- 9 Touch . The next time the device goes into suspend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

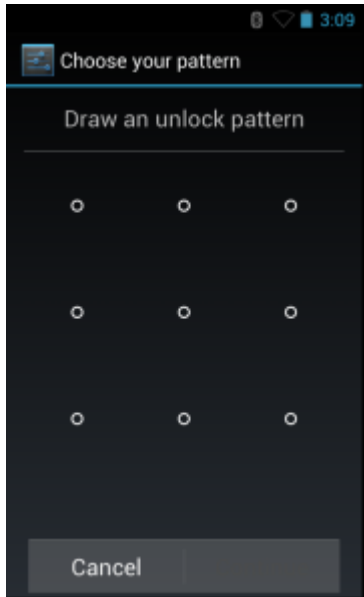
Figure 64: Password Screen




## Set Screen Unlock Using Pattern

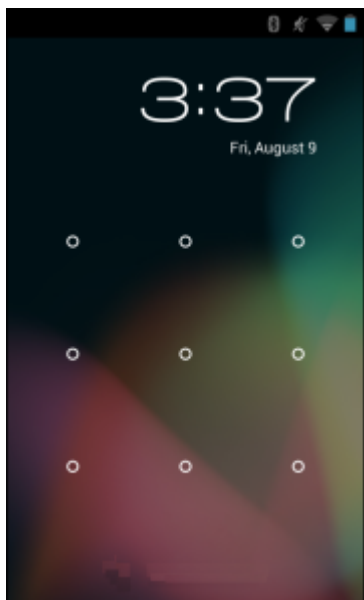
### Procedure:

- 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 65: Choose Your Pattern Screen**

- 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 66: Pattern Screen**

## Multiple User Mode

For Multi-user Mode configuration, see [Administrator Utilities on page 77](#).

## 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 Programming

---

Two of the TC55's buttons can be programmed to perform different functions or shortcuts to installed applications.

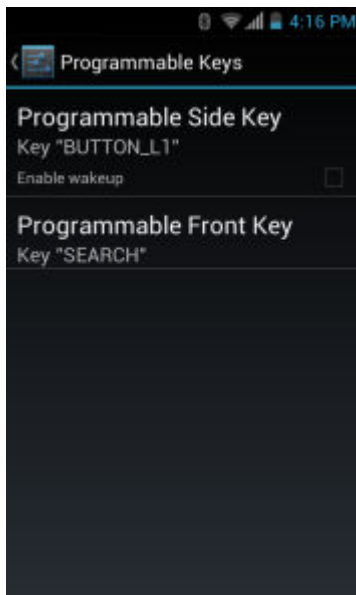
- Programmable button - Side Programmable button set to scanning by default.
- Search button - Oval button  below display.


## Programming a Button

### Procedure:

- 1 Touch .
- 2 Touch .
- 3 Touch  **Programmable keys**.

**Figure 67: Programmable Keys Screen**

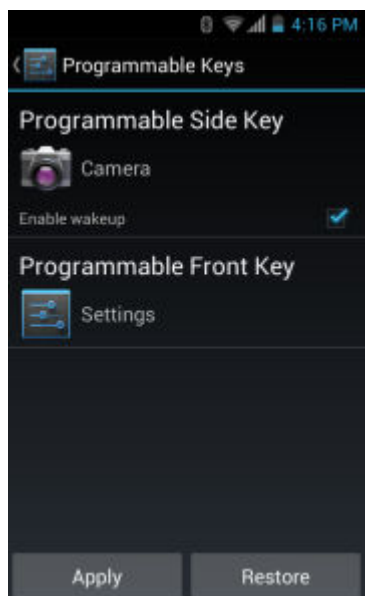



- 4 Select the button to remap.
  - **Programmable Side Key** - Side Programmable button set to scanning by default.
  - **Programmable Front Key** - .Oval button  below display.
- 5 Touch the **KEYS** tab or the **APPS** tab that lists the available functions and applications.
- 6 Touch a function or 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 68: Remapped Button



- 7 If setting the **Programmable Side Key**, check the **Enable wakeup** checkbox to wake the TC55 if the Programmable key is pressed.
- 8 Touch **Apply** to set the new key function.
- 9 Touch .

## Exporting a Programmable Key Configuration File

The Programmable Key configuration can be exported to an xml file and imported into other TC55 devices.

### Procedure:


- 1 Touch .
- 2 Touch .
- 3 Touch  **Programmable Keys**.
- 4 Touch .
- 5 Touch **Export**.





**Step result:** The configuration file (`key_config.xml`) is saved in the folder: `/enterprise/device/settings/keyboard`.

- 6 Copy the xml file from the folder to a host computer. See [USB Communication on page 45](#) for more information.

## Importing a Programmable Key Configuration File

### Procedure:

- 1 Copy the configuration file (`key_config.xml`) from a host computer to the TC55. See [USB Communication on page 45](#) for more information.
- 2 On the TC55, use **File Browser** to move the file to the folder: `/enterprise/device/settings/keyboard`.
- 3 Touch .

- 4 Touch .
- 5 Touch  **Programmable Keys**.
- 6 Touch .
- 7 Touch **Import**.
- 8 Touch `/enterprise/device/settings/keyboard/keys_config.xml` to import the configuration file or touch **Factory Settings** to reset the key settings back to the factory default.
- 9 Touch .

## 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.

**Result:** 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 phrase 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 TC55. Touch  >  > **About device**.

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

- **Battery level** - Indicates the battery charge level.
- **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.
- **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
- **Serial number** - Displays the serial number of the device.
- **Up time** - Displays the time that the TC55 has been running since being turned on.
- **SW components** - Lists filenames and versions for various software on the TC55.
- **Legal information** - Opens a screen to view legal information about the software included on the TC55.
- **Battery Management** - Displays information about the battery.
- **SE 13 version** - Displays date of SE13 table.
- **QCN version** - Displays the QCN version number.
- **HW version** - Displays the hardware version.
- **TP FW Version** - Displays the touch panel firmware version.
- **WCNSS INI Version** - Displays .
- **S/N** - Displays the device serial number.
- **Model number** - Displays the device model number.
- **Android version** - Displays the operating system version.
- **Baseband version** - Displays WAN radio firmware version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.



# Chapter 8

## 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 45](#) 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

---

Get tools at <http://developer.android.com>.




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

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

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

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

Opens 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:

- **Take bug report**
- **Desktop backup password**
- **Stay awake**
- **Protect SD card**

- **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**
  - **Host Mode power 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, the USB driver has to be modified. This assumes that the development SDK has been installed on the host computer. Go to <http://developer.android.com/sdk/index.html> for details on setting up the development SDK.

ADB driver for Windows and Linux are available on the Motorola Solutions Support Central web site at <http://supportcentral.motorolasolutions.com>. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

## 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 112](#).
- Android Debug Bridge, see [Installing Applications Using the Android Debug Bridge on page 112](#).
- Mobility Services Platform (MSP) for Android.



## Installing Applications Using the USB Connection



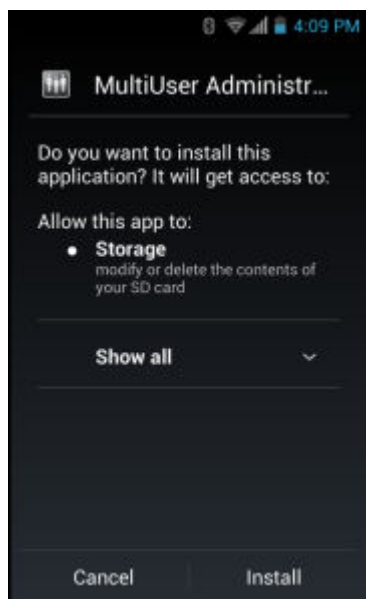
### Caution:

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 45](#).
- 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 45](#)
- 4 On the device, touch .
- 5 Touch  to view files on a microSD card or Internal Storage.
- 6 Locate the application .apk file.
- 7 Touch the application file to begin the installation process.
- 8 To confirm installation and accept what the application affects, touch **Install**. otherwise touch **Cancel**.

**Figure 69: Accept Installation Screen**



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

## Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.






### Caution:

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

**Prerequisites:** Ensure that the ADB drivers are installed on the host computer. See [ADB USB Setup on page 111](#).

### Procedure:

- 1 Connect the device to a host computer using USB. See [USB Communication on page 45](#).
- 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>
```

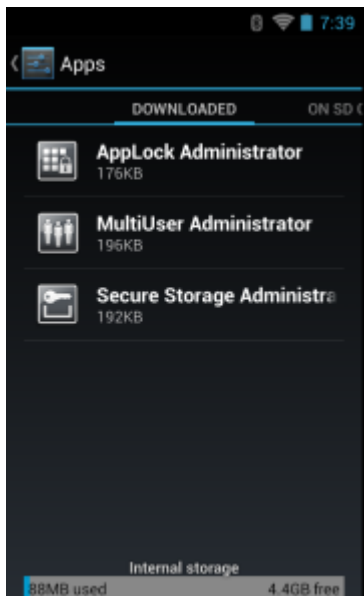
 where: <application> = the path and filename of the apk file.
- 9 Disconnect the device from the host computer. See [USB Communication on page 45](#).

## Uninstalling an Application

### Procedure:

- 1 Touch .
- 2 Touch .
- 3 Touch  **Apps**.
- 4 Swipe left or right until the **Downloaded** screen displays.

**Figure 70: Downloaded Screen**



- 5 Touch the application to uninstall.
- 6 Touch **Uninstall**.
- 7 Touch **OK** to confirm.

## Mobility Services Platform

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

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

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

## Updating the System

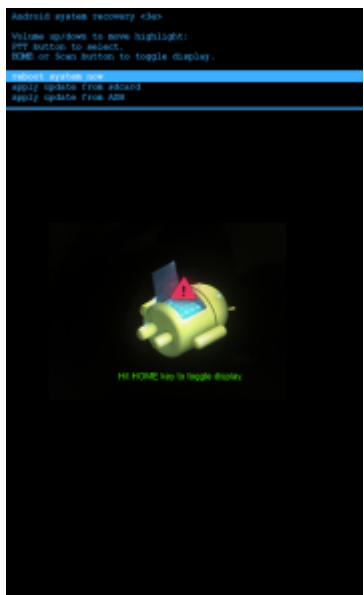
---

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://supportcentral.motorolasolutions.com>.
  - b) Download the appropriate System Update package to a host computer.
- 2 Locate the System Update package file on the host computer and un-compress the file into a separate directory.
- 3 Copy the TC55JenRUxxxxxxx.zip file to the root directory of the microSD card or Internal Storage. See [USB Communication on page 45](#) for more information.
- 4 Press and hold the Power button until the menu appears.
- 5 Touch **Reset**.
- 6 Press and hold the Volume Up button.
- 7 When the System Recovery screen appears, release the button.

**Figure 71: System Recovery Screen**



- 8 Press the Volume Up and Volume Down buttons to navigate to **apply from SD card** or **apply from internal**.
- 9 Press the Scan button.
- 10 Press the Volume Up and Volume Down buttons to navigate to the FullPackageUpdate.zip file.
- 11 Press the Scan button. The System Update installs and then the TC55 resets.

## Storage

The device contains four types of file storage:

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

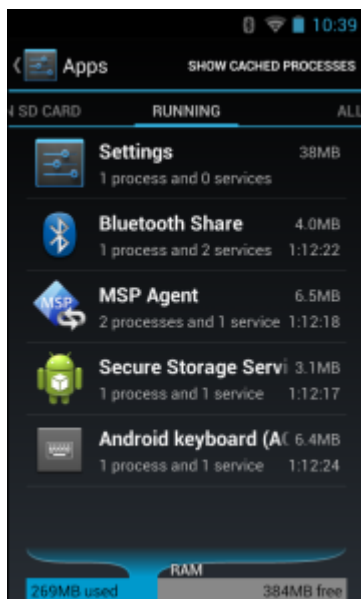
## Random Access Memory

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 72: Running Screen**






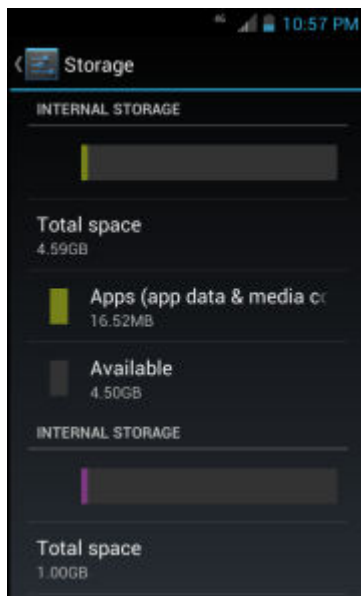
The bar at the bottom of the screen displays the amount of used and free RAM.

## Internal Storage

There are two types of Internal Storage. The first type, is the memory where most applications and data are stored.




The operating system protects all data and applications from power-related loss. Because the operating system mounts the entire file system in persistent storage, TC55 devices provide a reliable storage platform even in the absence of battery power. Internal Storage provides application developers with a reliable storage system available through the standard ext4 file system. Data in Internal storage is lost upon a Factory or Enterprise reset.

Internal Storage is approximately 4.6 GB (formatted). To view the available internal storage, touch  >  >  > **Storage**.

**Figure 73: Storage Settings - Internal Storage**

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

The second type acts like an internal SD card where pictures, videos and data files are stored. This memory can be accessed from a host computer using a USB connection.

This Internal Storage is approximately 1.0 GB (formatted). To view the available internal storage, touch   >  **Storage**.




**Figure 74: Storage Settings - Internal Storage**

- **Total space** - Displays the total amount of space.
- **Pictures, videos** - Displays the available space used for pictures and videos.

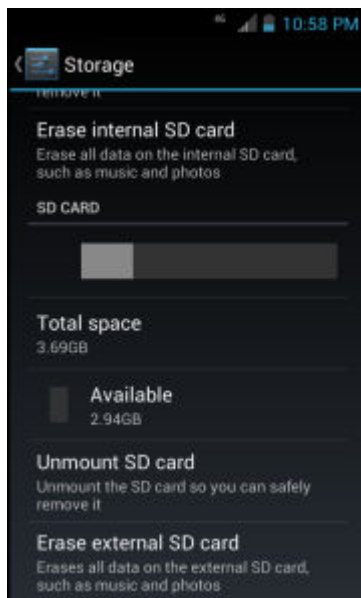
- **Available** - Displays the available space on the internal storage.
- **Unmount SD card** - Unmounts the internal SD card.
- **Erase internal SD card** - Permanently erases everything on the Internal Storage (internal SD card).

## External Storage

The TC55 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the TC55 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 75: Storage Settings**



- **Total space** - Displays the total amount of space on the installed microSD card.
- **Apps** - Displays the available space used for applications and media content on the installed microSD card.
- **Pictures, videos** - Displays the available space used for pictures and videos on the installed microSD card.
- **Available** - Displays the available space on the installed microSD card.
- **Unmount SD card** - Unmounts the installed microSD card from the TC55 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.


## 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.

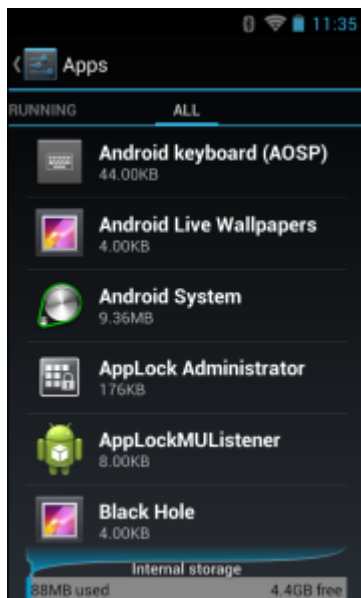
## Application Management

---

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 76: Manage Applications Screen**



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

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

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


When on the **Downloaded**, **All**, or **On SD card** tab, 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 113](#) 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.

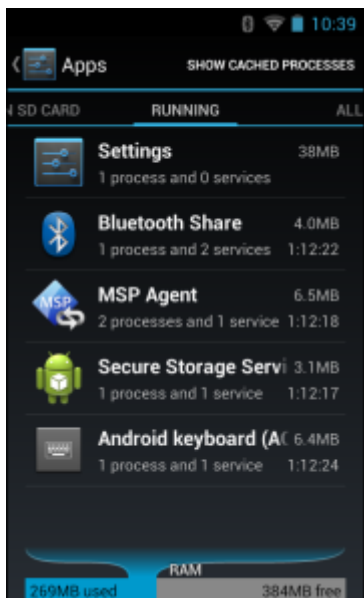
## Stopping an Application


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 77: Running Applications**




- 4 The graph at the bottom of the screen displays the total RAM in use and the amount free. Touch an application, process, or service.
- 5  **Note:** Stopping an application or operating system processes and services disables one or more dependant functions on the device. The device may need to be reset to restore full functionality.

Touch **Stop**.

## Changing Application Location

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

### Procedure:

- 1 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 SD card** to move the bulk of the application from the device's internal storage to the microSD card.
- 6 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.

# Chapter

# 9

## Maintenance and Troubleshooting

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

### Maintaining the TC55

---

For trouble-free service, observe the following tips when using the TC55:

- Do not scratch the screen of the TC55. When working with the TC55, use a finger, glove or approved stylus or pen intended for use with a capacitive touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the TC55 screen.
- The touch-sensitive screen of the TC55 is glass. Do not drop the TC55 or subject it to strong impact.
- Protect the TC55 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 TC55 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the TC55. If the surface of the TC55 screen becomes soiled, clean it with a soft cloth moistened with isopropyl alcohol.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.

### Battery Safety Guidelines

---

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Follow battery usage, storage, and charging guidelines found in this guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between 0 °C and +45 °C (+32 °F and +113 °F)
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact Motorola Solutions Global Customer Support Center.
- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.

- Battery usage by children should be supervised.
- Please follow local regulations to properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, contact Motorola Solutions Global Customer Support Center to arrange for inspection.

## 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 Solutions 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, 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; aqueous 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 TC55

### 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.

## Connector Cleaning

To clean the connectors:

### Procedure:

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



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

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

## Cleaning Cradle Connectors

To clean the connectors on a cradle:

### Procedure:

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



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

- 5 Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.
- 6 Remove any lint left by the cotton-tipped applicator.

- 7 If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.
- 8 Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.  
If the temperature is low and humidity is high, longer drying time is required. Warm temperature and dry humidity requires less drying time.

## Troubleshooting

---

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

### Troubleshooting the TC55

**Table 4: Troubleshooting the TC55**

Problem	Cause	Solution
When the user presses the Power button, the TC55 does not turn on.	Battery is completely discharged.	Re-charge or replace the battery.
	Battery not installed properly.	Install the battery properly. See Installing the Battery.
	Power button not held down long enough.	Press the Power button until the LED lights green.
	TC55 not responding.	Perform a hard reset. See Resetting the TC55.
When the user presses the Power button the TC55 does not turn on but a charge battery icon appears on the screen.	Battery charge level is very low.	Re-charge or replace the battery.
After connecting the TC55 to the Rugged Charge Cable, a battery charging icon appears on the screen.	Battery is depleted but is charging.	Press and hold the Power button to turn on the TC55.
When charging, the LED slowly blinks red.	The TC55 is at an extremely low power state.	Charge the TC55 for a few minutes. The LED will change to flashing green then press the Power button to turn on the TC55. If LED continuously blinks red, check power connections. Disconnect and reconnect connections.
Battery did not charge.	Battery failed.	Replace battery. If the TC55 still does not operate, perform a hardware reset.
	TC55 was removed from power while battery was charging.	Insert TC55 in cradle or attach Charge Cable. The 2940 mAh battery fully charges in approximately three hours and the 4410 mAh battery charges in approximately 4.5 hours.

*Table continued...*






Problem	Cause	Solution
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	TC55 removed from USB cable or disconnected from host computer during communication.	Reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
During data communication over Wi-Fi, no data transmitted, or transmitted data was incomplete.	Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
	You moved out of range of an access point.	Move closed to an access point.
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	Bluetooth radio is not on.	Turn on the Bluetooth radio.
	You moved out of range of another Bluetooth device.	Move without 10 m (32.8 ft.) of the other device.
During data communication over WAN, no data transmitted, or transmitted data was incomplete.	You are in an area of poor cellular service.	Move into an area that has better service.
	APN is not set up correctly.	See system administrator for APN setup information.
	SIM card not installed properly.	Remove and re-install the SIM card. See <i>Installing the SIM Card on page 21</i> .
	Data plan not activated.	Contact your service provider and ensure that your data plan is enable.
No sound.	Volume setting is low or turned off.	Adjust the volume.
TC55 turns off.	TC55 is inactive.	The display turns off after a period of inactivity. Set this period to 15 seconds, 30 seconds, 1, 2, 5, 10, or 30 minutes.
	Battery is depleted.	Recharge or replace the battery.
	Extreme battery temperature.	Move device to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).
A message appears stating not enough storage memory.	Too many applications installed on the TC55.	Remove user-installed applications on the TC55 to recover memory. Select  >  <b>Apps &gt; Downloaded</b> . Select the unused programs and touch <b>Uninstall</b> .

Table continued...

Problem	Cause	Solution
The TC55 does not decode when reading bar code.	DataWedge is not enable.	Ensure that DataWedge is enabled and configured properly. See <a href="#">DataWedge Configuration on page 47</a> for more information.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between the TC55 and bar code is incorrect.	Place the TC55 within proper scanning range.
	TC55 is not programmed for the bar code type.	Program the TC55 to accept the type of bar code being scanned. See <a href="#">DataWedge Configuration on page 47</a> for DataWedge configuration.
TC55 cannot find any Bluetooth devices nearby.	TC55 is not programmed to generate a beep.	If the TC55 does not beep on a good decode, set the application to generate a beep on good decode.
	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.

## Five-Slot Charge Only Cradle CRDUNIV-55–5000R Troubleshooting

**Table 5: Troubleshooting the Five-Slot Charge Only Cradle**

Problem	Cause	Solution
Battery is not charging.	TC55 removed from the cradle too soon.	Replace the TC55 in the cradle. The 2,940 mAh battery fully charges in approximately three hours and the 4,410 mAh battery charges in approximately 4.5 hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	TC55 is not inserted correctly in the cradle.	Remove the TC55 and reinsert it correctly. Verify charging is active. Touch  >  >  <b>About device</b> > <b>Status</b> to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

# Chapter 10

## Technical Specifications

The following sections provide technical specification for the device.

### TC55 Technical Specifications

---

The following table summarize the TC55's intended operating environment and technical hardware specifications.

**Table 6: TC55 Technical Specifications**

Item	Description
<b>Physical Characteristics</b>	
Dimensions	Height: 137 mm (5.4 in.) Width: 69 mm (2.7 in.) Depth (with 2940 mAh battery): 15.9 mm (0.63 in.) Depth (with 4410 mAh battery): 22.5 mm (0.89 in.)
Weight	220 g (7.8 oz)
Display	4.3 in. color WVGA; 800 x 480, 700 NITs
Touch Panel	Gorilla Glass® 2
Backlight	LED backlight
Battery Pack	Rechargeable Lithium Ion 3.7V, 2,940 or 4,410 mAh Smart battery
Expansion Slot	User accessible microSD slot, up to 32 GB.
Connectivity	USB 2.0 (Host/Client)
Notification	LED, audio and vibration.
Keypad Options	On-screen keyboard and 4 capacitive front panel keys.
Audio	Speakers, dual noise cancelling microphones and headset connector (3.5 mm jack with microphone). Three speakers, including two front facing speakers; dual noise-cancelling microphones; high-quality speaker phone; 3.5 mm headset jack and Bluetooth wireless headset support.
<b>Performance Characteristics</b>	
CPU	1.5 GHz Dual Core Processor
Operating System	Android-based, Android Open-Source Project (AOSP) 4.1.2.

*Table continued...*

Item	Description
Memory	1 GB RAM, 8 GB Flash
Output Power (USB)	300 mA
<b>User Environment</b>	
Operating Temperature	-10 °C to 50 °C (14 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0° C to 40° C (32 °F to 104 °F)
Humidity	5% to 95% RH non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) drops per MIL-STD 810G specifications. With protective boot: Multiple 1.2 m (4 ft.) drops to concrete across the operating temperature range.
Tumble Specification	150 0.5 m (1.5 ft.) tumbles (300 drops); With protective boot: 300 0.5 m (1.5 ft.) tumbles (600 drops); per applicable IEC tumble specifications.
Sealing	IP67 per applicable IEC sealing specifications.
<b>Wireless WAN Data and Voice Communications</b>	
Wireless Wide Area Network (WWAN) radio	4G LTE, HSPA+, DC-HSPA, EDGE/GPRS/GSM
Frequency band	<b>TC55AH:</b> GSM/EDGE: 850/900/1800/1900 MHz WCDMA: FDD2, FDD4, FDD5, FDD17 LTE Americas: LTE Band 2, LTE Band 4, LTE Band 5, LTE Band 17 <b>TC55BH:</b> GSM/EDGE: 850/900/1800/1900 MHz WCDMA: FDD1, FDD2, FDD5, FDD8
GPS	Integrated, Autonomous, Assisted-GPS (A-GPS), GLONASS
<b>Wireless LAN Data Communications</b>	
Wireless Local Area Network (WLAN) radio	IEEE® 802.11a/b/g/n with internal antenna
Data Rates Supported	<b>802.11b:</b> 1, 2, 5.5, 11 Mbps <b>802.11a/g:</b> 6, 9, 12, 18, 24, 36, 48, 54 Mbps <b>802.11n:</b> 6.5, 13, 19.5, 26, 39, 52, 58.5, 65 Mbps Note that 802.11n data rates may be higher.
Operating Channels	Channel 36-165 (5180 – 5825 MHz), Channel 1-13 (2412-2472 MHz); actual operating channels/frequencies depend on regulatory rules and certification agency
Security	<b>Security Modes:</b> Legacy, WPA and WPA2

*Table continued...*

Item	Description
	<p><b>Encryption:</b> WEP (40 and 128 bit), TKIP and AES</p> <p><b>Authentication:</b> TLS, TTLS (MS-CHAP), TTLS (MS-CHAP v2), TTLS (PAP), PEAP (MS-CHAP v2), PEAP (GTC).</p>
Spreading Technique	Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM)
<b>Wireless PAN Data and Voice Communications</b>	
Bluetooth	Class II, v 4.0; integrated antenna.
<b>Data Capture</b>	
Linear Imager	Captures 1D bar codes.
Camera	For bar code scanning and image capture: 8 MP auto-focus camera; captures 1D and 2D bar codes, photographs, video, signatures and documents.
CS3070 Bluetooth Scanner (optional)	Captures 1D bar codes.
RS507 Hands-free Imager (optional)	Captures 1D and 2D bar codes.
<b>Sensors</b>	
Motion Sensor	3-axis accelerometer that enables motion sensing applications for dynamic screen orientation and power management.
Ambient Light Sensor	Automatically adjusts required display backlight to maximize power efficiency.
Proximity Sensor	Automatically detects when the user places the handset against head during a phone call to disable display output and touch input.
Electronic Compass	Independent — does not depend on GPS.
<b>Imager (SE655) Specifications</b>	
Scan Repetition Rate	Nominally 50 scans/second
Scan Angle	$53.3^\circ \pm 3^\circ$
Roll	$\pm 25^\circ$
Pitch Angle	$\pm 65^\circ$ from normal
Skew Tolerance	$\pm 50^\circ$ from normal
Ambient Light	Fluorescent: 450 ft. candles (4845 lux) High Efficiency Fluorescent: 450 ft. candles (4845 lux) Incandescent: 450 ft. candles (4845 lux) Mercury Vapor: 450 ft. candles (4845 lux) Sodium Vapor: 450 ft. candles (4845 lux) Sunlight: 900 ft. candles (9690 lux)
<b>Supported Symbologies</b>	

*Table continued...*

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

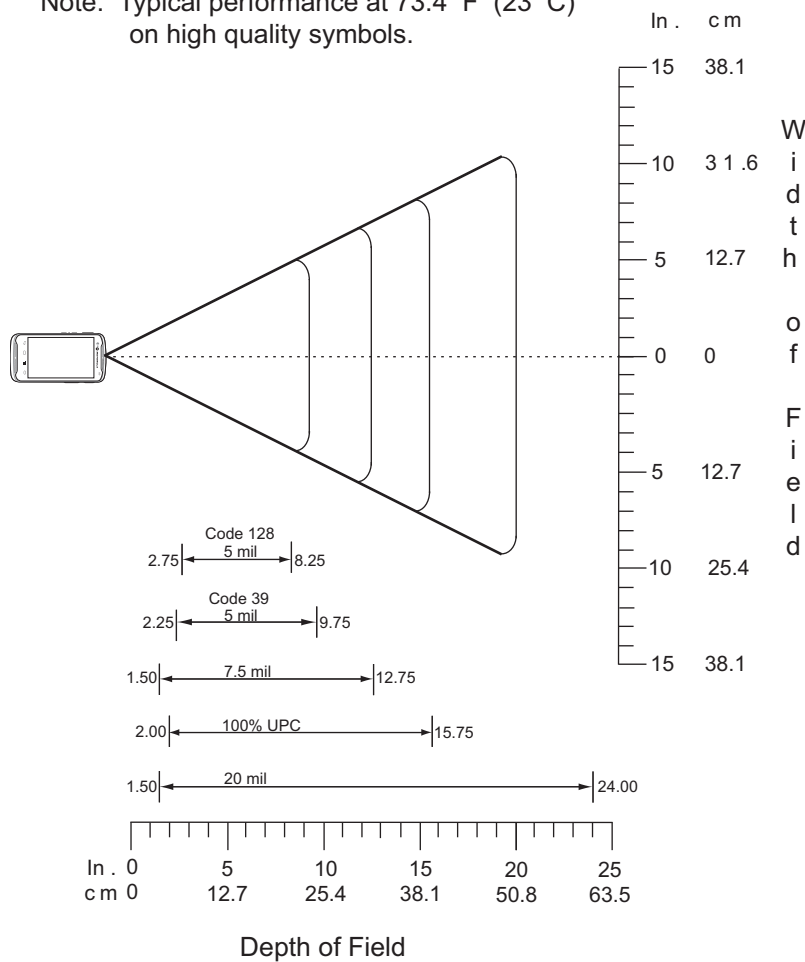
## TC55 Decode Zone

### SE655

The figure below shows the decode zone for the SE-655. Typical values appear. [Table 7: SE-655 Decode Distances on page 131](#) lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

**Figure 78: SE-655 Decode Zone**

Note: Typical performance at 73.4° F (23° C)  
on high quality symbols.



\*Minimum distance determined by symbol length and scan angle

## SE-655 Decode Distances

**Table 7: SE-655 Decode Distances**

Symbol Density / Bar Code Type	Typical Working Ranges	
	Near	Far
5.0 mil Code 128	2.75 in 7.00 cm	8.25 in 21.0 cm
5.0 mil Code 39	2.25 in 5.70 cm	9.75 in 24.8 cm
7.5 mil Code 39	1.5 in 3.80 cm	12.75 in 32.4 cm

*Table continued...*

Symbol Density / Bar Code Type	Typical Working Ranges	
	Near	Far
100% UPC-A	2.00 in 5.10 cm	15.75 in 40.0 cm
	See Note 2	
20 mil Code 39	1.50 in 3.80 cm	24.0 in 61.0 cm
	See Note 2	

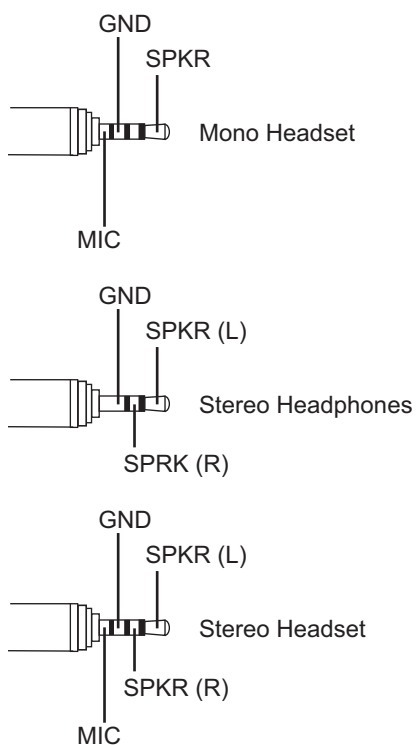
**Note:**

- 1 Distances measured from front edge of scan engine chassis.
- 2 Near distances are Field of View (FOV) limited.
- 3 Maximum allowable roll angle of symbols relative to the engine mounting base plane is +/- 3.0 degrees.

## TC55 Connector Pin-Outs

### Headset Connector

Figure 79: Headset Connector

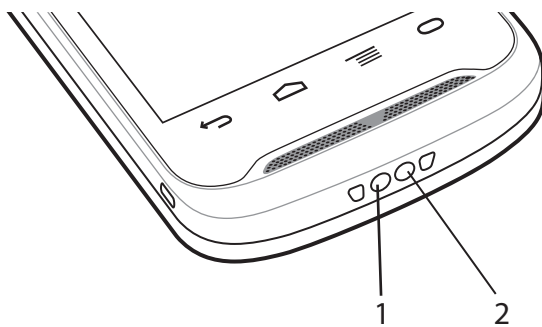


**Table 8: Headset Connector Pin-Outs**

Signal name	Description
MIC	Microphone positive
SPKR	Speaker (mono)
SPKR (R)	Right Speaker
SPKR (L)	Left Speaker
GND	Ground

**Power Connector**

**Figure 80: Power Connector**

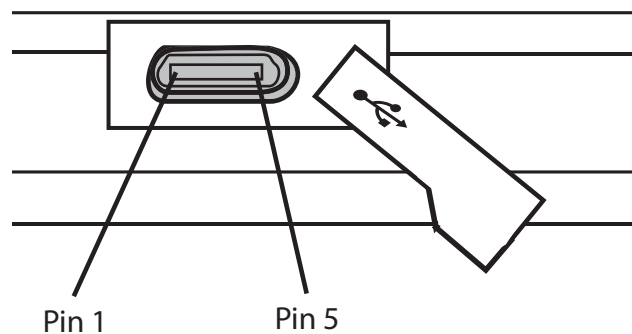


**Table 9: Power Connector Pin-Outs**

Pin	Description
1	+5 VDC input power.
2	Ground

**USB Connector**

**Figure 81: micro-B USB Connector**



**Table 10: micro-B USB Connector Pin-Outs**

Pin	Description
1	+5 VDC

*Table continued...*

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

## Five-Slot Charge Only Cradle CRDUNIV-55-5000R Technical Specifications

**Table 11: Five-Slot Charge Only Cradle Technical Specifications**

Item	Description
Dimensions	Height: 90.1 mm (3.5 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)
Weight	1.31 kg (2.89 lbs.)
Input Voltage	12 VDC
Power Consumption	37.5 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

# Chapter 11

## Keypad Remap Strings

**Table 12: Remap Key Event/Scancodes**

Key Event	Scancode
SOFT_LEFT	105
SOFT_RIGHT	106
HOME	102
BACK	158
CALL	231
ENDCALL	107
0	11
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
STAR227	227
POUND	228
DPAD_UP	103
DPAD_DOWN	108
DPAD_LEFT	105
DPAD_RIGHT	106
DPAD_CENTER	232
VOLUME_UP	115
VOLUME_DOWN	114
CAMERA	212

*Table continued...*

Key Event	Scancode
A	30
B	48
C	46
D	32
E	18
F	33
G	34
H	35
I	23
J	36
K	37
L	38
M	50
N	49
O	24
P	25
Q	16
R	19
S	31
T	20
U	22
V	47
W	17
X	45
Y	21
Z	44
COMMA	51
PERIOD	52
ALT_LEFT	56
ALT_RIGHT	100
SHIFT_LEFT	42
SHIFT_RIGHT	54
TAB	15
SPACE	57
EXPLORER	150

*Table continued...*

Key Event	Scancode
ENVELOPE	155
ENTER	28
DEL	111
GRAVE	399
MINUS	12
EQUALS	13
LEFT_BRACKET	26
RIGHT_BRACKET	27
BACKSLASH	43
SEMICOLON	39
APOSTROPHE	40
SLASH	53
AT	215
PLUS	78
MENU	139
SEARCH	217
PAGE_UP	59
PAGE_DOWN	60
PICTSYMBOLS	61
SWITCH_CHARSET	62
BUTTON_A	63
BUTTON_B	64
BUTTON_C	65
BUTTON_X	66
BUTTON_Y	67
BUTTON_Z	68
BUTTON_L1	183
BUTTON_R1	184
BUTTON_L2	185
BUTTON_R2	186
BUTTON_THUMBL	187
BUTTON_THUMBR	188
BUTTON_START	189
BUTTON_SELECT	190
BUTTON_MODE	191



# Index

## A

android version [17](#)  
approved cleanser [122](#)

## B

battery  
    charging [28](#)  
    installation [26](#)  
build number [17](#)

## C

camera [17](#)  
charge cable [39](#)  
charging error [29](#)  
charging indications [29](#)  
charging temperature [29](#)  
cleaning [122](#)  
cleaning instructions [122](#)  
configuration [17](#)  
cradle  
    connector cleaning [123](#)

## D

display  
    cleaning [123](#)

## F

five slot charge only cradle [40](#)  
five-slot charge only cradle [39](#)  
five-slot charge only cradle base [39](#)

## H

harmful ingredients [122](#)

## I

installing the battery [26](#)

## M

main battery charging [28](#)  
memory [17](#)  
micro USB cable [39](#)

## O

operating system [17](#)

## P

power on [30](#)

## R

radios [17](#)

## S

serial number [17](#)  
service information [19](#)  
setup [21](#)  
SIM card installation [22](#)  
soft reset [36](#)  
spare battery [39](#)

## V

vehicle cradle [39](#)

