TC51

Touch Computer

Integrator Guide
for Android™ Version 6.0.1

ZEBRA

TC51 INTEGRATOR GUIDE
FOR ANDROID VERSION 6.0.1

Revision History

Changes to the original manual are listed below:

Change	Date	Description
-01 Rev A	11/2016	Initial release.
-02 Rev B	12/2016	Update Ethernet setup information.

TABLE OF CONTENTS

Table of Contents

ABOUT THIS GUIDE

Introduction

This guide provides information about using the TC51 touch computer and accessories.

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

Documentation Set

The documentation set for the TC51 provides information for specific user needs, and includes:

- *TC51* Touch Computer Quick Start Guide - describes how to get the TC51 up and running.

- *TC51* Touch Computer User Guide for Android Version 6.0.1 - describes how to use the TC51.

- *TC51* Touch Computer Integrator Guide for Android Version 6.0.1 - describes how to set up the TC51 and accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
TC510K-1	WLAN: 802.11 a/b/g/n/d/h/i/k/r WPAN: Bluetooth v4.1 Low Energy	5.0" High Definition (1280 x 720) LCD	2 GB RAM / 16 GB Flash or 4 GB RAM / 32 GB Flash	2D imager and integrated NFC	Android-based, Android Open-Source Project 6.0.1
TC510K-2	WLAN: 802.11 a/b/g/n/d/h/i/k/r WPAN: Bluetooth v4.1 Low Energy	5.0" High Definition (1280 x 720) LCD	2 GB RAM / 16 GB Flash or 4 GB RAM / 32 GB Flash	2D imager and integrated NFC	Android-based, Google Mobile Services (GMS) 6.0.1.

Software Versions

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

- **Model number**- Displays the model number.

- **Android version** - Displays the operating system version.

- **Kernel version** - Displays the kernel version number.

- **Build number** - Displays the software build number.

To determine the device serial number touch 🔧 > ⓘ **About phone** > **Status**.

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

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started* provides information on getting the TC51 up and running for the first time.

- *Chapter 2, Accessories* describes the available accessories and how to use them with the TC51.

- *Chapter 3, DataWedge* describes how to use and configure the DataWedge application.

- *Chapter 5, Settings* provides the settings for configuring the TC51.

- *Chapter 6, Application Deployment* provides information for developing and managing applications.

- *Chapter 7, Maintenance and Troubleshooting* includes instructions on cleaning and storing the TC51, and provides troubleshooting solutions for potential problems during TC51 operation.

- *Appendix A, Technical Specifications* provides the technical specifications for the TC51.

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.

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.

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.

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.**

Related Documents

- *TC51Touch Computer Quick Start Guide*, p/n MN-002879-xx.
- *TC51 Touch Computer Regulatory Guide*, p/n MN-002880-xx.
- *TC51 Touch Computer User Guide* for Android Version 6.0.1, p/n MN-002868-xx.

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

Service Information

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

When contacting support, please have the following information available:

- Serial number of the unit (found on manufacturing label)

- Model number or product name (found on manufacturing label)

- Software type and version number

- IMEI number
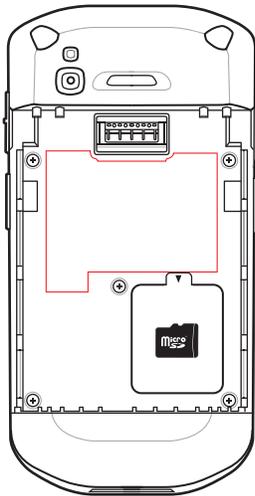
Customer Support responds to calls by email or telephone within the time limits set forth in support agreements.

If the problem cannot be solved by Customer Support, the user may need to return the equipment for servicing and will be given specific directions. We are not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty. Remove the microSD card from the device before shipping for service.

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

CHAPTER 1 GETTING STARTED

Introduction

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

Setup

Perform this procedure to start using the TC51 for the first time.

1. Install a micro secure digital (SD) card (optional).
2. Install the battery.
3. Charge the TC51.
4. Power on the TC51.

Installing a microSD Card

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

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

1. Lift the access door.
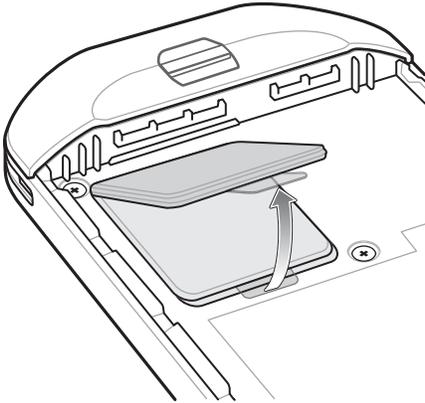
Figure 1-1   *Lift Access Door*

2.   Slide the microSD card holder to the unlock position.
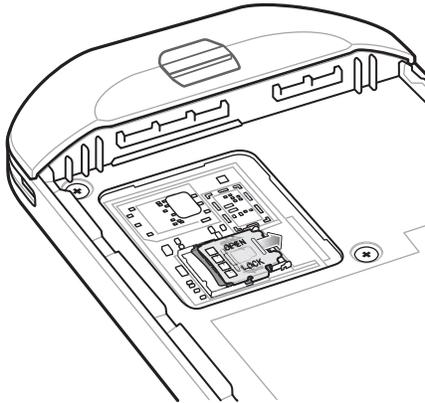
Figure 1-2   *Unlock microSD Card Holder*

3.   Lift the microSD card holder.
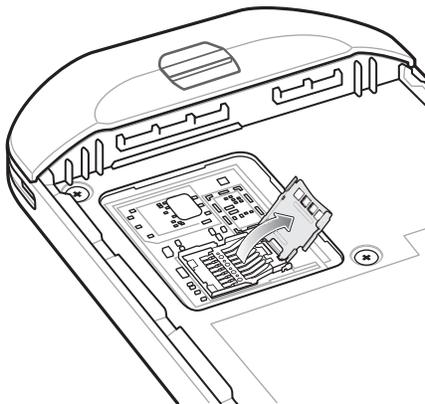
Figure 1-3   *Lift the microSD Card Holder*

4.   Insert the microSD card into the card holder door ensuring that the card slides into the holding tabs on each side of the door.
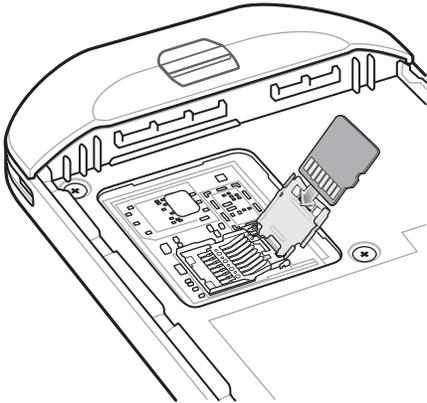
Figure 1-4   *Insert microSD Card in Holder*

5. Close the microSD card holder and slide into the lock position.
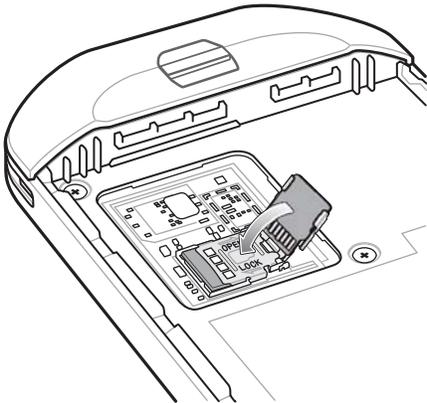
Figure 1-5   *Re-install Access Door*

⚠️   *CAUTION* Access door must be replaced and securely seated to ensure proper device sealing.

6. Re-install the access door.
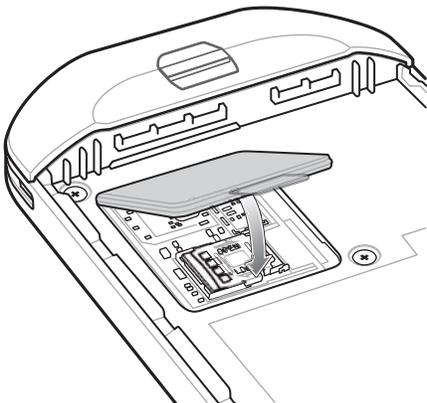
Figure 1-6   *Replace Access Door*

Installing the Battery

1.   Insert the battery, bottom first, into the battery compartment in the back of the TC51.
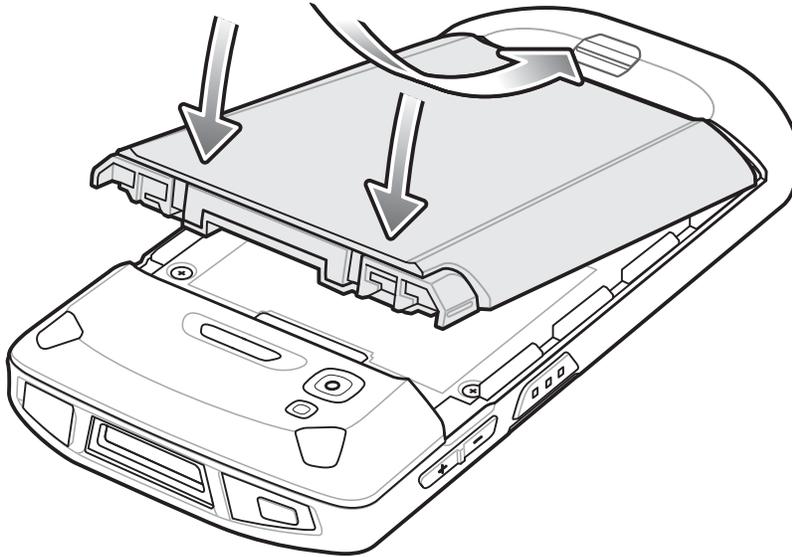
Figure 1-7   *Insert Bottom of Battery into Battery Compartment*

2.   Press the battery down into the battery compartment until the battery release latches snap into place.

Charging the Battery

Before using the TC51 for the first time, charge the main battery until the green Charging/Notification light emitting diode (LED) remains lit. To charge the TC51 use a cable or a cradle with the appropriate power supply. For information about the accessories available for the TC51 see *Chapter 2, Accessories* for more information.

The 4,300 mAh battery charges to 90% in less than 2.5 hours at room temperature.

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The TC51 or accessory always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the TC51 or accessory may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC51 or accessory indicates when charging is disabled due to abnormal temperatures via its LED and a notification appears on the display.

1.   To charge the main battery, connect the charging accessory to the appropriate power source.
2.   Insert the TC51 into a cradle or attach to a cable. The TC51 turns on and begins charging. The Charging/Notification LED blinks amber while charging, then turns solid green when fully charged.

Charging Indicators

Table 1-1   *Charging/Notification LED Charging Indicators*

State	LED	Indication
Off		TC51 is not charging. TC51 is not inserted correctly in the cradle or connected to a power source. Charger/cradle is not powered.
Slow Blinking Amber (1 blink every 4 seconds)		TC51 is charging.
Slow Blinking Red (1 blink every 4 seconds)		TC51 is charging but the battery is at end of useful life.
Solid Green		Charging complete.
Solid Red		Charging complete but the battery is at end of useful life.
Fast Blinking Amber (2 blinks/second)		Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).
Fast Blinking Red (2 blinks/second)		Charging error but the battery is at end of useful life., e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).

Replacing the Battery

⚠ **CAUTION** Do not add or remove microSD card during battery replacement.

1. Press the Power button until the menu appears.
2. Touch **Battery Swap**.
3. Follow the on-screen instructions.
4. Wait for the LED to turn off.
5. If hand strap is attached, remove hand strap.
6. Press the two battery latches in.
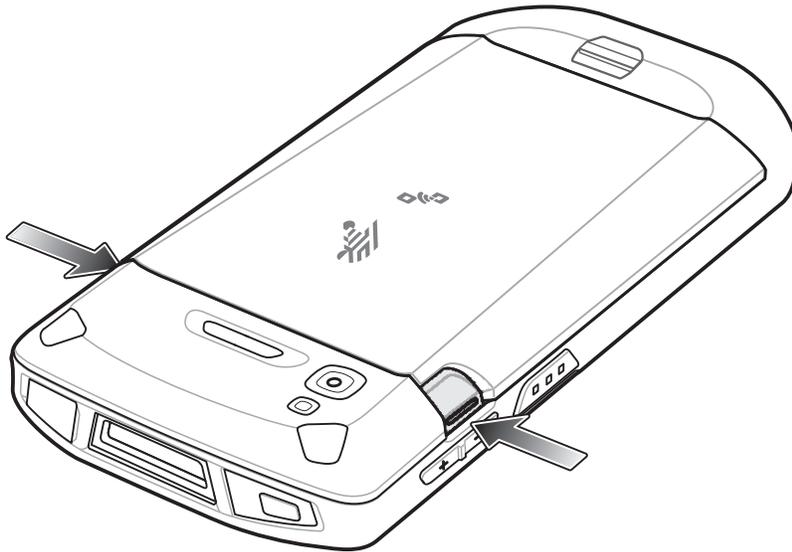
Figure 1-8   *Press Battery Latches*

7.   Lift the battery from the TC51.
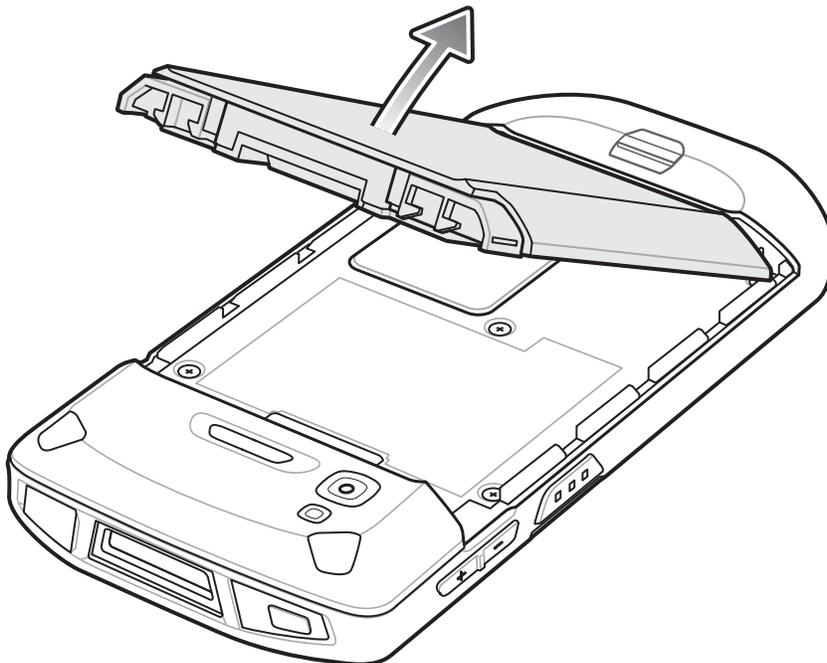
Figure 1-9   *Lift the Battery*

⚠ **CAUTION** Replace the battery within 90 seconds. After two minutes the device reboots and data may be lost.

8.   Insert the replacement battery, bottom first, into the battery compartment in the back of the TC51.

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

10. Replace the hand strap, if required.

11. Press the Power button to turn on the TC51.

Replacing the microSD Card

To replace the microSD card:

1. Press the Power button until the menu appears.
2. Touch **Power off**.
3. Touch **OK**.
4. If hand strap is attached, slide the hand strap clip up toward the top of the TC51 and then lift.
5. Press the two battery latches in.
6. Lift the battery from the TC51.
7. Lift the access door.
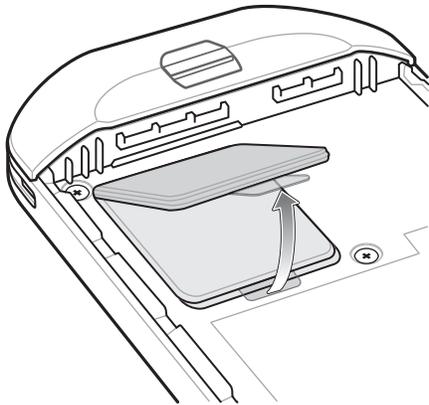
Figure 1-10   *Remove Access Door*

8. Remove microSD card from holder.
9. Press the access door down and ensure that it is properly seated.
10. Insert the replacement microSD card.

⚠️ **CAUTION** Access door must be replaced and securely seated to ensure proper device sealing.

11. Replace the access door.
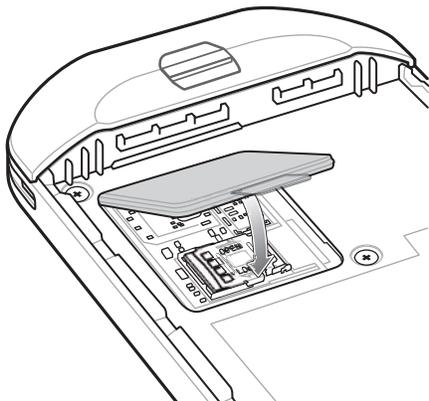
Figure 1-11   *Replace Access Door*

12. Insert the battery, bottom first, into the battery compartment in the back of the TC51.

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

14. Replace the hand strap, if required.

15. Press and hold the Power button to turn on the TC51.

Resetting the TC51

There are four reset functions:

- Soft reset
- Hard reset
- Enterprise reset. See *Performing an Enterprise Reset on page 6-12*.
- Factory reset See *Performing a Factory Reset on page 6-13*.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

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

2. Touch **Reset**.

3. The device reboots.

Performing a Hard Reset

⚠️ **CAUTION** Performing a hard reset with a SD card installed in the TC51 may cause damage or data corruption to the SD card.

Perform a hard reset if the TC51 stops responding.

1. Simultaneously press the Power, Scan and Volume Up buttons for at least four seconds.

2. When the screen turns off, release the buttons.

3. The TC51 reboots.

CHAPTER 2 ACCESSORIES

Introduction

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

Accessories

This table lists the accessories available for the TC51.

Table 2-1 *TC51 Accessories*

Accessory	Part Number	Description
Cradles		
1-Slot USB/Charge Only Cradle Kit	CRD-TC51-1SCU-01	Provides device charging and communication. Includes cradle, power supply, and DC line cord or PWR-BGA12V50W0WW.
4-Slot Charge Only Cradle with Battery Charger Kit	CRD-TC51-5SC4B-01	Charges up to four devices and four spare batteries. Includes, cradle, power supply, or PWR-BGA12V108W0WW and DC line cord
5-Slot Charge Only Cradle Kit	CRD-TC51-5SCHG-01	Charges up to five devices. Includes, cradle, power supply, or PWR-BGA12V108W0WW and DC line cord. Can accommodate one 4-Slot Battery Charger using the Battery Adapter Cup.
5-Slot Ethernet Cradle Kit	CRD-TC51-5SETH-01	Provides device charging and provides Ethernet communication for up to five devices. Includes cradle, power supply, and DC line cord. Can accommodate one 4-Slot Battery Charger using the Battery Adapter Cup.
Cradle Mount	BRKT-SCRD-SMRK-01	Mounts the 5-Slot Charge Only Cradle, 5-Slot Ethernet Cradle, and 4-Slot Battery Charger to a wall or rack.

Table 2-1   *TC51 Accessories (Continued)*

Accessory	Part Number	Description
Batteries and Chargers		
4,300 mAh PowerPrecision battery	BTRY-TC51-43MA1-01	Replacement battery (single pack).
	BTRY-TC51-43MA1-10	Replacement battery (10–pack).
4-Slot Battery Charger Kit	SAC-TC51-4SCHG-01	Charges up to four battery packs. Includes cradle, power supply and DC line cord
Vehicle Solutions		
Cigarette Light Adapter Auto Charge Cable	CHG-AUTO-USB1-01	Provides power to the device from a cigarette lighter socket.
Charge and Communication Cables		
Rugged Charge/USB Cable	CBL-TC51-USB1-01	Provides communication and power to the device. Use with power supply, p/n PWRS-14000-249R, sold separately.
Audio Accessories		
2.5 mm Audio Adapter	CBL-TC51-HDST25-01	Plugs into the device and provides audio to a wired headset with 2.5 mm plug.
2.5 mm Headset	HDST-25MM-PTVP-01	Use for PTT and VoIP calls
3.5 mm Audio Adapter	CBL-TC51-HDST35-01	Plugs into the device and provides audio to a wired headset with collared 3.5 mm plug.
3.5 mm Headset	HDST-35MM-PTVP-01	Use for PTT and VoIP calls.
Miscellaneous		
Rugged Boot	SG-TC51-EXO1-01	Provides additional protection for the device. Requires power supply PWR-WUA5V12W0xx.
Trigger Handle	TRG-TC51-SNP1-01	Adds gun-style handle with a scanner trigger for comfortable and productive scanning. Requires Rugged Boot.
Trigger Handle Kit (with Rugged Boot)	TRG-TC51-TRG1-01	Adds gun-style handle with a scanner trigger for comfortable and productive scanning.
Screen Protector	KT-TC51-SCRNP1-01	Add additional screen protection.
Carrying Solutions		
Soft Holster	SG-TC51-HLSTR1-01	Use to hold the device on hip. Accepts device with Rugged Boot and Trigger Handle
Hand Strap	SG-TC51-EHDSTP1-03	Replacement hand strap with hand strap mounting clip (3–pack).
Basic Hand Strap	SG-TC51-BHDSTP1-03	Provide a hand strap to assist in holding the TC51 without a Rugged Boot.
Stylus and Coiled Tether	SG-TC7X-STYLUS-03	Stylus with coiled tether (3-pack).

Table 2-1   *TC51 Accessories (Continued)*

Accessory	Part Number	Description
Power Supplies		
Power Supply	PWR-BGA12V50W0WW	Provides power to the 1-Slot USB Charge cradle and 4-Slot Spare Battery Charger. Requires AC line cord.
Power Supply	PWR-BGA12V108W0WW	Provides power to the 4-Slot Charge Only Cradle with battery Charger, 5-Slot Charge Only cradle and the 5-Slot Ethernet Cradle. Requires DC Line Cord, p/n 50–16002–029R and country specific three wire grounded AC line cord sold separately.
Power Supply	PWR-WUA5V12W0US	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in United States.
Power Supply	PWR-WUA5V12W0GB	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in the European Union.
Power Supply	PWR-WUA5V12W0EU	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in United Kingdom.
Power Supply	PWR-WUA5V12W0AU	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in Australia.
Power Supply	PWR-WUA5V12W0CN	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in China.
Power Supply	PWR-WUA5V12W0IN	Provides 5 VDC, 2.5 A power to the Rugged Charge/USB cable. Includes plug adapter for use in India.
DC Line Cord	CBL-DC-382A1-01	Provides power from the power supply (PWR-BGA12V108W0WW) to the 4-Slot Charge Only Cradle with Battery Charger, 5-Slot Charge Only Cradle and 5-Slot Ethernet Cradle.
DC Line Cord	CBL-DC-388A1-01	Provides power from the power supply (PWR-BGA12V50W0WW) to the 1-Slot USB/Charge Only Cradle and 4-Slot Battery Charger.

1-Slot USB Charge Cradle

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-2*.

The 1-Slot USB Charge Cradle:

- Provides 5 VDC power for operating the device.
- Charges the device's battery.
- Provides USB communication with host computer.
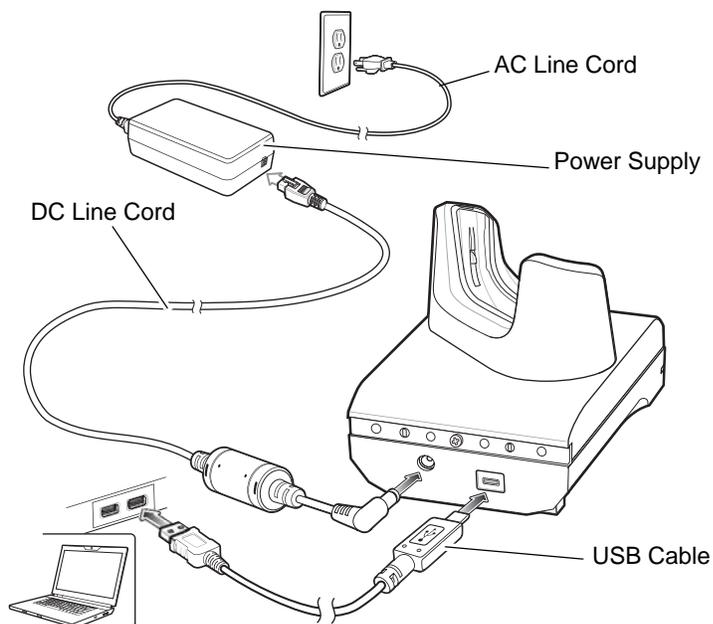
Figure 2-1   *1–Slot USB Charge Cradle Setup*

Charging the Device

To charge a device:

✓ **NOTE** If the device has a Rugged Boot, remove the cup insert before inserting the device. See *TC51 Touch Computer Integrator Guide for Android Version 6.0.1* for details.

1. Insert the device into the slot to begin charging.
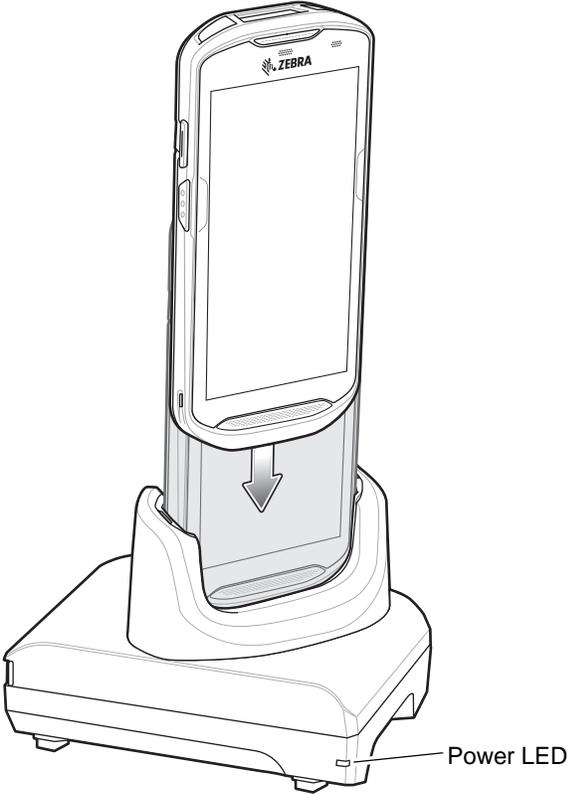
Figure 2-2   *Battery Charging*

2. Ensure the device is seated properly.

Inserting a TC51 with Rugged Boot into Cradle

Each cradle cup has an insert that must be removed prior to inserting the TC51 with Rugged Boot. Remove the insert and then insert the TC51 into the cup.
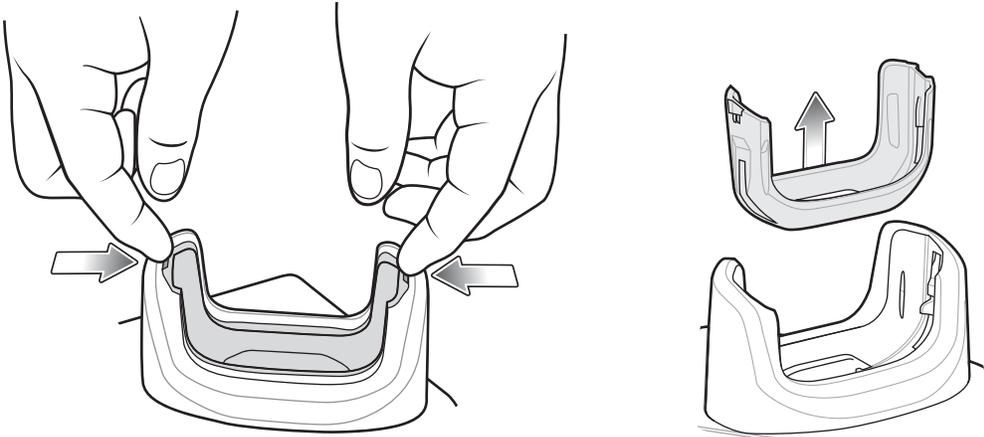
Figure 2-3   *Remove Insert from Cup*

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See *Table 1-1 on page 1-5* for device charging status. The 4,300 mAh battery charges to 90% in less than 2.5 hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

4-Slot Charge Only Cradle with Battery Charger

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-2*.

The 4-Slot Charge Only Cradle with Battery Charger:

- Provides 5 VDC power for operating the TC51.
- Simultaneously charges up to four TC51s and up to four spare batteries using the Battery Charger Adapter.
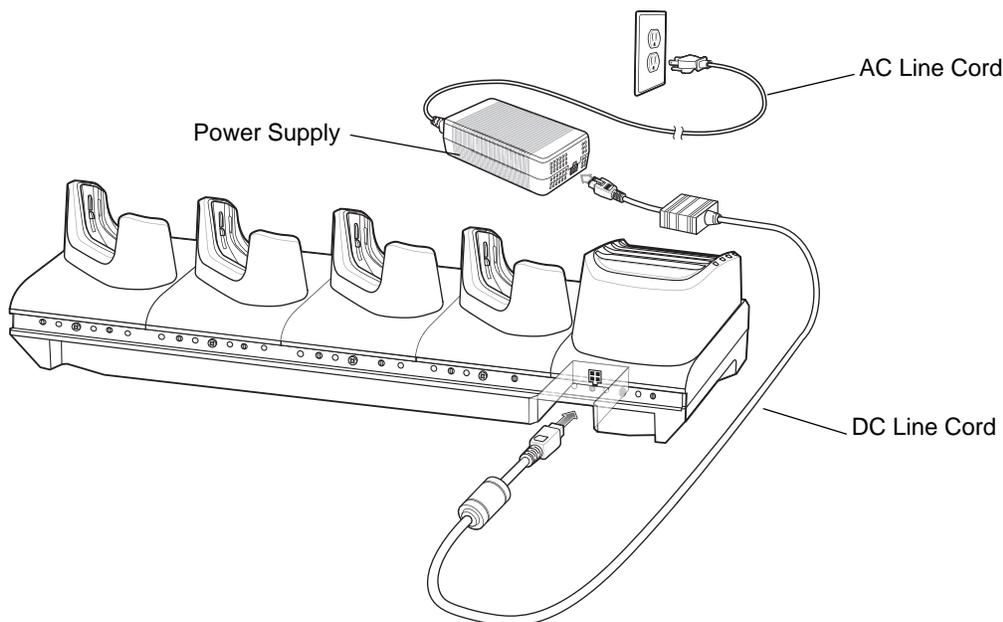
Figure 2-4   *4-Slot Charge Only Cradle with Battery Charger Setup*

Charging the TC51

To charge a device:

✓ **NOTE** If the device has a Rugged Boot, remove the cup insert before inserting the device. See *TC51 Touch Computer Integrator Guide for Android Version 6.0.1* for details.

1. Insert the TC51 into a slot to begin charging.
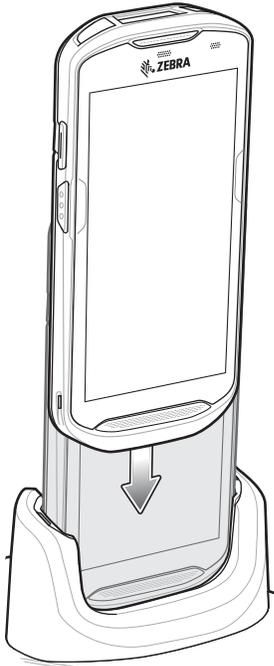
Figure 2-5   *TC51 Battery Charging*

Power LED
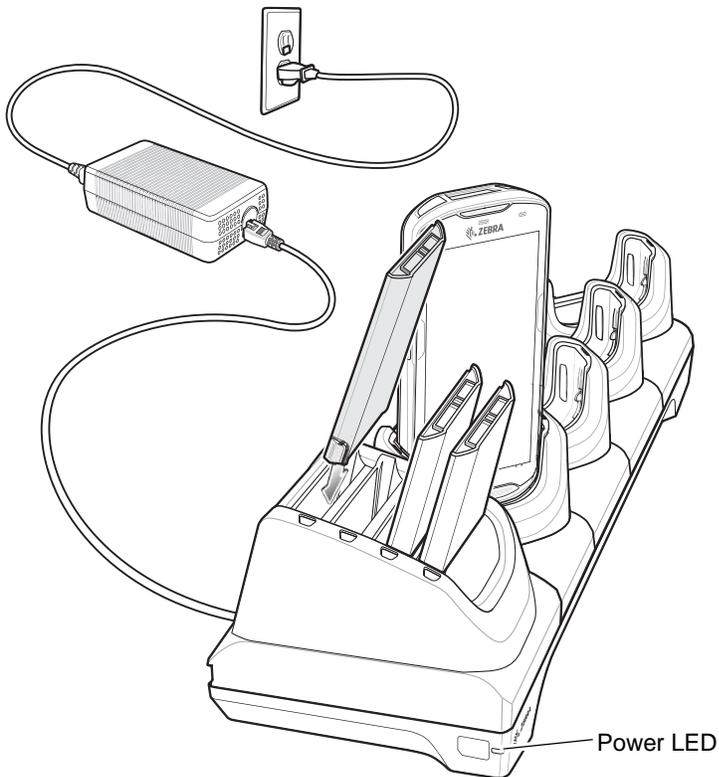
Figure 2-6   *Spare Battery Charging*

2.   Ensure the TC51 is seated properly.

✓ See the *TC51 Touch Computer Integrator Guide for Android Version 6.0.1 for Android Version 6.0.1* for information on installing the 4-Slot Battery Charger onto the cradle.

Inserting a TC51 with Rugged Boot into Cradle

Each cradle cup has an insert that must be removed prior to inserting the TC51 with Rugged Boot. Remove the insert and then insert the TC51 into the cup.
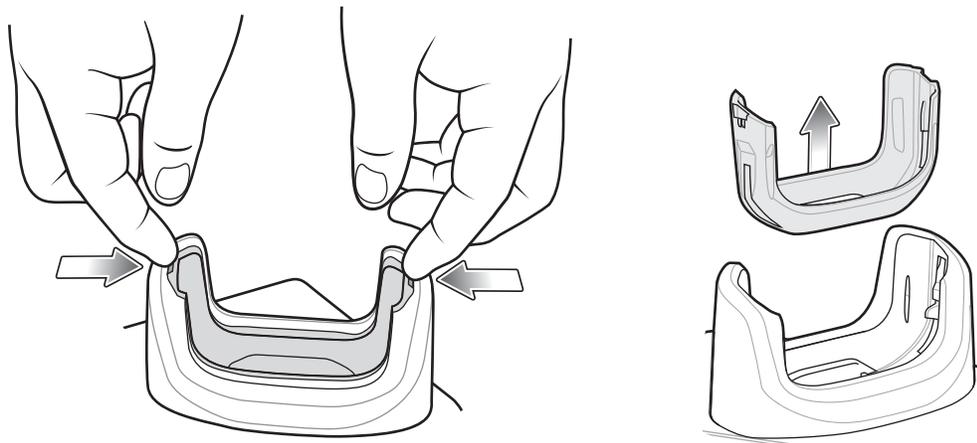
Figure 2-7 *Remove Insert from Cup*

Battery Charging

Main Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See *Table 1-1 on page 1-5* for device charging status. The 4,300 mAh battery fully charges in less than six hours at room temperature.

Spare Battery Charging

The Spare battery Charging LED on the cup indicates the status of the spare battery charging. The 4,300 mAh battery fully charges in less than six hours at room temperature.

Charging Temperature

Table 2-2 *Spare Battery LED Charging Indicators*

LED	LED	Indication
Solid amber		Spare battery is charging.
Solid amber with alternate bright amber		Best spare battery is charging.
Solid Green		Spare battery charging is complete.
Solid Green with alternate bright green		Best spare battery charging is complete.
Solid Red		Spare battery is charging and battery is at the end of useful life. Charging complete and battery is at the end of useful life.
Fast Blinking Red (2 blinks/second)		Error in charging; check placement of spare battery and battery is at the end of useful life.
Off		No spare battery in slot; spare battery not placed correctly; cradle is not powered.

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

5-Slot Charge Only Cradle

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-2*.

The 5-Slot Charge Only Cradle:

- Provides 5 VDC power for operating the TC51.
- Simultaneously charges up to five TC51s.
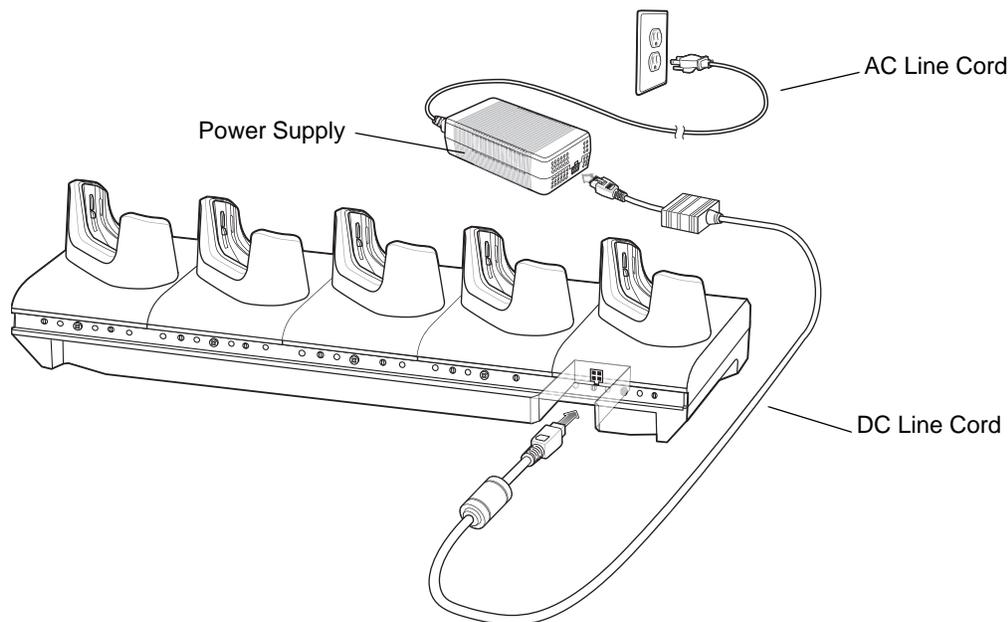
Figure 2-8   *5-Slot Charge Only Cradle Setup*

Charging the TC51

To charge a device:

✓ **NOTE** If the device has a Rugged Boot, remove the cup insert before inserting the device. See *TC51 Touch Computer Integrator Guide for Android Version 6.0.1* for details.

1. Insert the TC51 into a slot to begin charging.
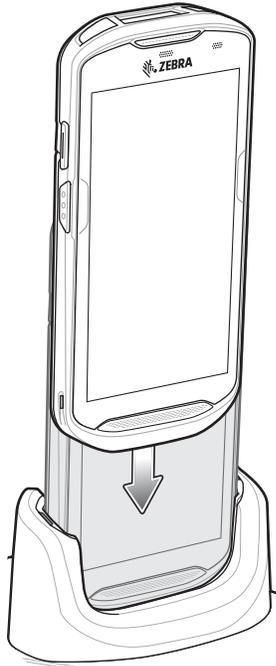
Figure 2-9 *TC51 Battery Charging*

2. Ensure the TC51 is seated properly.

✓ See the *TC51 Touch Computer Integrator Guide for Android Version 6.0.1* for information on installing the 4-Slot Battery Charger onto the cradle.

Inserting a TC51 with Rugged Boot into Cradle

Each cradle cup has an insert that must be removed prior to inserting the TC51 with Rugged Boot. Remove the insert and then insert the TC51 into the cup.
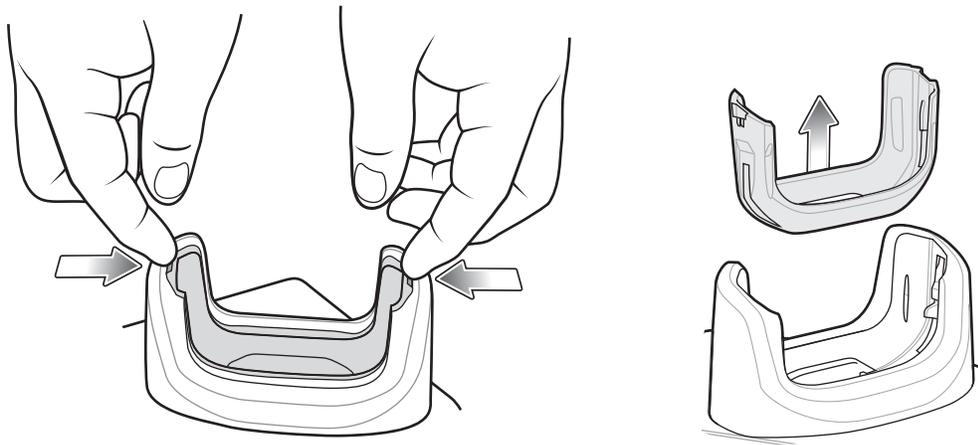
Figure 2-10 *Remove Insert from Cup*

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See *Table 1-1 on page 1-5* for device charging status. The 4,300 mAh battery fully charges in less than six hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

5-Slot Ethernet Cradle

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-2*.

The 5-Slot Ethernet Cradle:

- Provides 5.0 VDC power for operating the device.
- Connects the device (up to five) to an Ethernet network.
- Simultaneously charges up to five TC51s.

Connect the 5-Slot Ethernet cradle to a power source.

Primary Port
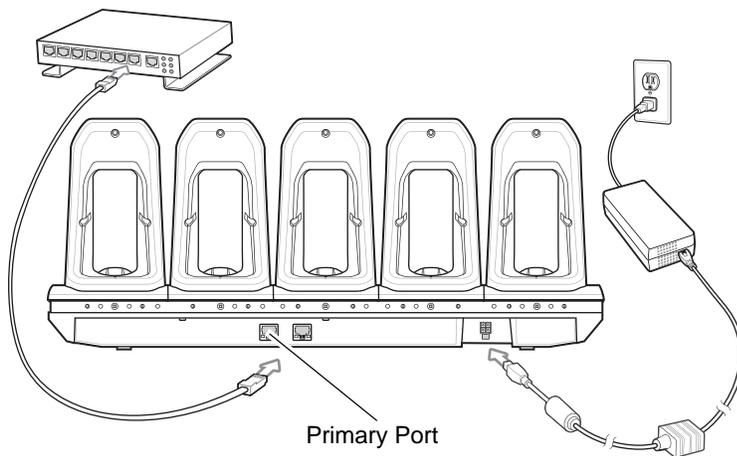
Figure 2-11   *5-Slot Ethernet Cradle Setup*

Daisy-chaining Ethernet Cradles

Daisy-chain up to ten 5-Slot Ethernet cradles to connect several cradles to an Ethernet network. Use either a straight or crossover cable. Daisy-chaining should not be attempted when the main Ethernet connection to the first cradle is 10 Mbps as throughput issues will almost certainly result.

To daisy-chain 5-Slot Ethernet cradles:

1. Connect power to each 5-Slot Ethernet cradle.
2. Connect an Ethernet cable to one of the ports on the switch and the other end to the to Primary Port of the first cradle.
3. Connect an Ethernet cable to the Secondary port of the first cradle.
4. Connect the other end of the Ethernet cable to the Primary port of the next 5-Slot Ethernet cradle.
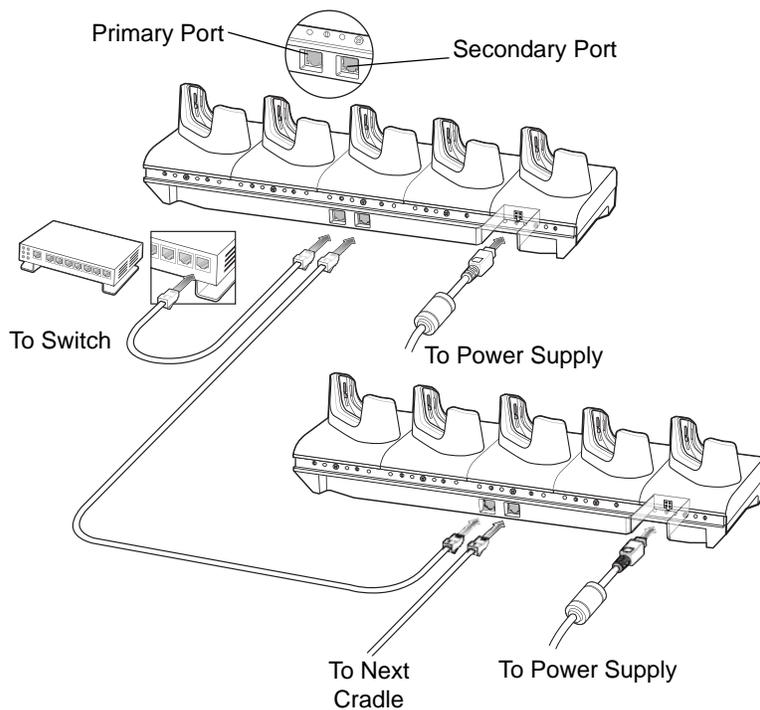
Figure 2-12 *Daisy-chaining 5-Slot Ethernet Cradles*

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

Ethernet Settings

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The TC51 includes Ethernet cradle drivers. After inserting the TC51, configure the Ethernet connection:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ⟨·⟩ **Ethernet**.

3. Place the TC51 into the Ethernet cradle slot.

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

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

6. Touch **Modify Proxy**.

7. Touch the **Proxy** drop-down list and select **Manual**.
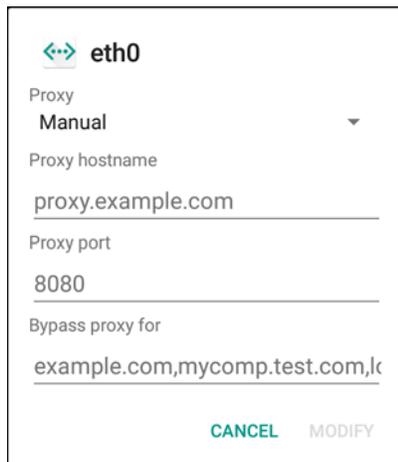
Figure 2-13 *Ethernet Proxy Settings*

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

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

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

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

11. Touch **MODIFY**.

12. Touch ◯.

Configuring Ethernet Static IP Address

The TC51 includes Ethernet cradle drivers. After inserting the TC51, configure the Ethernet connection:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ⟨⋯⟩ **Ethernet**.

3. Place the TC51 into the Ethernet cradle slot.

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

5. Touch **Eth0**.

6. Touch **Disconnect**.

7. Touch **Eth0**.

8. Touch and hold the IP settings drop-down list and select **Static**.

Figure 2-14   *Static IP Settings*

9.   In the **IP** address field, enter the proxy server address.

10. If required, in the **Gateway** field, enter a gateway address for the device.

11. If required, in the **Netmask** field, enter the network mask address

12. If required, in the **DNS** address fields, enter a Domain Name System (DNS) addresses.

13. Touch **CONNECT**.

14. Touch ◯.

Charging the TC51

To charge a device:

NOTE If the device has a Rugged Boot, remove the cup insert before inserting the device. See *TC51 Touch Computer Integrator Guide for Android Version 6.0.1* for details.

1.   Insert the TC51 into a slot to begin charging.
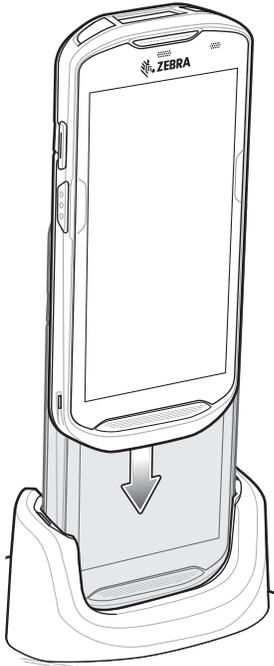
Figure 2-15   *TC51 Battery Charging*

2. Ensure the TC51 is seated properly.

Inserting a TC51 with Rugged Boot into Cradle

Each cradle cup has an insert that must be removed prior to inserting the TC51 with Rugged Boot. Remove the insert and then insert the TC51 into the cup.
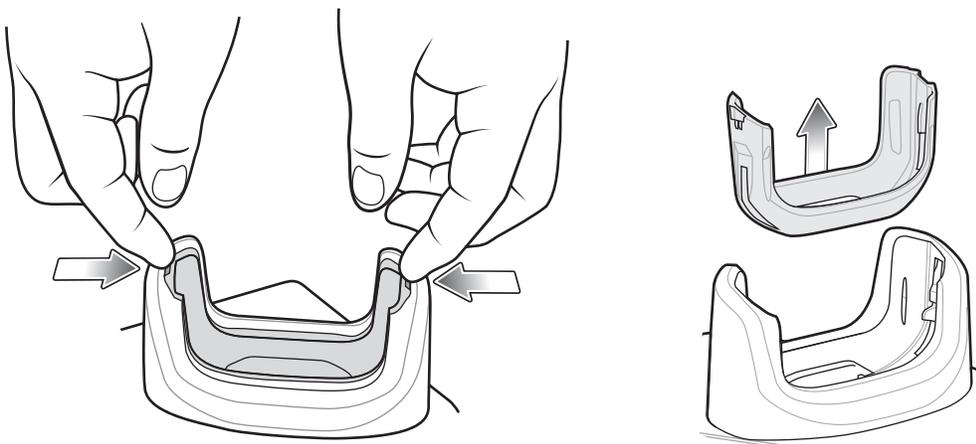
Figure 2-16   *Remove Insert from Cup*

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See *Table 1-1 on page 1-5* for device charging status. The 4,300 mAh battery fully charges in less than six hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

Establishing Ethernet Connection

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.
2. Touch **Ethernet**.
3. Slide the Ethernet switch to the **ON** position.
4. Insert the device into a slot.

   The ⟨⋅⋅⟩ icon appears in the Status bar.
5. Touch **Eth0** to view Ethernet connection details.

LED Indicators

There are two green LEDs on the side of the cradle. These green LEDs light and blink to indicate the data transfer rate.

Table 2-3 *LED Data Rate Indicators*

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

4-Slot Battery Charger

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-2*.

This section describes how to use the 4-Slot Battery Charger to charge up to four TC51 batteries.

Charging Spare Batteries

1. Connect the charger to a power source.
2. Insert the battery into a battery charging well and gently press down on the battery to ensure proper contact.
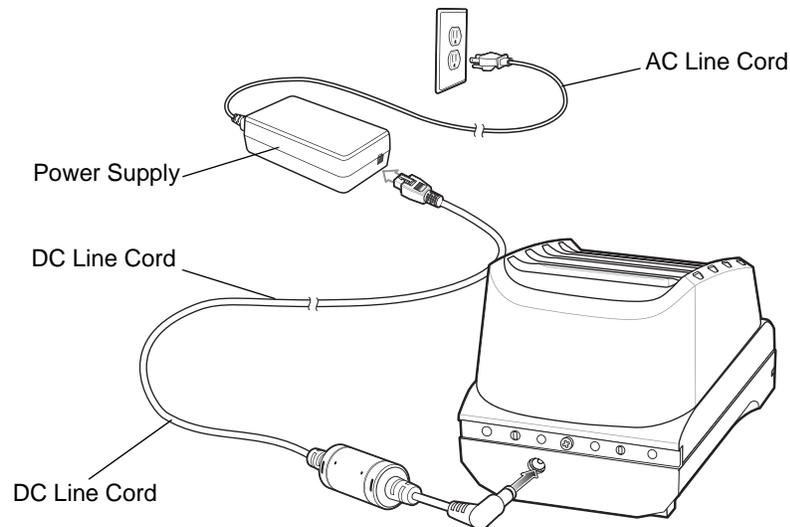
Figure 2-17 *4-Slot Battery Charger Power Setup*

Battery Charging

Spare Battery Charging
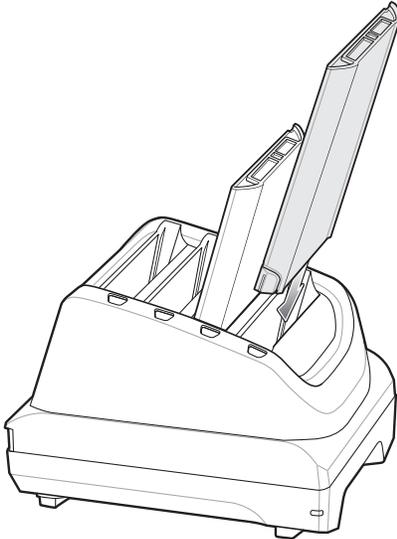
Figure 2-18 *Insert Battery into Charger*

Each Battery Charging LED indicates the status of the battery charging in each slot. See *Table 2-2 on page 2-10* for spare battery charging indicator descriptions.

The 4,300 mAh battery charges to 90% in less than 2.5 hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The battery charger always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the battery charger may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The battery charger indicates when charging is disabled due to abnormal temperatures via its LED.

5-Slot Cradle Rack Installation

Use the Rack/Wall Mount Bracket to mount a 5-slot cradle on a rack. When installing on a rack, first assemble the bracket and cradles/chargers and then install the assembly on the rack.

1. Place the power supply in bottom tray.

2. Connect AC line cord to power supply.

3. Connect DC line cord to power supply.

4. Secure power supply and cables to bottom tray with tie wraps.

✓ *NOTE* Ensure tie wrap buckle is on side of power supply. Tie wrap buckle on top of power supply interferes with top tray.

5. Route cables through cable slots.

DC line Cord   Power Supply   AC line Cord
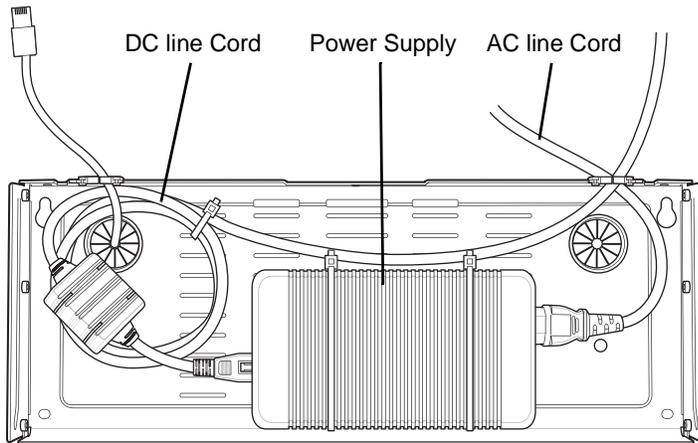
Figure 2-19 *Power Supply in Bottom Tray*

6. Secure four M2.5 studs to top tray as shown.
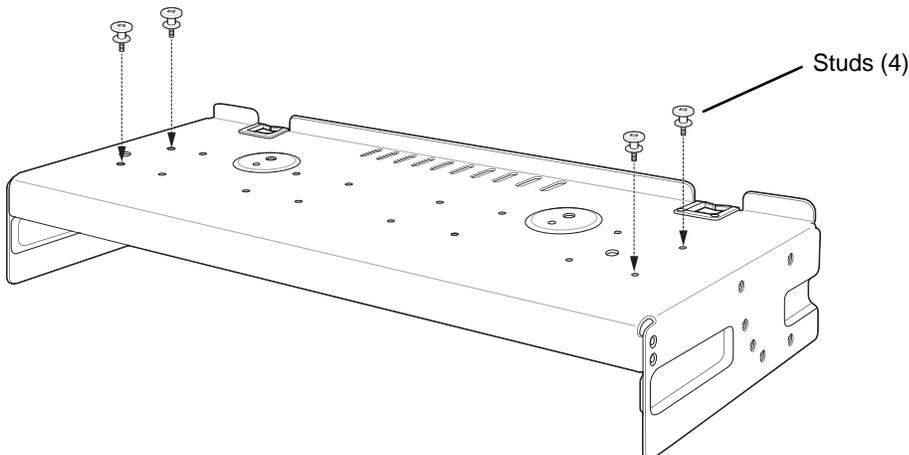
Studs (4)

Figure 2-20 *Install Studs*

7. Align and install 5-Slot cradle onto studs of top tray.
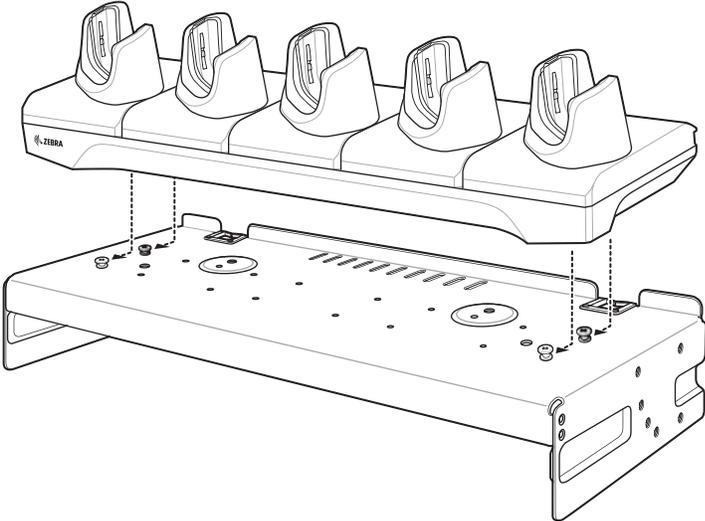
Figure 2-21 *Align Cradle on Studs*

8. Secure cradle to top tray with two M2.5 safety screws.

Safety Screws(2)
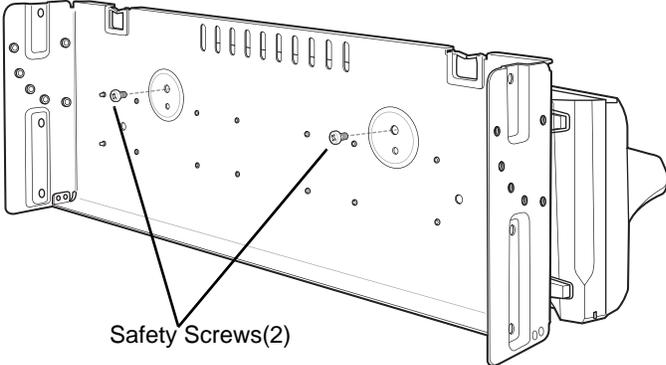
Figure 2-22 *Secure Cradle*

9. Slide top tray onto bottom tray.
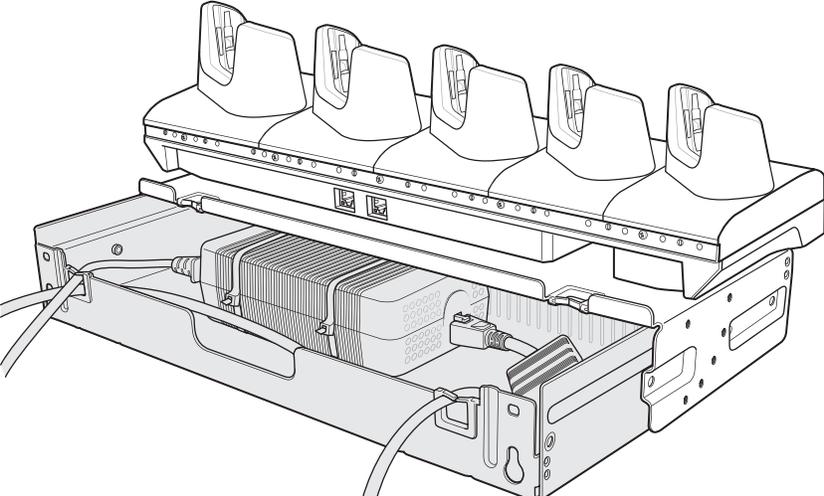
Figure 2-23 *Slide Top Tray onto Bottom Tray*

10. Connect cables to cradle.
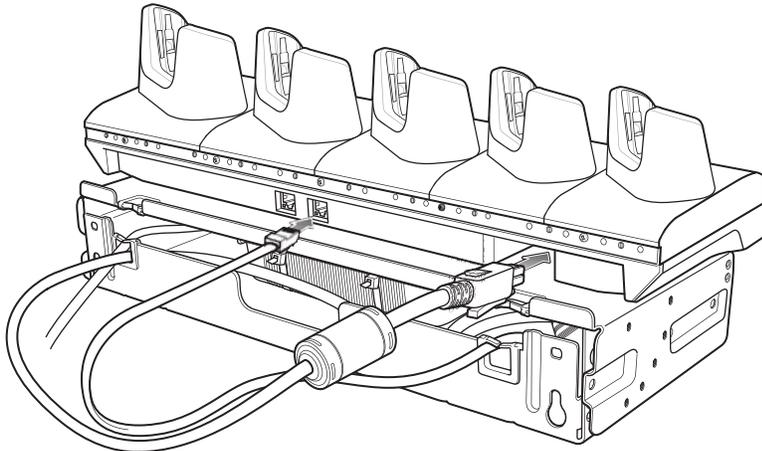
Figure 2-24 *Connect Cables*

11. Secure top tray to bottom tray with 4 M5 screws (two on each side).
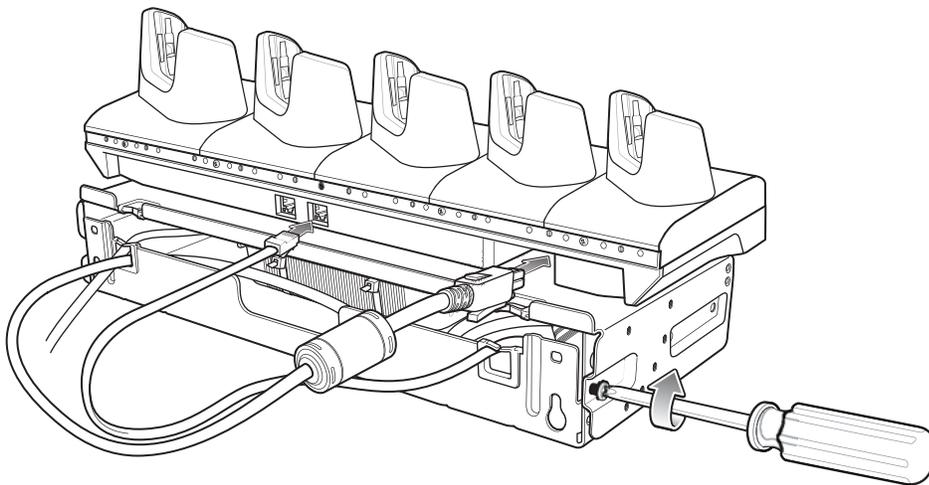
Figure 2-25 *Secure Top and Bottom Tray*

See *Rack Mount Installation on page 2-28* for installing the bracket assembly onto a rack.

4-Slot Battery Chargers Rack Installation

Use the Rack/Wall Mount Bracket to mount four 4-Slot Battery Chargers on a rack. When installing on a rack, first assemble the bracket and chargers and then install the assembly on the rack.

1. Place one power supply horizontally in bottom tray.

2. Place one power supply vertically in bottom tray.

3. Connect AC line cords to power supplies.

4. Connect DC line cords to power supplies.

5. Secure power supplies and cables to bottom tray with tie wraps.

6. Route cables through cable slots.
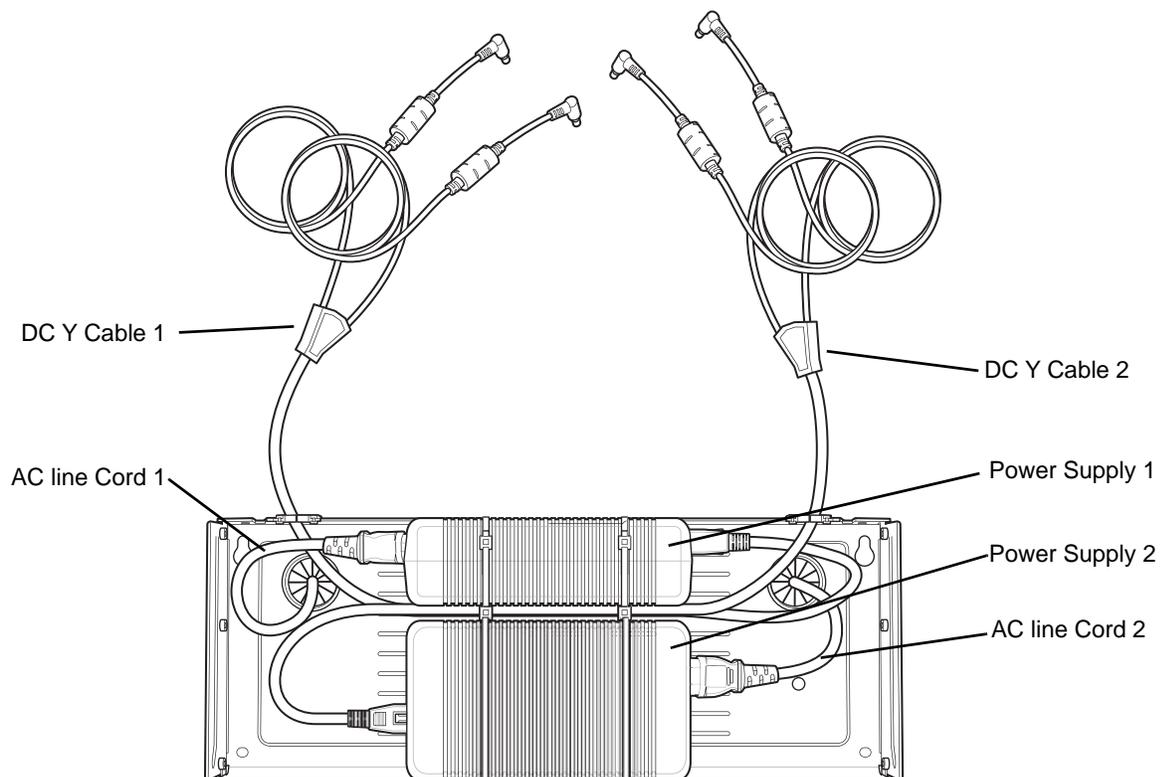
Figure 2-26   *Power Supplies in Bottom Tray*

7. Slide top tray onto bottom tray until top tray touches vertical power supply.
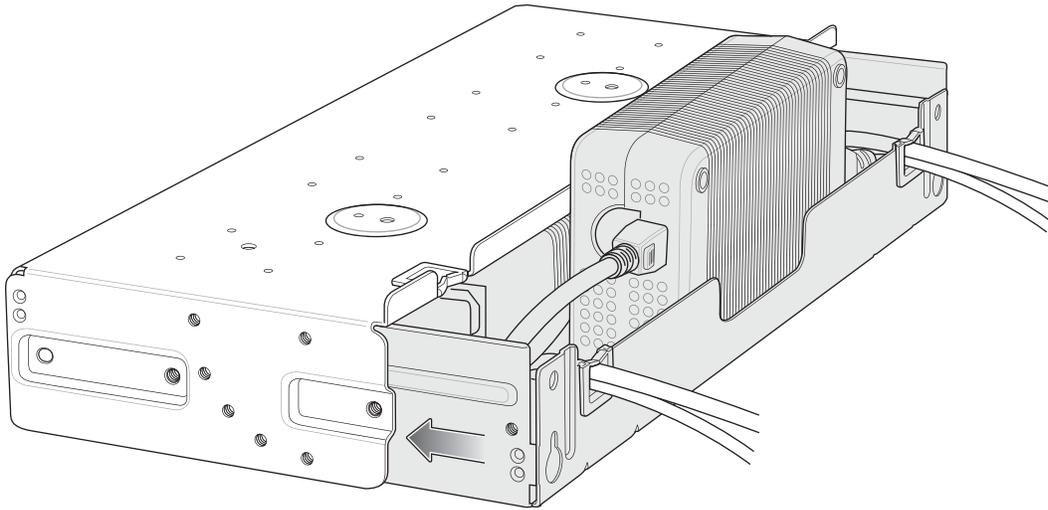
Figure 2-27   *Slide top Tray onto Bottom Tray*

8. Install 16 M2.5 studs onto top tray as shown below.
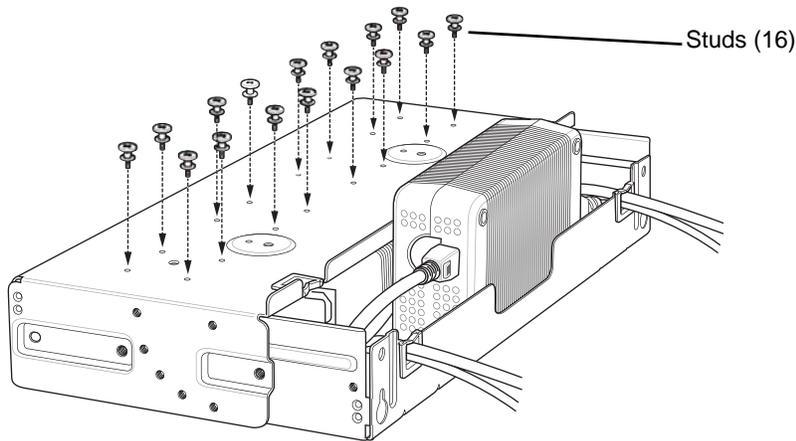
Figure 2-28   *Install Studs*

9. Align and install 4-Slot Battery Charger onto four studs.
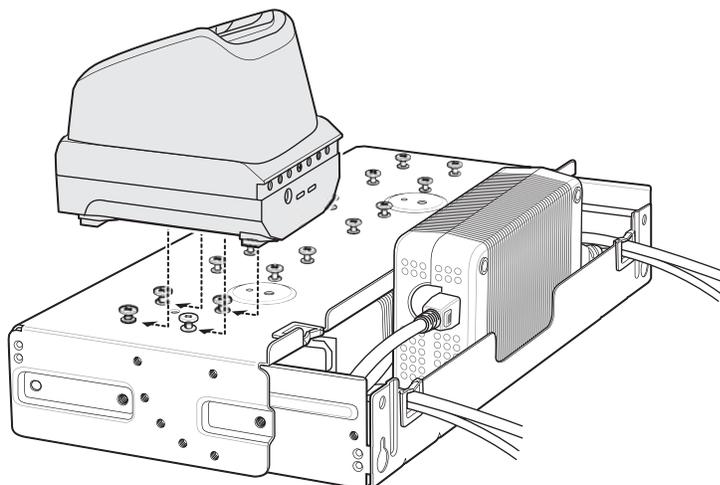
Figure 2-29   *Align Chargers on Studs*

10. Connect DC Y cables to four 4-Slot Battery Chargers.
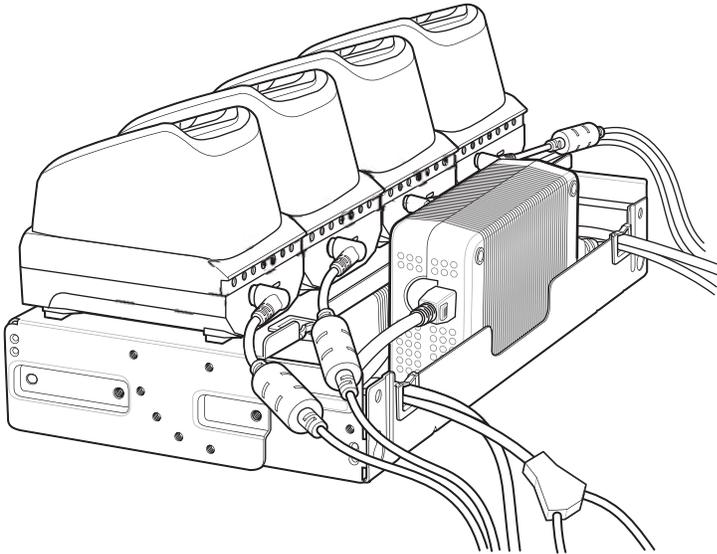
Figure 2-30 *Connect Cables*

11. Secure top tray to bottom tray with four M5 screws (two on each side).
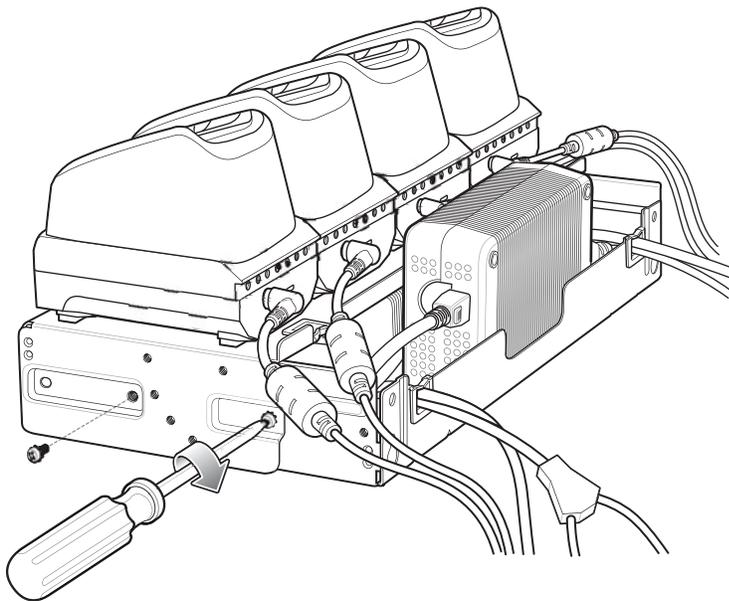
Figure 2-31 *Secure Top Tray to Bottom Tray*

See *Rack Mount Installation on page 2-28* for installing the bracket onto a rack.

Rack Mount Installation

✓ *NOTE* Use screws provided with rack system. Refer to rack user documentation for instructions.

1. Secure mounting brackets to both sides of top tray with four M5 screws (two on each side). For 5-Slot cradles, position the flange for horizontal installation. For 4-Slot Battery Chargers, position the flange for 25° installation.

Flange

Fifth Screw Hole
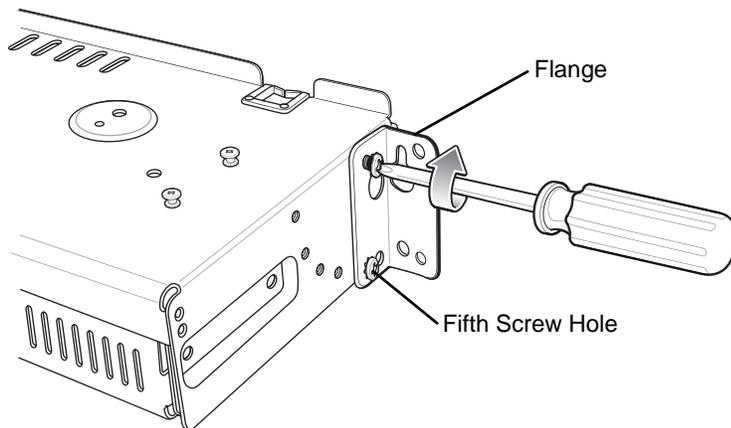
Figure 2-32 *Flange Horizontal Position (5-Slot Cradles)*

Top Screw Hole
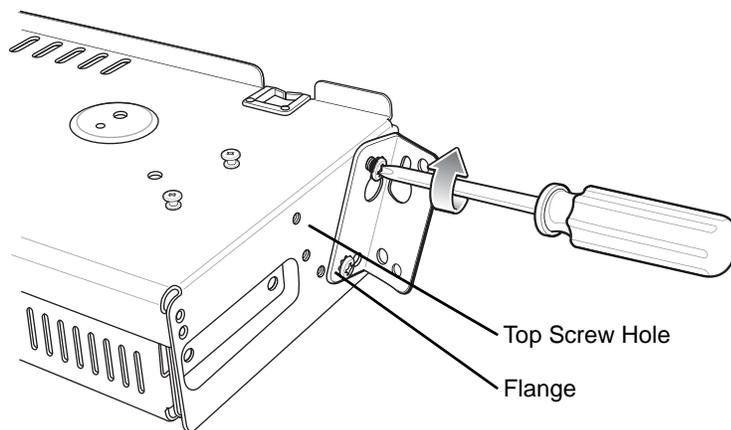
Flange

Figure 2-33 *Flange 25° Position (4-Slot Battery Chargers)*

⚠ *CAUTION* Install mounting bracket with 5-Slot cradle at a maximum height of four feet from ground.

Install mounting bracket with 4-Slot Battery Charger at a maximum height of three feet from ground.

✓ *NOTE* Distance between two horizontal mounted brackets should be at least 14" apart (from top of one flange to the top of the next flange).

Distance between a horizontal mounted bracket and a 25° mounted bracket should be at least 16.25" apart (from top of one flange to the top of the next flange).

There should be enough clearance (2.75") between the top of the device and the bottom of the mounting bracket above.

1. Install two rack system screws for top of mounting brackets. The screw heads should protrude half way from the rail.
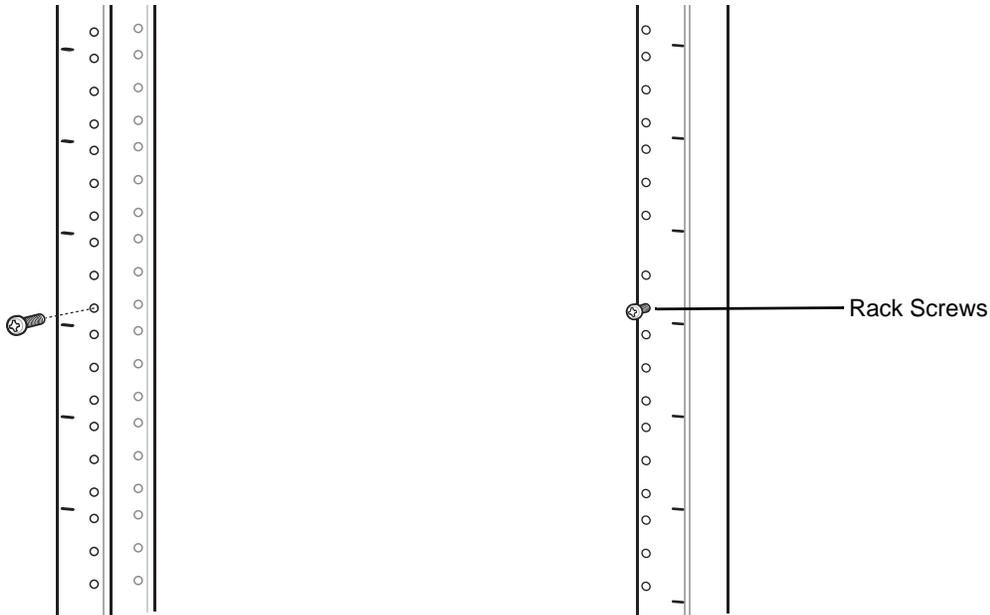
Figure 2-34   *Install Rack System Screws*

2. Align the mounting bracket's top mounting key holes with the screws.

3. Place the brackets on the screws.
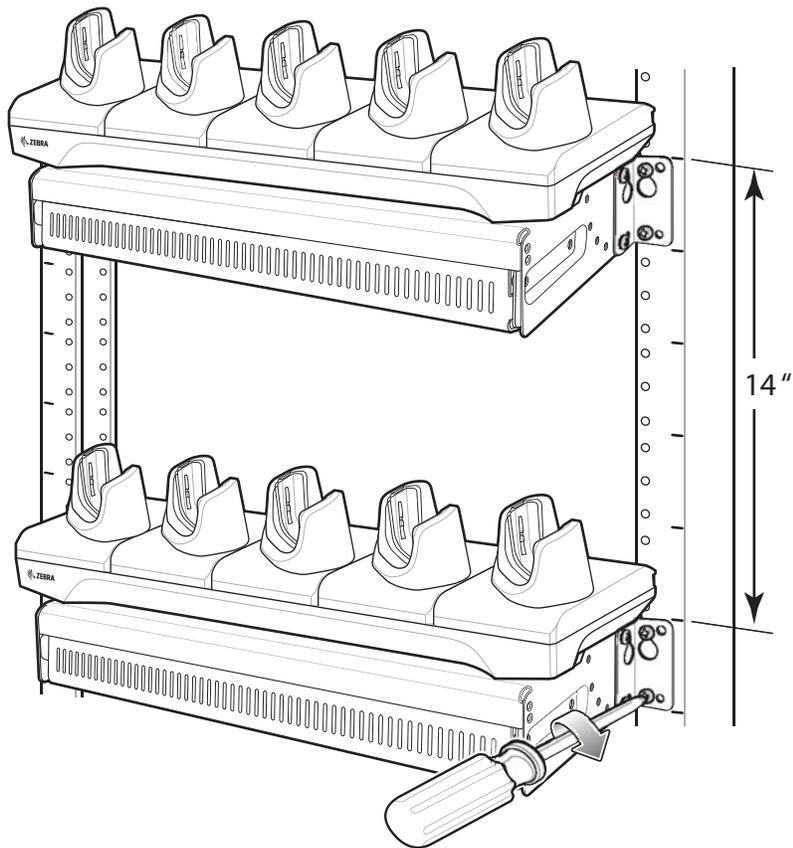
Figure 2-35 *Secure Bracket to Rack (Horizontal Position Shown)*

4. Secure the top screws.

5. Install bottom screws and tighten screws.

6. Route cables and connect to power source.

> ⚠️ **CAUTION** Installer should ensure that all building codes are followed when connecting the power supplies to an AC power source.

While installing the brackets, power supplies and cables:

- Use tie wraps to secure cables to the bracket and rails.

- Coil cables wherever possible.

- Route power cables along the rails.

- Route inter-cradle cables to the side rails and then from the rails to the bracket.

Wall Installation

Use the Rack/Wall Mount Bracket to mount four 4-Slot Battery Chargers or a cradle on a wall. When installing on a wall, first assemble the bottom tray, install the bottom tray on the wall and then assemble the top tray.

Use mounting hardware (screws and/or anchors) appropriate for the type of wall mounting the bracket onto. The Mount Bracket mounting slots dimensions are 5 mm (0.2 in.). Fasteners must be able to hold a minimum of 20 Kg (44 lbs.)

For proper installation consult a professional installer. Failure to install the bracket properly can possibly result in damage to the hardware.

> ⚠️ **CAUTION** Install mounting bracket with 5-Slot cradle at a maximum height of four feet from ground.
>
> Install mounting bracket with 4-Slot Battery Charger at a maximum height of three feet from ground.

Bottom Tray Assembly

Bracket Wall Mounting

1. Drill holes and install anchors according to the template supplied with the bracket.
2. Install two screws for bottom of bracket. The screw heads should protrude 2.5 mm (0.01") from the wall.
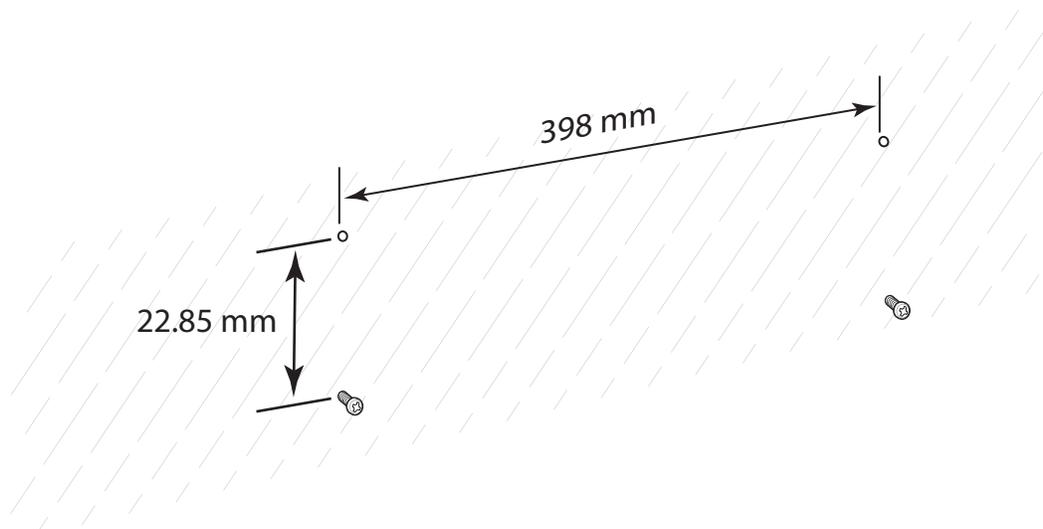
Figure 2-36 *Horizontal Mounting Template*

3. Align the mounting bracket's bottom mounting key holes with the screws.
4. Hang the bracket on the screws.
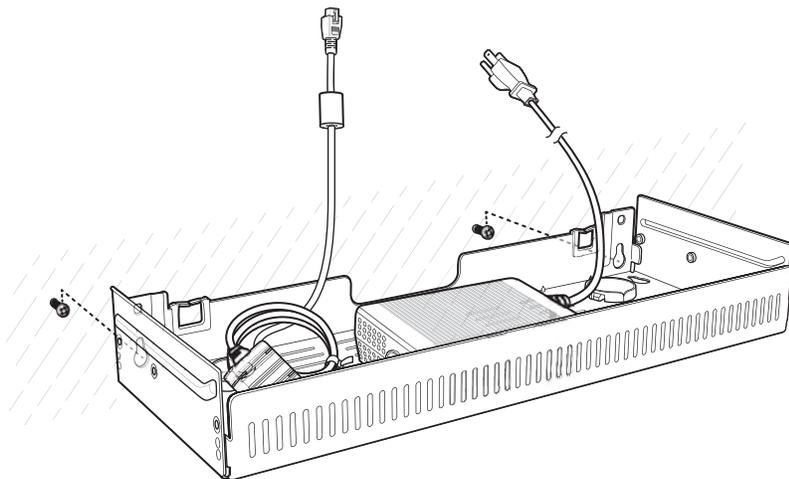
Figure 2-37 *Horizontal Installation*

5. Install two top screws.
6. Tighten all screws.
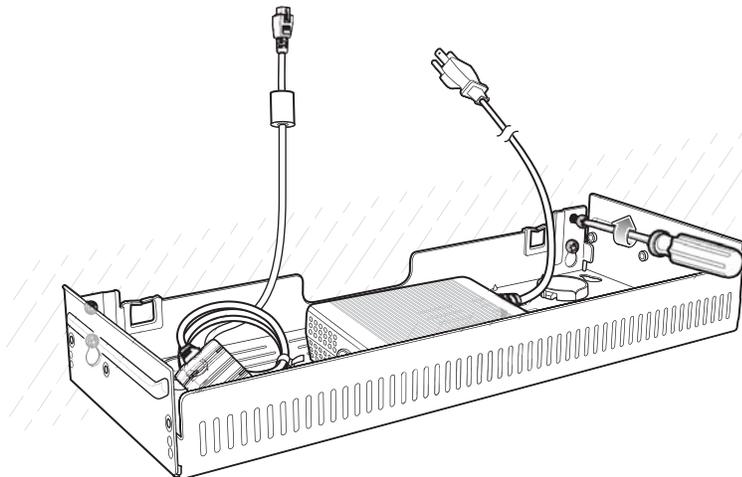
Figure 2-38 *Horizontal Installation - Tighten Screws*

7. Assembly the four 4-Slot Battery Chargers or cradle onto the bracket. See steps 7 through 11 on page 25.
8. Route cables and connect to power source.

⚠️ *CAUTION* Installer should ensure that all building codes are followed when connecting the power supplies to an AC power source.

While installing the brackets, power supplies and cables:

- Use tie wraps to secure cables to the bracket and rails.
- Coil cables wherever possible.
- Route power cables along the rails.
- Route inter-cradle cables to the side rails and then from the rails to the bracket.

CHAPTER 3 DATAWEDGE

Introduction

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

Basic Scanning

To capture bar code data:

1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Aim the exit window at a bar code.
3. Press and hold the a Scan button. The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern. The Data Capture LED lights red to indicate that data capture is in process.
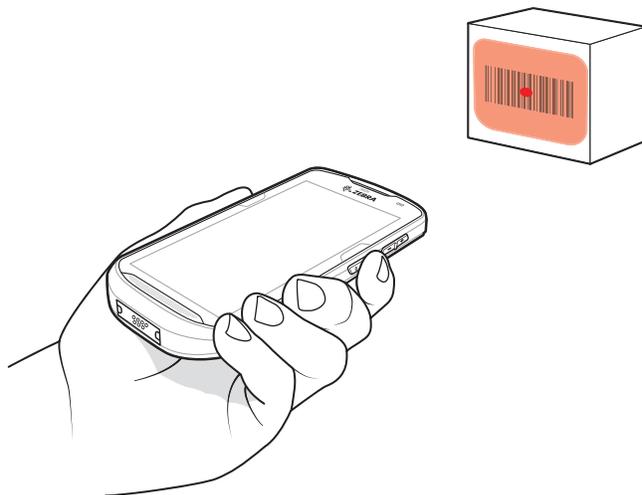
Figure 3-1   *TC51 Data Capture*

4.   The Data Capture LED lights green, a beep sounds and the device vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

Profiles

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

Profile information consists of:

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

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

DataWedge includes the following 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** - enables scanning when the Launcher is in foreground. Note: to save battery power, disable this profile when not required.
  - **DWDemo** - provides support for the DWDemo application.

Some Zebra applications are capable of capturing data by scanning. DataWedge is pre-loaded with private and hidden profiles for this purpose. There is no option to modify these private profiles.

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 ⊞ > ⥾ . By default, three profiles appear:

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

Profile0 is the default profile and is used when no other profile can be applied.
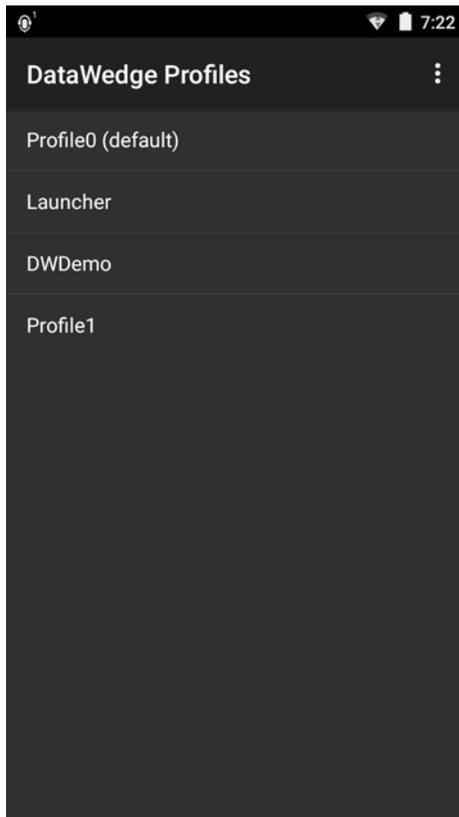
Figure 3-2   *DataWedge Profiles Screen*

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.
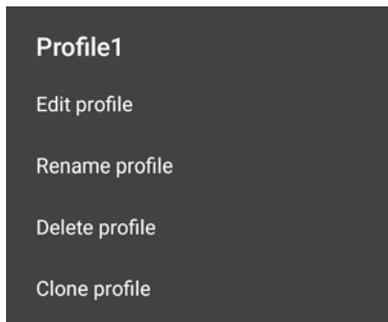
Figure 3-3   *Profile Context Menu*

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

Options Menu
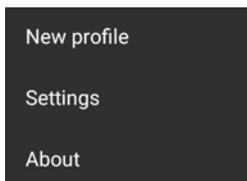
Figure 3-4   *DataWedge Options Menu*

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

Disabling DataWedge

1. Touch ⊞ > ▥ .
2. Touch ⋮ .
3. Touch **Settings**.
4. Touch **DataWedge enabled**.

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

Creating a New Profile

5. Touch ⊞ > ▥ .
6. Touch ⋮ .
7. Touch **New profile**.
8. 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).
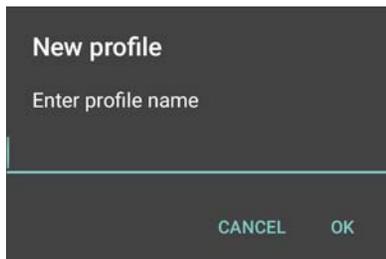
Figure 3-5   *New Profile Name Dialog Box*

9. Touch **OK**.

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

Profile Configuration

To configure the Profile0 or a user-created profile, touch the profile name.
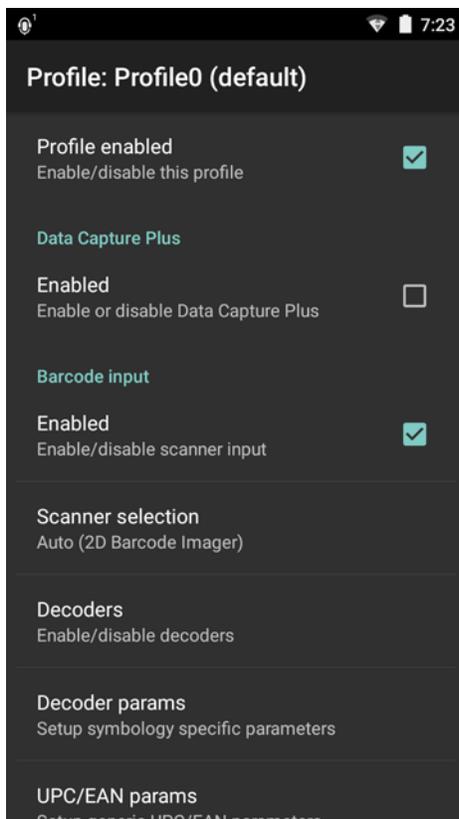
Figure 3-6   *Profile Configuration Screen*

The configuration screen lists the following sections:

- Profile enabled
- Applications
- Data Capture panel (DCP)
- Barcode Input

  • Keystroke output
  • Intent Output
  • IP Output.

Associating Applications

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

1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.
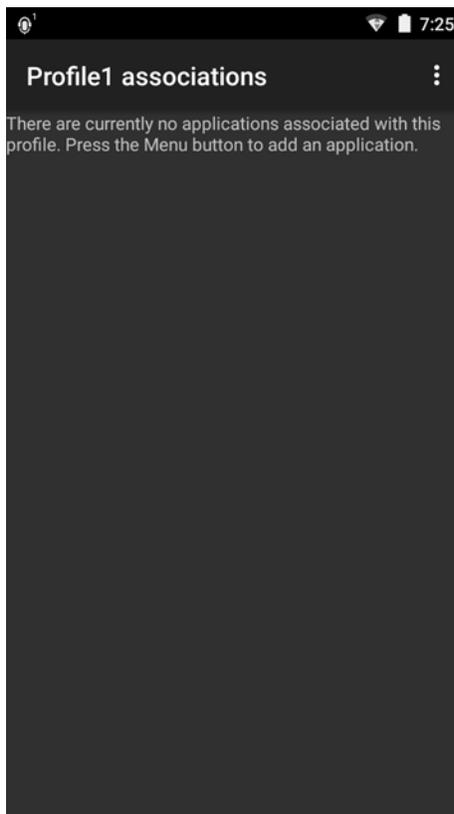
Figure 3-7   *Associated Apps Screen*

2. Touch ⋮ .
3. Touch **New app/activity**.
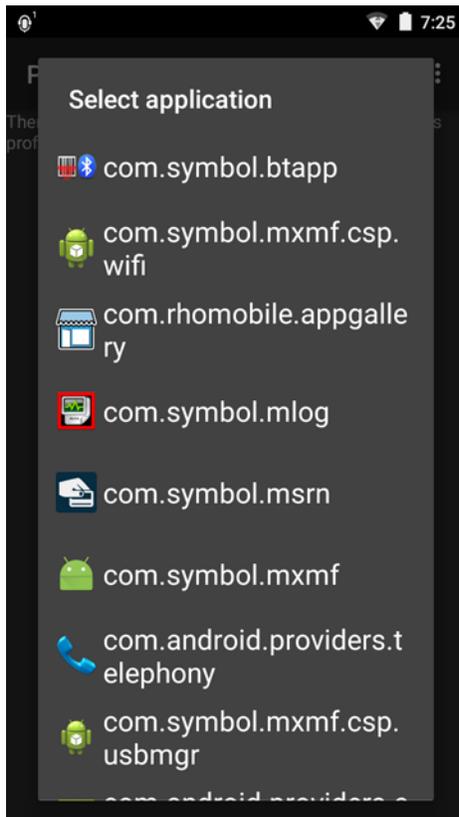
Figure 3-8   *Select Application Menu*

4. In the **Select application** screen, select the desired application from the list.

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

6. Touch ◁ .
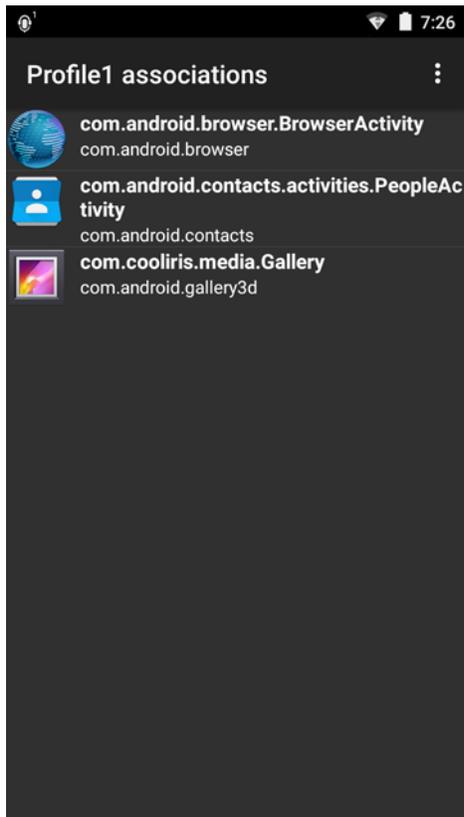
Figure 3-9   *Selected Application/Activity*

Data Capture Plus

Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching a designated part of the screen. A variable screen overlay acts like a scan button.

DCP Button
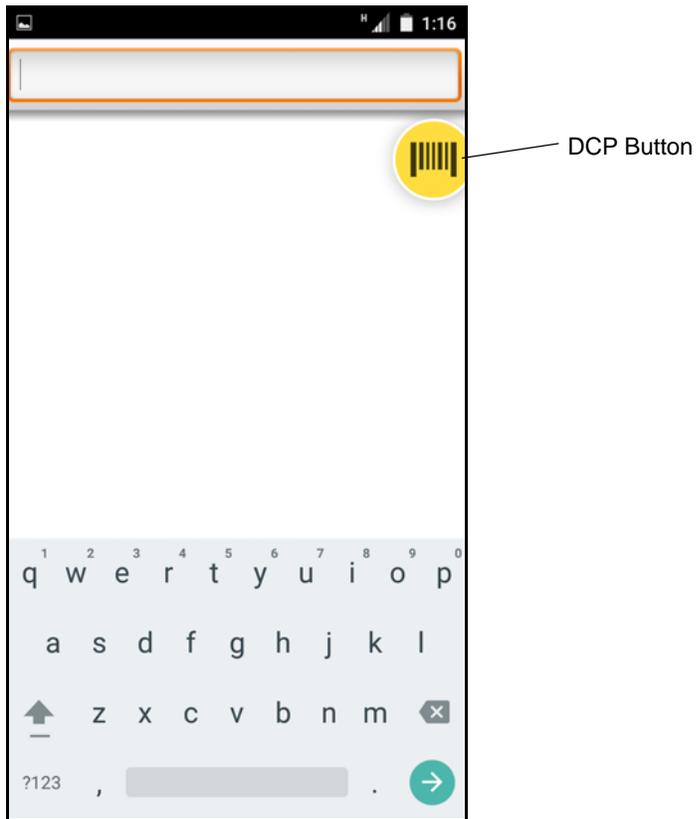
Figure 3-10   *Minimized Data Capture Panel*

The DataWedge profile configuration screen allows the user to configure how the DCP appears on the screen once the particular profile is enabled. The DCP is hidden by default. Enabling DCP option displays seven additional configuration parameters.
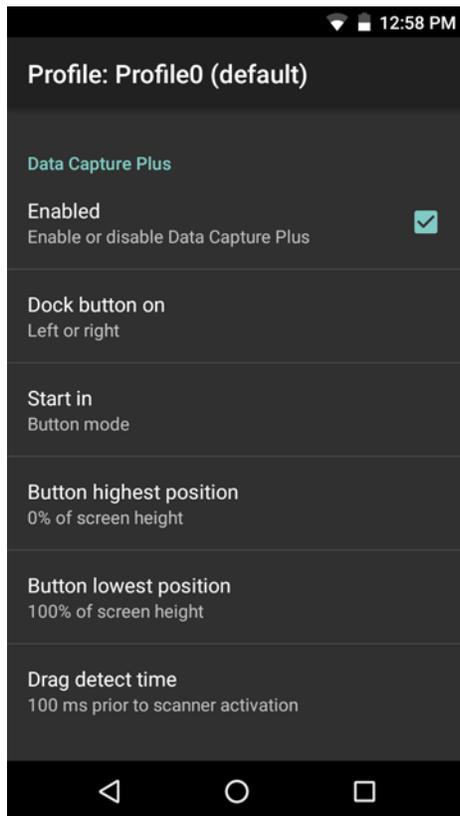
Figure 3-11 *Data Capture Panel Settings*

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

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

In Button mode, the user can place DCP in full screen mode by dragging the button over **Fullscreen mode**. The overlay covers the screen.
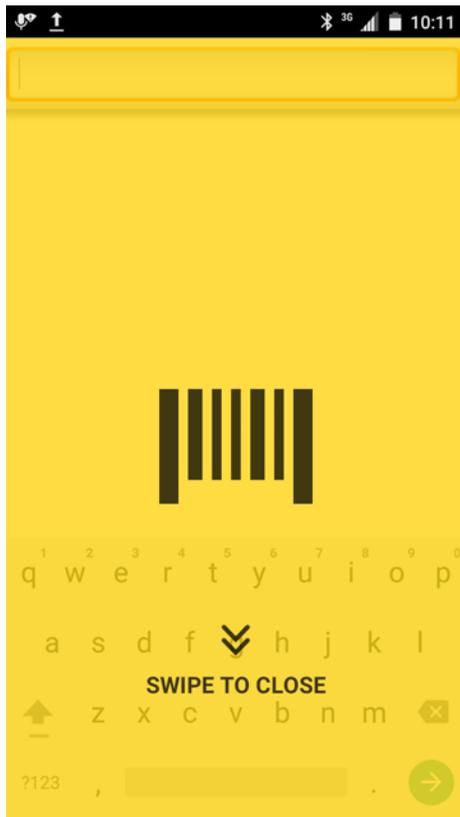
Figure 3-12   *Maximized DCP*

Swipe down to return to button mode.

Bar Code Input

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

Enabled

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

Scanner Selection

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

- **Auto** - The software automatically determines the best scanning device.
- **2D Barcode Imager** - Scanning is performed using the 2D Imager.
- **Bluetooth Scanner** - Scanning is performed using the option Bluetooth scanner.

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:

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

Table 3-1 *Supported Decoders*

Decoders	Imager	RS507
Australian Postal	Disabled	Disabled
Aztec	Enabled	Enabled
Canadian Postal	Disabled	Not supported
Chinese 2 of 5	Disabled	Disabled
Codabar	Enabled	Enabled
Code 11	Disabled	Disabled
Code 128	Enabled	Enabled
Code 39	Enabled	Enabled
Code 93	Disabled	Disabled
Composite AB	Disabled	Disabled
Composite C	Disabled	Disabled
Discrete 2 of 5	Disabled	Disabled
Datamatrix	Enabled	Enabled
Dutch Postal	Disabled	Disabled
EAN-13	Enabled	Enabled
EAN-8	Enabled	Enabled
GS1 DataBar	Enabled	Enabled
GS1 DataBar Expanded	Enabled	Enabled
GS1 DataBar Limited	Disabled	Disabled
HAN XIN	Disabled	Not supported
Interleaved 2 of 5	Disabled	Disabled
Japanese Postal	Disabled	Disabled
Korean 3 of 5	Disabled	Disabled
MAIL MARK	Enabled	Not supported
Matrix 2 of 5	Disabled	Disabled

Table 3-1 *Supported Decoders (Continued)*

Decoders	Imager	RS507
Maxicode	Enabled	Enabled
MicroPDF	Disabled	Disabled
MicroQR	Disabled	Disabled
MSI	Disabled	Disabled
PDF417	Enabled	Enabled
QR Code	Enabled	Enabled
Decoder Signature	Disabled	Disabled
TLC 39	Disabled	Disabled
Trioptic 39	Disabled	Disabled
UK Postal	Disabled	Disabled
UPC-A	Enabled	Enabled
UPC-E0	Enabled	Enabled
UPC-E1	Disabled	Disabled
US4state	Disabled	Disabled
US4state FICS	Disabled	Disabled
US Planet	Disabled	Disabled
US Postnet	Disabled	Disabled

Touch ◁ to return to the previous screen.

Decoder Params

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

Codabar

- **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 3-20* for more information.
- **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

Code 11

- **Length1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).
- **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code.
    - **No Check Digit** - Do not verify check digit.
    - **1 Check Digit** - Bar code contains one check digit (default).
    - **2 Check Digits** - Bar code contains two check digits.

Code128

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 bar codes (Imager only).
- **Ignore Code128 FCN4** - When enabled, and a Code 128 bar code has an embedded FNC4 character, it will be removed from the data and the following characters will not be changed. When the feature is disabled, the FNC4 character will not be transmitted but the following character will have 128 added to it (Imager only).
- **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:
    - **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
    - **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
    - **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 3-20* for more information.
- **Length2**- Use to set decode lengths (default - 55). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

- **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.
  - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
  - **Security Level 1** - This setting eliminates most misdecodes (default).
  - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
  - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.

Code39

- **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 bar codes (imager only).
- **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
- **Full ASCII**- Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled),
- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
- **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character "A" to all Code 32 bar codes (default - disabled).
- **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).
  - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
  - **Security Level 1** - This setting eliminates most misdecodes (default).
  - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
  - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.
- **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).

Code93

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

Composite AB

- **UCC Link Mode**
  - **Link Flag ignored** - 1D component is transmitted regardless of whether a 2D component is detected.
  - **Always Linked** - 1D and the 2D components are transmitted. If 2D is not present, the 1D component is not transmitted.
  - **Auto Discriminate** - the digital scanner determines if there is a 2D portion, then transmits the 1D component, as well as the 2D portion if present. (default).

Discrete 2 of 5

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

GS1 DataBar Limited

- **GS1 Limited Security Level**
  - **GS1 Security Level 1** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
  - **GS1 Security Level 2** - This setting eliminates most misdecodes (default).
  - **GS1 Security Level 3** - Select this option if Security level 2 fails to eliminate misdecodes.
  - **GS1 Security Level 4** - If Security Level 3 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.

HAN XIN

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

Interleaved 2 of 5

- **Check Digit**
  - **No Check Digit** - A check digit is not used. (default)
  - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
  - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
- **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).

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

Matrix 2 of 5

- **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 3-20* for more information.
- **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
- **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).

MSI

- **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
  - **One Check Digit** - Verify one check digit (default).
  - **Two Check Digits** - Verify two check digits.
- **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
  - **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
  - **Mod-10-10** - Both check digits are MOD 10.
- **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 3-20* for more information.
- **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 3-20* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).

Trioptic 39

- **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) (RS507 only).

UK Postal

- **Report Check Digit** - Transmit UK Postal data with or without the check digit. A check in the checkbox indicates to send UK Postal data with check digit (default - disabled).

UPCA

- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

    There are three options for transmitting a UPCA preamble:

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

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - enabled).

UPCE0

- **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).

- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

    There are three options for transmitting a UPCE0 preamble:

  - **Preamble 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).

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

UPCE1

- **Convert UPCE1 To UPCA** - Enable this to convert UPCE1 decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable this to transmit UPCE1 decoded data as UPCE1 data, without conversion (default - disabled).

- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

    There are three options for transmitting a UPCE1 preamble:

  - **Preamble 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).

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

US Planet

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

Decode Lengths

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

UPC EAN Params

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

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC bar codes (Imager only).
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **Bookland Format -** If Bookland EAN is enabled, select one of the following formats for Bookland data:
  - **Format ISBN-10** - The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
  - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled.
- **Coupon Report Mode** - Traditional coupon symbols are composed of two bar code: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded bar code. The new format offers more options for purchase values (up to $999.999) and supports complex discount offers as a second purchase requirement. An interim coupon symbol also exists that contain both types of bar codes: UPC/EAN and Databar Expanded. This format accommodates both retailers that do not recognize or use the additional information included in the new coupon symbol, as well as those who can process new coupon symbols.
  - **Old Coupon Report Mode** - Scanning an old coupon symbol reports both UPC and Code 128, scanning is interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
  - **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
  - **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
- **Ean Zero Extended** – Enable this parameter to add five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols. Disable this to transmit EAN-8 symbols as is. Default – disabled.
- **Linear Decode** - This option applies to code types containing two adjacent blocks (e.g., UPC-A, EAN-8, EAN-13). Enable this parameter to transmit a bar code only when both the left and right blocks are successfully decoded within one laser scan. Enable this option when bar codes are in proximity to each other (RS507 only).

- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).

- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.

  - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding "in-spec" UPC/EAN bar codes (default).

  - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.

  - **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.

  - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.

- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.

- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.

- **Supplemental Mode**

  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).

  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.

  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.

  - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

  - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

  - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

  - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not

starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

- **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN bar code not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

Reader Params

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

- **1D Quiet Zone Level** - Sets the level of aggressiveness in decoding bar codes with a reduced quiet zone (the area in front of and at the end of a bar code), and applies to symbologies enabled by a Reduced Quiet Zone parameter. Because higher levels increase the decoding time and risk of misdecodes, Zebra strongly recommends enabling only the symbologies which require higher quiet zone levels, and leaving Reduced Quiet Zone disabled for all other symbologies (Imager only).

  Options are:
  - **0** - The scanner performs normally in terms of quiet zone.
  - **1** - The scanner performs more aggressively in terms of quiet zone (default).
  - **2** - The scanner only requires one side EB (end of bar code) for decoding.
  - **3** - The scanner decodes anything in terms of quiet zone or end of bar code.
- **Aim mode** - Turns the scanner cross-hairs on or off.
  - **On** - Cross-hair is on (default).
  - **Off** - Cross-hair is off.
- **Character Set Selection**
  - **ISO-88959-1** - part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
  - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
  - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
- **Time Delay to Low Power** - Sets the time the decoder remains active after decoding. After a scan session, the decoder waits this amount of time before entering Low Power Mode. Options: **1 Second** (default), **30 Seconds**, **1 Minute** or **5 Minutes** (RS507 only).
- **Illumination Brightness** - Sets the brightness of the illumination by altering LED power. The default is 10, which is maximum LED brightness. For values from 1 to 10, LED brightness varies from lowest to highest level of brightness (RS507 only).
- **Illumination mode** - Turns imager illumination on and off. This option is only available when **Bluetooth Scanner** is selected in the **Barcode input**, **Scanner selection** option.
  - **On** - Illumination is on (default).
  - **Off** - Illumination is off.
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D bar codes (RS507 only).
  - **Disable** - Disables decoding of inverse 1D bar codes (default).
  - **Enable** - Enables decoding of only inverse 1D bar codes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D bar codes.

- **LCD Mode** - Enables or disables LCD mode. LCD mode enhances the ability of the imager to read bar codes from LCD displays such as cellphones (Imager only).
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.
- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.
  - **Disabled** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Enabled** – Enables Picklist mode so that only the bar code under the projected reticle can be decoded.
- **Poor Quality Decode Effort** - Enable poor quality bar code decoding enhancement feature (Imager only).
- **Aim Timer** - Sets the maximum amount of time that aiming remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the aim to stay on indefinitely (default - 500).
- **Aim Type** - Set the aiming usage.
  - **Trigger** - A trigger event activates decode processing, which continues until the trigger event ends or a valid decode occurs.
  - **Timed Hold** - A trigger pull and hold activates the laser for aiming, which continues until the trigger is released, a valid decode, or the decode session time-out is expired.
  - **Timed Release** - A trigger pull activates the laser for aiming, which continues until a valid decode or the remaining decode session time has expired.
  - **Press and Release** - A trigger pull and release activates the laser for aiming, which continues until a trigger is pressed again, a valid decode, or the decode session time-out is expired.
  - **Continuous Read** - When the imager detects an object in its field of view, it triggers and attempt to decode.
- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -500).
- **Different Symbol Timeout** - Controls the time the scanner is inactive between decoding different symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.
- **Same Symbol Timeout** - Controls the time the scanner is inactive between decoding same symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.

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** - Insert AIM Character prefix.
  - **Code ID Type Symbol** - Insert Symbol character prefix.
- **Engine Decode LED** - Use to turn on scanner red LED when the scan beam is emitting either by scanner trigger or using soft scan button (RS507 only).
- **BT Disconnect On Exit** - Bluetooth connection is disconnected when data capture application is closed (RS507 only).
- **Connection Idle Time** - Set connection idle time. The Bluetooth connection disconnects after being idle for set time (RS507 only).

- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).
- **Display BT Address Barcode** - Enable or disable displaying Bluetooth Address bar code if there is no Bluetooth scanner being paired when application tries to enable the Bluetooth scanner (RS507 only).
- **Establish Connection Time** - The timeout which the device will try to enable or reconnect to the Bluetooth scanner when the Bluetooth scanner is not in the vicinity or not paired (RS507 only).
- **Audio Feedback Mode** - Select good decode audio indication (RS507 only).
  - **Local Audio Feedback** - Good decode audio indication on TC51 only.
  - **Remote Audio Feedback** - Good decode audio indication on RS507 only.
  - **Both** - Good decode audio indication on TC51 and RS507.
  - **Disable** - No good decode audio indication on either TC51 or RS507 (default).
- **LED Feedback Mode** - Select good decode LED indication (RS507 only).
  - **Local LED Feedback** - Good decode LED indication on TC51 only.
  - **Remote LED Feedback** - Good decode LED indication on RS507 only.
  - **Both** - Good decode LED indication on TC51 and RS507 (default).
  - **Disable** - No good decode LED indication on either TC51 or RS507.
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).
- **Decode Feedback LED Timer** - Set the amount of time (in milliseconds) that the green Data Capture LED stays lit after a good decode. (default - 75 msec.)
- **Beep Volume Channel** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.

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

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

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.
- **Multi byte character display** - Set the amount of time (in milliseconds) of the inter character delay for multi byte characters. (default - 0.)
- **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 3-31* for more information.
- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Output

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).

- **Intent delivery** - Select the method by which the intent is delivered:
  - Send via StartActivity
  - Send via startService (default)
  - Broadcast intent
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 3-31* for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Overview

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

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

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

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

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

and the Intent category would be:

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

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

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

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

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

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

IP Output

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

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.
- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 3-31* 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**.
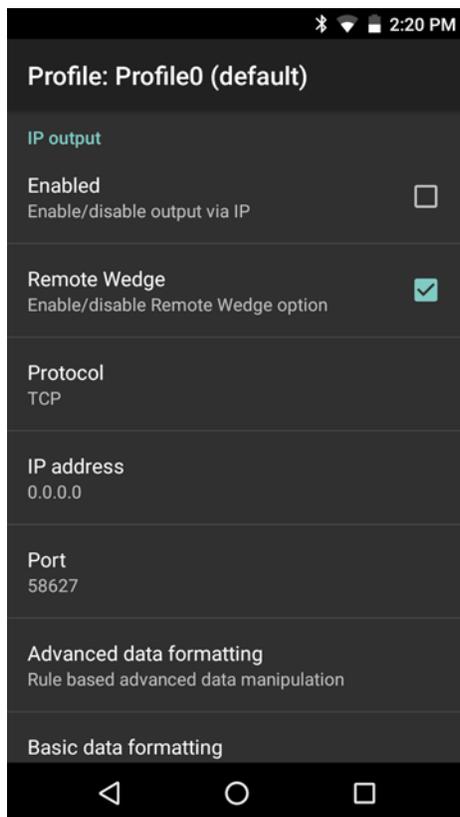
Figure 3-13   *IP Output Screen*

Using IP Output with IPWedge

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

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

    A check appears in the checkbox.

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

3. Touch **Protocol**.

4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).
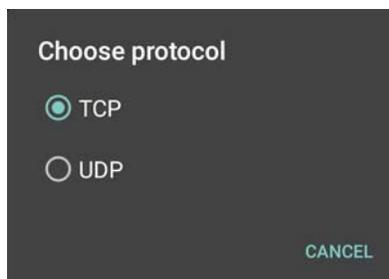
Figure 3-14   *Protocol Selection*

5. Touch **IP Address**.

6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.
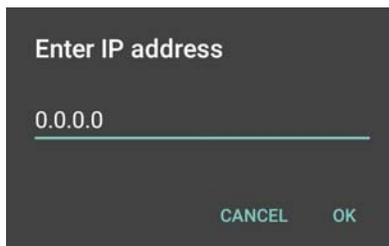
Figure 3-15   *IP Address Entry*

7. Touch **Port**.

8. In the **Enter port number** dialog box, enter same port number selected for IPWedge computer application.
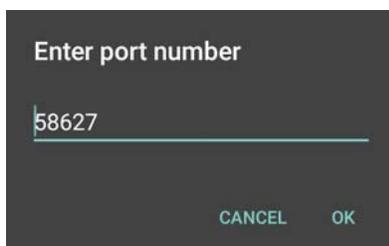
Figure 3-16   *Port Number Entry*

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

Using IP Output without IPWedge

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

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

   A check appears in the checkbox.

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

3. Touch **Protocol**.

4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).
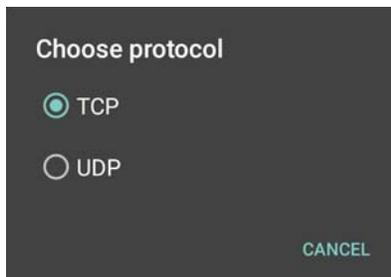
Figure 3-17 *Protocol Selection*

5. Touch **IP Address**.

6. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.
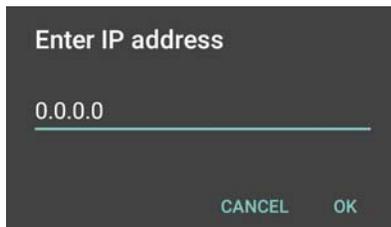
Figure 3-18 *IP Address Entry*

7. Touch **Port**.

8. In the **Enter port number** dialog box, enter the port number that the host computer application is listening on.
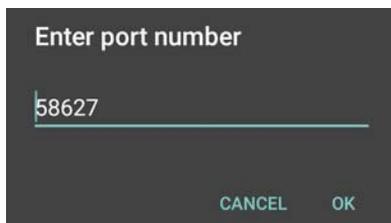
Figure 3-19 *Port Number Entry*

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

Generating Advanced Data Formatting Rules

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

- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.

- Criteria - Criteria can be set according to Input plug-in, symbology, matching string within the data (at the specified position) and/or data length. Received data must match the defined criteria in order for the data to be processed.

- Actions - A set of procedures defined to format data. There are four types of actions which are for formatting cursor movement, data modification, data sending and delay specifications. An action can be defined to send the first number of characters to the Output plug-in, pad the output data with spaces or zeros, remove spaces in data, etc.

Configuring ADF Plug-in

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

1. Touch (⊞) > ▥ .
2. Touch a DataWedge profile.
3. In **Keystroke Output**, touch **Advanced data formatting**.
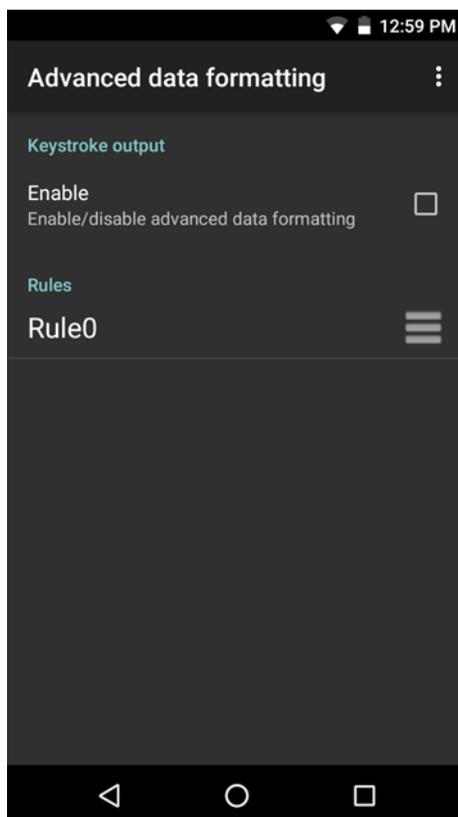
Figure 3-20   *Advanced Data Formatting Screen*

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

Creating a Rule

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

1. Touch ⋮.
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 **OK**.

Defining a Rule

1. Touch the newly created rule in the **Rules** list.
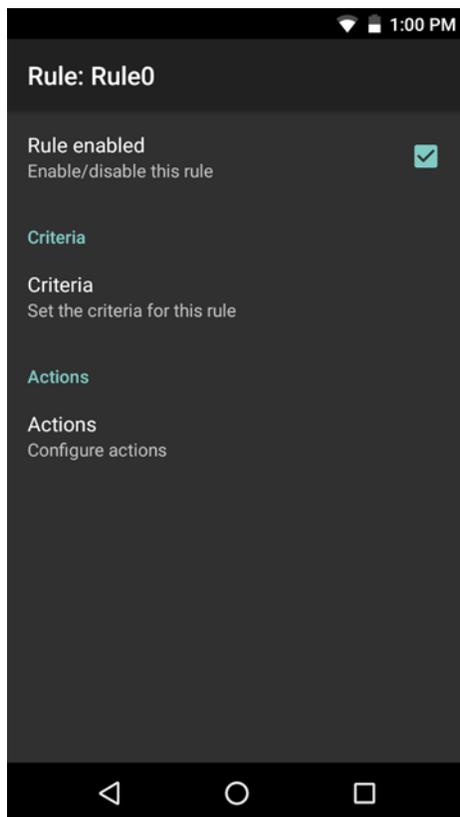
Figure 3-21   *Rule List Screen*

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

Defining Criteria

1. Touch **Criteria**.
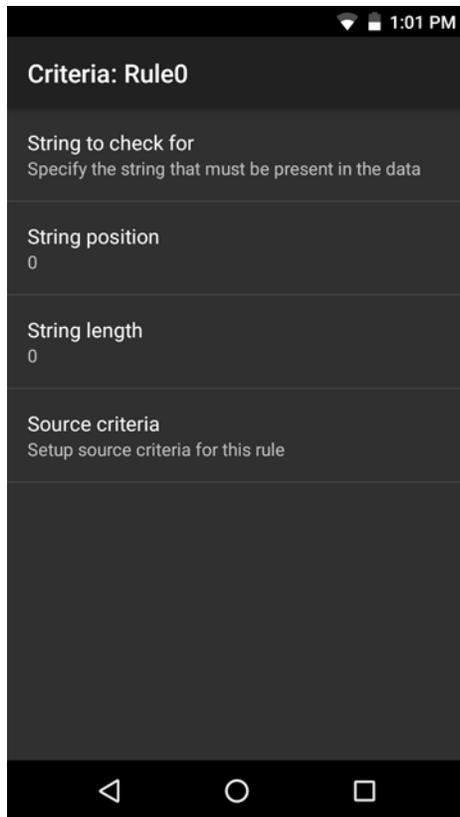
Figure 3-22 *Criteria Screen*

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

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

4. Touch **OK**.

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

6. Touch the **+** or **-** to change the value.

7. Touch **OK**.

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

9. Touch the **+** or **-** to change the value.

10. Touch **OK**.

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

12. Touch **Barcode input**. Options vary depending upon the device configuration.

13. Touch the **Source enabled** checkbox to accept data from this source.
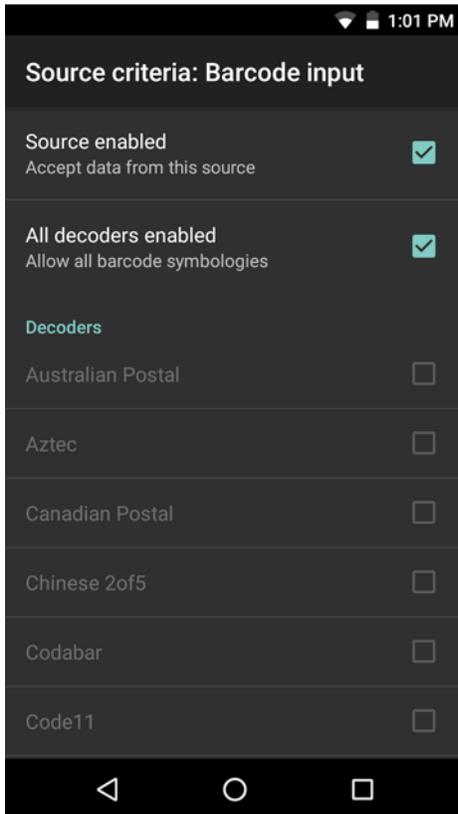
Figure 3-23   *Barcode Input Screen*

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

15. Touch ◁ until the **Rule** screen appears.

16. If required, repeat steps to create another rule.

17. Touch ◁ until the Rule screen appears.

Defining an Action

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

1. Touch ⋮.

2. Touch **New action**.

3. In the **New action** menu, select an action to add to the **Actions** list. See *Table 3-2 on page 3-35* 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

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 3-2 *ADF Supported Actions*

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

Table 3-2 *ADF Supported Actions (Continued)*

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

Deleting an Action

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

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

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

Modify the data as follows:

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

To create an ADF rule for the above example:

1. Touch ⊞ > ⷮ.
2. Touch **Profile0**.
3. Under **Keystroke Output**, touch **Advanced data formatting**.
4. Touch **Enable**.
5. Touch **Rule0**.
6. Touch **Criteria**.
7. Touch **String to check for**.
8. In the **Enter the string to check for** text box, enter 129 and then touch **OK**.
9. Touch **String position**.
10. Change the value to 0.
11. Touch **OK**.
12. Touch **String length**.
13. Change value to 12.
14. Touch **OK**.
15. Touch **Source criteria**.
16. Touch **Barcode input**.
17. Touch **All decoders enabled** to disable all decoders.
18. Touch **Code 39**.
19. Touch ◁ three times.
20. Touch **Actions**.
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 ◁.

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 ◁.

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 ◁.
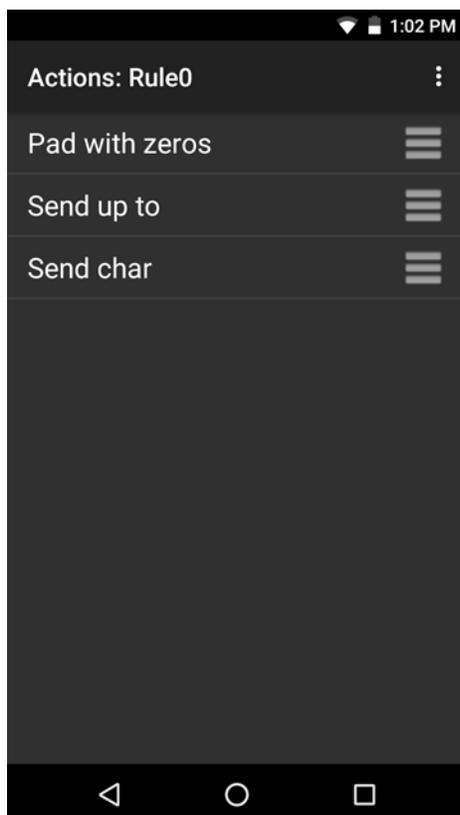
Figure 3-24   *ADF Sample Screen*

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 3-25   *Sample Bar Code*

48. Press and hold the scan key.

    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.

49. The LED lights green, a beep sounds and the device vibrates, by default, to indicate the bar code was decoded successfully. The formatted data 0000129 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.
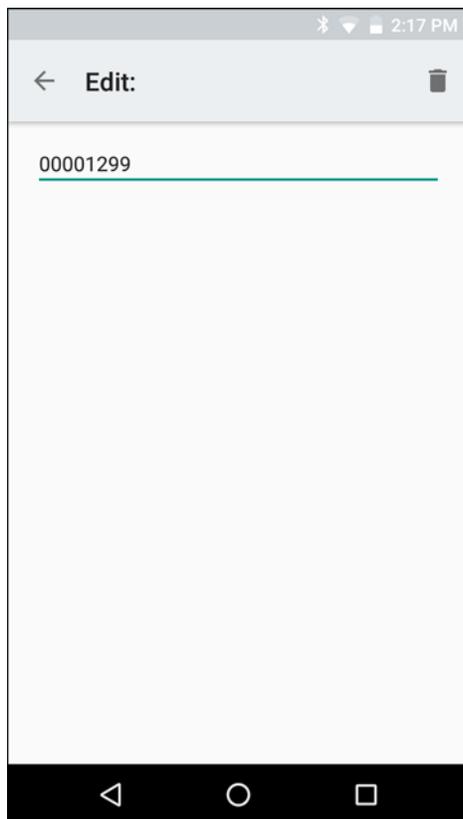
Figure 3-26   *Formatted Data*

DataWedge Settings

The DataWedge Settings screen provides access to general, non-profile related options. Touch ⋮ > **Settings**.
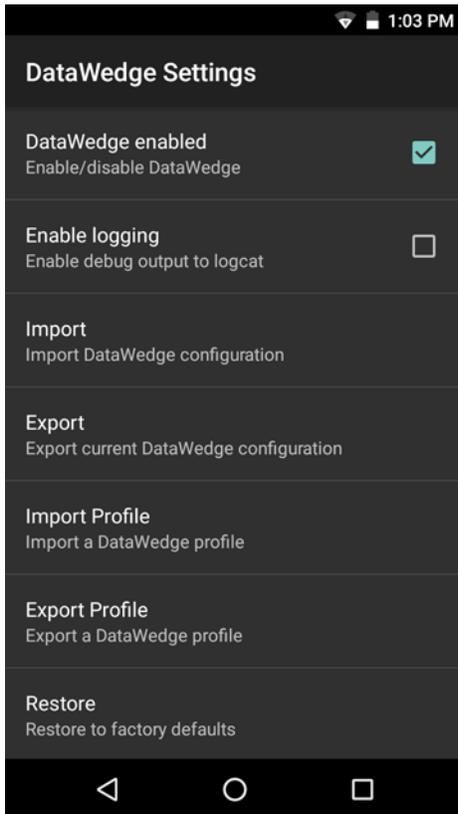
Figure 3-27 *DataWedge Settings Window*

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

Importing a Configuration File

1. Copy the configuration file to the microSD card **/Android/data/com.symbol.datawedge/files** folder.
2. Touch ⊞ > ▮▮ .
3. Touch ⋮ .
4. Touch **Settings**.
5. Touch **Import**.
6. Touch filename to import.

   The configuration file (*datawedge.db*) is imported and replaces the current configuration.

Exporting a Configuration File

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

Importing a Profile File

> ✓ *NOTE* Do not change the filename of the of the profile file. If the filename is changed, the file will not be imported.

1. Copy the profile file to the On Device Storage **/Android/data/com.symbol.datawedge** folder.
2. Touch ⊞ > 📊 .
3. Touch ⋮ .
4. Touch **Settings**.
5. Touch **Import Profile**.
6. Touch the profile file to import.
7. 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

1. Touch ⊞ > 📊 .
2. Touch ⋮ .
3. Touch **Settings**.
4. Touch **Export Profile**.
5. Touch the profile to export.
6. Touch **Export**.

   The profile file (*dwprofile_x.db*, where x = name of the profile) is saved to the root of the On-device Storage.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Touch ⊞ > 📊 .
2. Touch ⋮ .
3. Touch **Settings**.
4. Touch **Restore**.
5. 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 On-device Storage. The configuration file created is automatically named *datawedge.db*. The profile file created is automatically named *dwprofile_x.db*, where *x* is the profile name. The files can then the copied to the On-device Storage of other devices and imported into DataWedge on those devices. Importing a configuration or profile replaces the existing settings.

Enterprise Folder

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

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

Auto Import

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

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

> **NOTE** A Factory Reset deletes all files in the Enterprise folder.
>
> It is strongly recommended that the user exits DataWedge before remotely deploying any configuration or profile. It is required that the file permissions are set to 666.

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

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 Device and Mass Deploy

To disable DataWedge and deploy onto multiple devices:

1. Touch ⊞ > ⬛ .
2. Touch ⋮ .
3. Touch **Settings**.
4. Unselect the **DataWedge enabled** check box.
5. Export the DataWedge configuration. See *Exporting a Configuration File on page 3-41* for instructions. See *Configuration and Profile File Management on page 3-42* for instructions for using the auto import feature.

Soft Scan Feature

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

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

action: "com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER"

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

name: "com.symbol.emdk.datawedge.api.EXTRA_PARAMETER"

value: "START_SCANNING" or "STOP_SCANNING" or "TOGGLE_SCANNING"

Sample

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

Scanner Input Plugin

The ScannerInputPlugin API command can be used to enable/disable the scanner plug-in being used by the currently active Profile. Disabling the scanner plug-in effectively disables scanning in that Profile, regardless of whether the Profile is associated or unassociated. Valid only when Barcode Input is enabled in the active Profile.

✓ *NOTE* Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

Function Prototype

```
Intent i = new Intent();
i.setAction(ACTION);
i.putExtra(EXTRA_DATA, "<parameter>");
```

Parameters

action: String "com.symbol.datawedge.api.ACTION_SCANNERINPUTPLUGIN"

extra_data: String "com.symbol.datawedge.api.EXTRA_PARAMETER"

<parameter>: The parameter as a string, using either of the following:

- "ENABLE_PLUGIN" - enables the plug-in
- "DISABLE_PLUGIN" - disables the plug-in

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, e.g.

```
$ adb logcat -s DWAPI
```

Error messages will be logged for invalid actions and parameters.

Example

```
// define action and data strings
String scannerInputPlugin =
"com.symbol.datawedge.api.ACTION_SCANNERINPUTPLUGIN";
String extraData = "com.symbol.datawedge.api.EXTRA_PARAMETER";


public void onResume() {
    // create the intent
    Intent i = new Intent();
    // set the action to perform
    i.setAction(scannerInputPlugin);
    // add additional info
    i.putExtra(extraData, "DISABLE_PLUGIN");
    // send the intent to DataWedge
    context.this.sendBroadcast(i);
}
```

Comments

This Data Capture API intent allows the scanner plug-in for the current Profile to be enabled or disabled. For example, activity A launches and uses the Data Capture API intent to switch to ProfileA in which the scanner plug-in is enabled, then at some point it uses the Data Capture API to disable the scanner plug-in. Activity B is launched. In DataWedge, ProfileB is associated with activity B. DataWedge switches to ProfileB. When activity A comes back to the foreground, in the **onResume** method, activity A needs to use the Data Capture API intent to switch back to ProfileA, then use the Data Capture API intent again to disable the scanner plug-in, to return back to the state it was in.

NOTE Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

The above assumes that ProfileA is not associated with any applications/activities, therefore when focus switches back to activity A, DataWedge will not automatically switch to ProfileA therefore activity A must switch back to ProfileA in its onResume method. Because DataWedge will automatically switch Profile when an activity is paused, it is recommended that this API function be called from the onResume method of the activity.

Enumerate Scanners

Use the enumerateScanners API command to get a list of scanners available on the device.

Function Prototype

```
Intent i = new Intent();
i.setAction(ACTION);
```

Parameters

action: String "com.symbol.datawedge.api.ACTION_ENUMERATESCANNERS"

Return Values

The enumerated list of scanners will be returned via a broadcast Intent. The broadcast Intent action is "com.symbol.datawedge.api.ACTION_ENUMERATEDSCANNERLIST" and the list of scanners is returned as a string array (see the example below).

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, e.g.

```
$ adb logcat -s DWAPI
```

Error messages will be logged for invalid actions and parameters

Example

```
// first send the intent to enumerate the available scanners on the device
// define action string
String enumerateScanners = "com.symbol.datawedge.api.ACTION_ENUMERATESCANNERS";
// create the intent
Intent i = new Intent();
// set the action to perform
i.setAction(enumerateScanners);
// send the intent to DataWedge
context.this.sendBroadcast(i);

// now we need to be able to receive the enumerate list of available scanners
String enumeratedList = "com.symbol.datawedge.api.ACTION_ENUMERATEDSCANNERLIST";
String KEY_ENUMERATEDSCANNERLIST = "DataWedgeAPI_KEY_ENUMERATEDSCANNERLIST";
// Create a filter for the broadcast intent
IntentFilter filter = new IntentFilter();
filter.addAction(enumeratedList);
registerReceiver(myBroadcastReceiver, filter);

// now we need a broadcast receiver
private BroadcastReceiver myBroadcastReceiver = new BroadcastReceiver() {
   @Override
   public void onReceive(Context context, Intent intent) {
      String action = intent.getAction();
      if (action.equals(enumeratedList)) {
         Bundle b = intent.getExtras();
         String[] scanner_list = b.getStringArray(KEY_ENUMERATEDSCANNERLIST);
      }
   }
};
```

Comments

The scanner and its parameters are set based on the currently active Profile.

Set Default Profile

Use the setDefaultProfile API function to set the specified Profile as the default Profile.

Default Profile Recap

Profile0 is the generic Profile used when there are no user created Profiles associated with an application.

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.

Usage Scenario

A launcher application has a list of apps that a user can launch and that none of the listed apps has an associated DataWedge Profile. Once the user has selected an app, the launcher needs to set the appropriate DataWedge Profile for the selected app. This could be done by using **setDefaultProfile** to set the default Profile to the required Profile. Then when the user launches the selected app, DataWedge auto Profile switching switches to the default Profile (which is now the required Profile for that app).

If, for some reason, the launched app has an associated DataWedge Profile then that will override the set default Profile.

When control is returned to the launcher application, **resetDefaultProfile** can be used to reset the default Profile.

Function Prototype

```
Intent i = new Intent();

i.setAction(ACTION);

i.putExtra(EXTRA_DATA, "<profile name>");
```

Parameters

action: String "com.symbol.datawedge.api.ACTION_SETDEFAULTPROFILE"

extra_data: String "com.symbol.datawedge.api.EXTRA_PROFILENAME"

<profile name>: The Profile name to set as the default Profile as a string (case-sensitive).

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, e.g.

```
$ adb logcat -s DWAPI
```

Error messages will be logged for invalid actions, parameters and failures (e.g. Profile not found or associated with an application).

Example

```
// define action and data strings
String setDefaultProfile = "com.symbol.datawedge.api.ACTION_SETDEFAULTPROFILE";
String extraData = "com.symbol.datawedge.api.EXTRA_PROFILENAME";

public void onResume() {
   // create the intent
   Intent i = new Intent();
   // set the action to perform
   i.setAction(setDefaultProfile);
   // add additional info
   i.putExtra(extraData, "myProfile");
   // send the intent to DataWedge
   context.this.sendBroadcast(i);
}
```

Comments

The API command will have no effect if the specified Profile does not exist or if the specified Profile is already associated with an application. DataWedge will automatically switch Profiles when the activity is paused, so it is recommended that this API function be called from the onResume method of the activity.

Zebra recommends that this Profile be created to cater to all applications/activities that would otherwise default to using Profile0. This will ensure that these applications/activities continue to work with a consistent configuration. For example, let's say that initially Profile0 is the default Profile using the camera as the barcode scanner. Using the Browser application and scanning a barcode with the camera, DataWedge enters the data into the Browser. Now launch an application that changes the default Profile to a Profile using the blockbuster as the barcode scanner. When returning to the Browser application, since it is using the default Profile, scanning will now be via the blockbuster not the camera as previously. To ensure that the Browser continues to use the camera as the barcode scanner a Profile should be created and associated with the Browser that specifies the camera as the barcode scanner.

Reset Default Profile

Use the resetDefaultProfile API function to reset the default Profile back to Profile0.

Function Prototype

```
Intent i = new Intent();


i.setAction(ACTION);
i.putExtra(EXTRA_DATA, "<Profile name>");
```

Parameters

action: String "com.symbol.datawedge.api.ACTION_RESETDEFAULTPROFILE"

extra_data: String "com.symbol.datawedge.api.EXTRA_PROFILENAME"

<Profile name>: The Profile name to set as the default Profile as a string (case-sensitive).

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, e.g.

```
$ adb logcat -s DWAPI
```

Error messages will be logged for invalid actions, parameters and failures (e.g. Profile not found or associated with an application).

Example

```
// define action string
String resetDefaultProfile =
"com.symbol.datawedge.api.ACTION_RESETDEFAULTPROFILE";

public void onResume() {
    // create the intent
    Intent i = new Intent();
    // set the action to perform
    i.setAction(resetDefaultProfile);
    context.this.sendBroadcast(i);
}
```

Comments

None.

Switch To Profile

Use the SwitchToProfile API action to switch to the specified Profile.

Profiles Recap

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

DataWedge includes a default Profile, Profile0, that is created automatically the first time DataWedge runs.

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.

✓ **NOTE** Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

NOTE

A single Profile may be associated with one or many activities/apps, however, given an activity, only one Profile may be associated with it.

Usage Scenario

An application has two activities. Activity A only requires EAN13 bar codes to be scanned. Activity B only requires MSR card data. Profile B is configured to only scan EAN13 bar codes and is left unassociated. Profile M is configured to only accept MSR input and is left unassociated. When Activity A launches it uses SwitchToProfile to activate Profile B. Similarly, when Activity B launches it uses switchToProfile to activate Profile M.

If another activity/app comes to the foreground, DataWedge auto Profile switching will set the DataWedge Profile accordingly either to the default Profile or to an associated Profile.

When Activity A (or Activity B) comes back to the foreground it will use switchToProfile to reset the Profile back to Profile B (or Profile M).

Function Prototype

```
Intent i = new Intent();
i.setAction(ACTION);
i.putExtra(EXTRA_DATA, "<profile name>");
```

Parameters

action: String "com.symbol.datawedge.api.ACTION_SWITCHTOPROFILE"

extra_data: String "com.symbol.datawedge.api.EXTRA_PROFILENAME"

<profile name>: The Profile name to switch to as a string (case-sensitive).

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, e.g.

```
$ adb logcat -s DWAPI
```

Error messages will be logged for invalid actions, parameters and failures (e.g. Profile not found or associated with an application).

Example

```
// define action and data strings
String switchToProfile = "com.symbol.datawedge.api.ACTION_SWITCHTOPROFILE";
String extraData = "com.symbol.datawedge.api.EXTRA_PROFILENAME";


public void onResume() {
        super.onResume();
        // create the intent
        Intent i = new Intent();
        // set the action to perform
        i.setAction(switchToProfile);
        // add additional info
        i.putExtra(extraData, "myProfile");
        // send the intent to DataWedge
        context.this.sendBroadcast(i);
}
```

Comments

This API function will have no effect if the specified Profile does not exist or is already associated with an application.

DataWedge has a one-to-one relationship between Profiles and activities; a Profile can be associated only with a single activity. When a Profile is first created, it's not associated with any application, and will not be activated until associated. This makes it possible to create multiple unassociated Profiles.

This API function activates such Profiles.

For example, Profile A is unassociated and Profile B is associated with activity B. If activity A is launched and uses **SwitchToProfile** function to switch to Profile A, then Profile A will be active whenever activity A is in the foreground. When activity B comes to the foreground, DataWedge will automatically switch to Profile B.

When activity A returns to the foreground, the app must use `SwitchToProfile` again to switch back to Profile A. This would be done in the `onResume` method of activity A.

> ✓ **NOTE** Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

Notes

Because DataWedge will automatically switch Profile when the activity is paused, Zebra recommends that this API function be called from the onResume method of the activity.

After switching to a Profile, this unassociated Profile does not get assigned to the application/activity and is available to be used in the future with a different app/activity.

For backward compatibility, DataWedge's automatic Profile switching is not affected by the above API commands. This why the commands work only with unassociated Profiles and apps.

DataWedge auto Profile switching works as follows:

Every second…

- Sets newProfileId to the associated Profile ID of the current foreground activity.
- If no associated Profile is found, sets newProfileId to the associated Profile ID of the current foreground app.
- If no associated Profile is found, sets newProfileId to the current default Profile (which MAY NOT be Profile0).
- Checks the newProfileId against the currentProfileId. If they are different:
  - deactivates current Profile
  - activates new Profile (newProfileId)
  - sets currentProfileId = newProfileId

CHAPTER 4 USB COMMUNICATION

Introduction

Connect the TC51 to a host computer using the Rugged Charge/USB cable or the 1-Slot USB/Charge Only cradle to transfer files between the TC51 and the host computer. See *Chapter 2, Accessories* for more information.

When connecting the TC51 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Transferring Files using Media Transfer Protocol

✓ **NOTE** Use Media Transfer Protocol (MTP) to copy files between the TC51 (internal memory or microSD card) and the host computer.

1. Connect the Rugged Charge/USB Cable to the TC51 or place the TC51 into the 1-Slot USB/Charge Only Cradle. See *Chapter 2, Accessories* for setup information.

2. Pull down the Notification panel and touch **USB for Charging**.
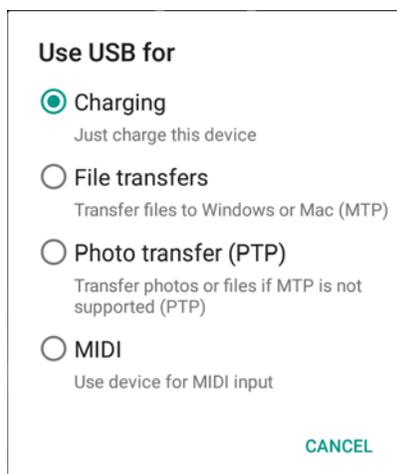
Figure 4-1 *Use USB Dialog Box*

3. Touch **File transfers**.

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

5. Locate the **TC51** as a portable device.

6. Open the **SD card** or the **Internal storage** folder.

7. Copy files to and from the TC51 or delete files as required.

Transferring Files using Photo Transfer Protocol

✓ *NOTE* Use Photo Transfer Protocol (PTP) to copy photos from either the microSD card or internal memory to the host computer.

1. Connect the Rugged Charge/USB Cable to the TC51 or place the TC51 into the 1-Slot USB/Charge Only Cradle. See *Chapter 2, Accessories* for setup information.

2. Pull down the Notification panel and touch **USB for Charging**.
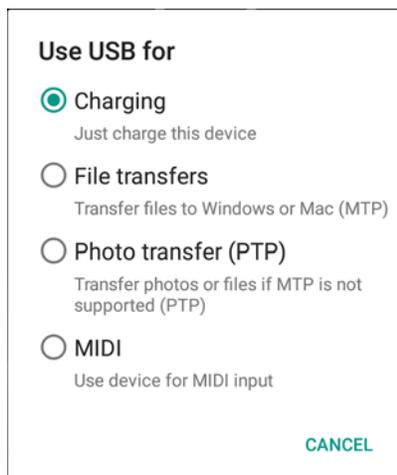
Figure 4-2   *Use USB Dialog Box*

3. Touch **Photo transfer (PTP)**.

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

5. Open the **SD card** or the **Internal storage** folder.

6. Copy or delete photos as required.

Disconnect from the Host Computer

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

1. On the host computer, unmount the device.

2. Remove the Rugged Charge/USB cable from the device or remove the device from the cradle.

CHAPTER 5 SETTINGS

Introduction

This chapter describes settings available for configuring the device.

WLAN Configuration

Configuring a Wi-Fi Network

To set up a Wi-Fi network:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🔽 **Wi-Fi**.

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

4. The device searches for WLANs in the area and lists them on the screen.

5. Scroll through the list and select the desired WLAN network.

6. Touch the desired network. If the network security is **Open**, the device automatically connects to the network. For all other network security a dialog box appears.
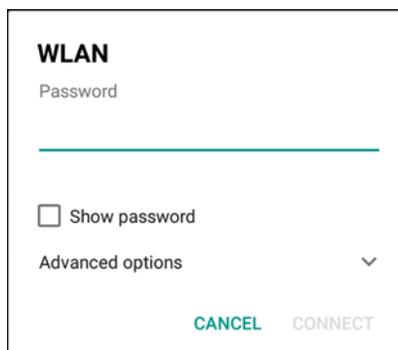
Figure 5-1   *WLAN WEP Network Security Dialog Box*

Figure 5-2   *WLAN 802.11 EAP Network Security Dialog Box*

7.   If the network security is **WEP** or **WPA/WPS2 PSK**, enter the required password and then touch **Connect**.

8.   If the network security is 802.1x EAP:

   • Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **TTLS** or **LEAP**.

   • Touch the **Phase 2 authentication** drop-down list and select an authentication method.

   • If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.

   • If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the Location & security settings.

   • If required, in the **Identity** text box, enter the username credentials.

   • If desired, in the **Anonymous identity** text box, enter an anonymous identity username.

   • If required, in the **Password** text box, enter the password for then given identity.

   NOTE By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See *Configuring for a Proxy Server on page 5-3* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 5-4* for setting the device to use a static IP address.

9.   Touch **Connect**.

10. Touch ○.

Manually Adding a Wi-Fi Network

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

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🔻 **Wi-Fi**.

3. Slide the Wi-Fi switch to the **On** position.

4. Touch ⋮ > **Add network**.

5. In the **Network SSID** text box, enter the name of the Wi-Fi network.

6. In the **Security** drop-down list, select the type of security. Options:

    • **None**

    • **WEP**

    • **WPA/WPA2 PSK**

    • **802.1x EAP**.

7. If the network security is **None**, touch **Save**.

8. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password and then touch **Save**.

9. If the network security is **802.1x EAP**:

    • Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **TTLS** or **LEAP**.

    • Touch the **Phase 2 authentication** drop-down list and select an authentication method.

    • If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.

    • If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the **Security** settings.

    • If required, in the **Identity** text box, enter the username credentials.

    • If desired, in the **Anonymous** identity text box, enter an anonymous identity username.

    • If required, in the **Password** text box, enter the password for then given identity.

    ✓ **NOTE** By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See *Configuring for a Proxy Server on page 5-3* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 5-4* for setting the device to use a static IP address.

10. Touch **Save**. To connect to the saved network, touch and hold on the saved network and select **Connect to network**.

11. Touch ○.

Configuring for a Proxy Server

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

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

1. In the network dialog box, touch a network.

    2.   Touch **Advanced options**.

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

Figure 5-3   *Proxy Settings*

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

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

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

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

    7.   Touch **Connect**.

    8.   Touch ◯.

Configuring the Device to Use a Static IP Address

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

    1.   In the network dialog box, touch a network.

    2.   Touch **Advanced options**.

    3.   Touch **IP settings** and select **Static**.

Figure 5-4   *Static IP Settings*

4. In the **IP address** text box, enter an IP address for the device.

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

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

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

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

9. Touch **Connect**.

10. Touch ◯.

Advanced Wi-Fi Settings

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

Use the **Advanced** settings to configure additional Wi-Fi settings. From the **Wi-Fi** screen, touch ≡ > **Advanced** to view the advanced settings.

- **Network notification** - When enabled, notifies the user when an open network is available.
- **Keep Wi-Fi on during sleep** - Opens a menu to set whether and when the Wi-Fi radio turns off.
    - **Always On** - The radio stays on when the device enters suspend mode (default).
    - **Only when plugged in** - The radio stays on while the device is connected to external power.
    - **Never On** - The radio turns off when the device enters suspend mode (default).
- **Wi-Fi frequency band** - Touch to select the frequency band. Options: **Automatic** (default), **5 GHz only** or **2.4 GHz only**.
- **Install Certificates** – Touch to install certificates.

- **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **IP address** - Displays the IP address assigned to the device.

Touch **Additional settings**.

- **Regulatory**
  - **Country selection** - Displays the acquired country code if 802.11d is enabled else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Use to select the frequency band. Options: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
  - **Available channels (2.4 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
  - **Available channels (5 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
- **Logging**
  - **Advanced Logging** – Touch to enable advanced logging. Advanced logging
  - **Wireless logs** - Use to capture Wi-Fi log files.
    - **Fusion Logger** - Touch to open the **Fusion Logger** application. This application maintains a history of high level WLAN events which helps to understand the status of connectivity.
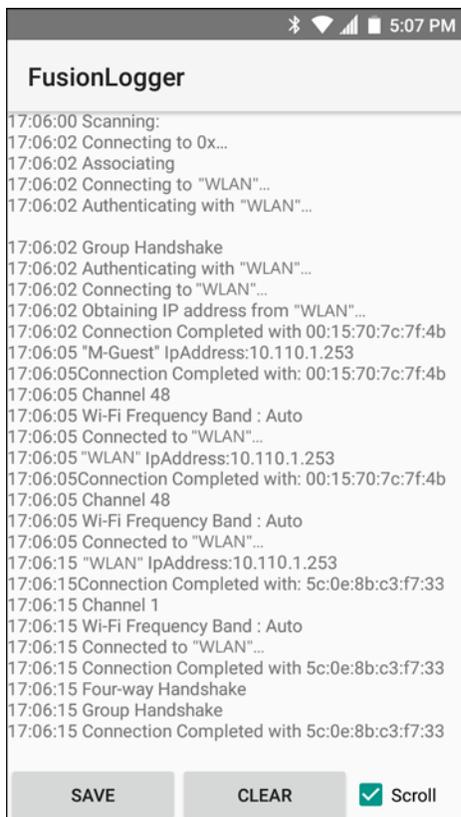
Figure 5-5   *Fusion Logger Screen*

- **Fusion Status** - Touch to display live status of WLAN state. Also provides information of device and connected profile.
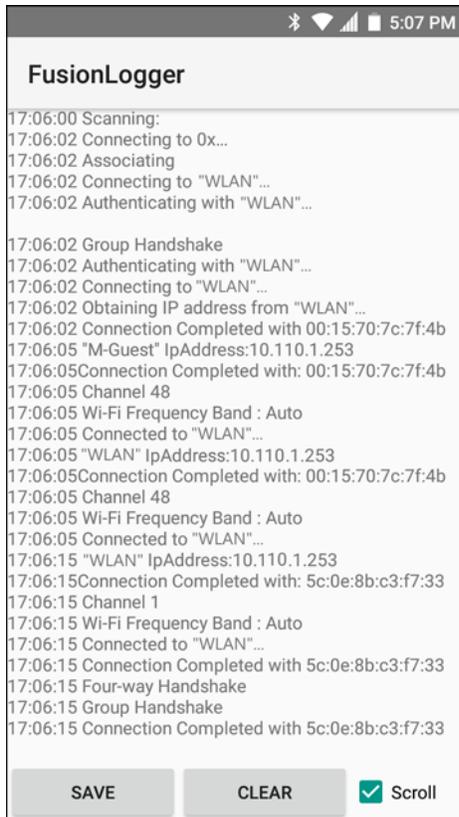
Figure 5-6   *Fusion Status Screen*

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

Screen Unlock Settings

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

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🔒 **Security**.

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

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.

    - **None** - Disable screen unlock security.
    - **Swipe** - Slide the lock icon to unlock the screen.
    - **Pattern** - Draw a pattern to unlock screen. See Set Screen Unlock Using Pattern for more information.
    - **PIN** - Enter a numeric PIN to unlock screen. See Set Screen Unlock Using PIN for more information.
    - **Password** - Enter a password to unlock screen. See Set Screen Unlock Using Password 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.

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

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

Slide 🔒 up to unlock the screen.If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.

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

Set Screen Unlock Using PIN

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.
2. Touch 🔒 **Security**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. Touch in the text field.
6. Enter a PIN (4 numbers) then touch **Next**.
7. Re-enter PIN and then touch **Next**.
8. Touch ◯. The next time the device goes into suspend mode a PIN is required upon waking.
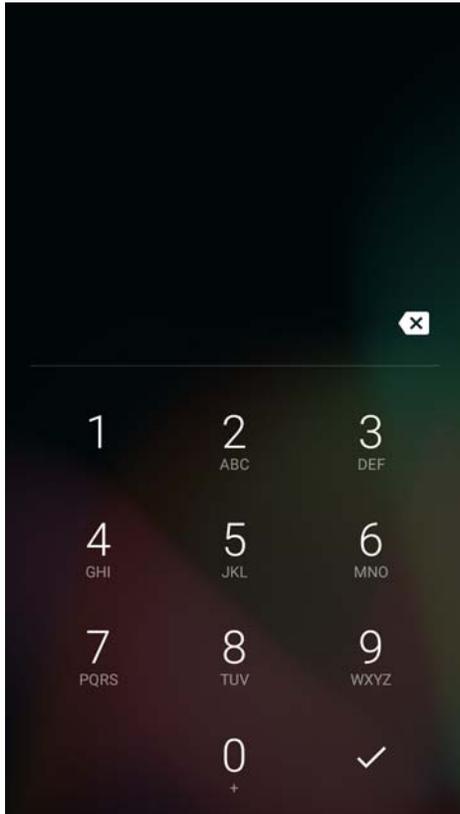
Figure 5-7   *PIN Screen*

Set Screen Unlock Using Password

1.   Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2.   Touch 🔒 **Security**.

3.   Touch **Screen lock**.

4.   Touch **Password**.

5.   Touch in the text field.

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

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

8.   Touch ◯. The next time the device goes into suspend mode a PIN is required upon waking.
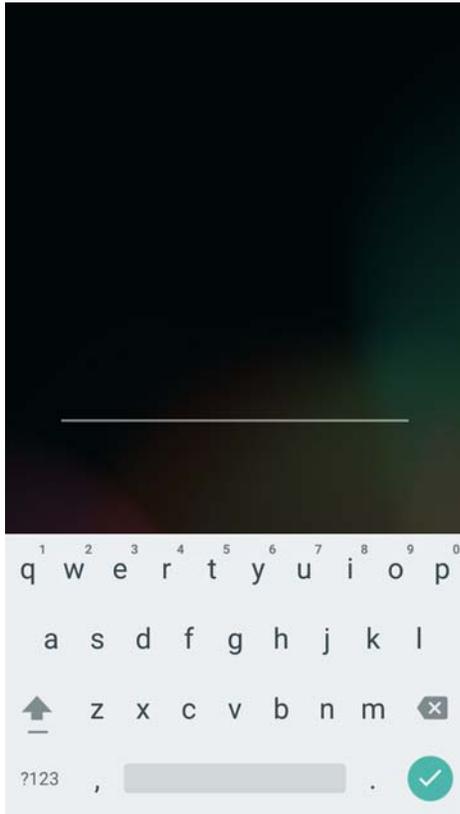
Figure 5-8 *Password Screen*

Set Screen Unlock Using Pattern

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🔒 **Security**.

3. Touch **Screen lock**.

4. Touch **Pattern**.

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

6. Draw a pattern connecting at least four dots.
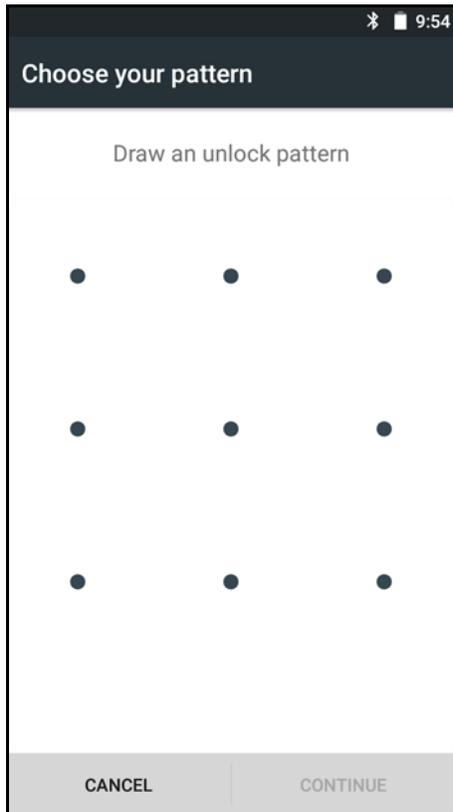
Figure 5-9   *Choose Your Pattern Screen*

7. Touch **Continue**.

8. Re-draw the pattern.

9. Touch **Confirm**.

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

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

12. Touch ○. The next time the device goes into suspend mode a Pattern is required upon waking.
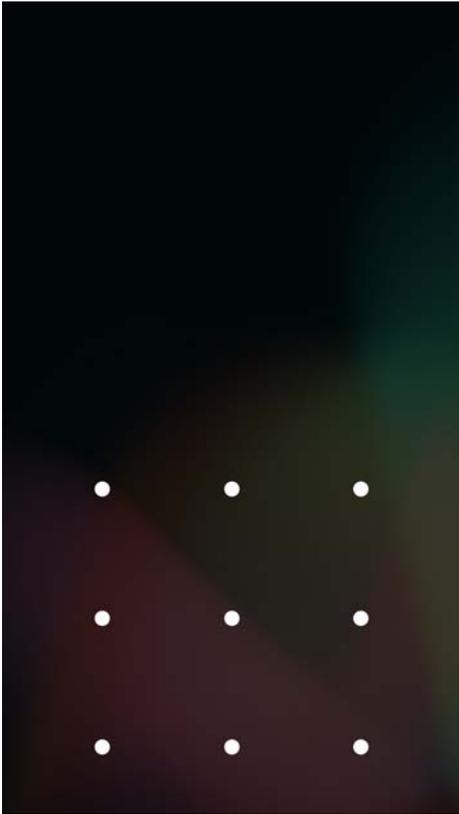
Figure 5-10 *Pattern Screen*

Passwords

To set the device to briefly show password characters as the user types:

Touch ⊞ > ⚙ > 🔒 **Security**. Slide the **Make passwords visible** switch to the ON position.

Button Remapping

The TC51's buttons can be programmed to perform different functions or shortcuts to installed applications.

✓ **NOTE** It is not recommended to remap the scan button.

- Scan
- VOLUMEDOWN
- VOLUMEUP
- LEFT_TRIGGER_2
- REAR_BUTTON.

Remapping a Button

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ▦ **Key Programmer**.
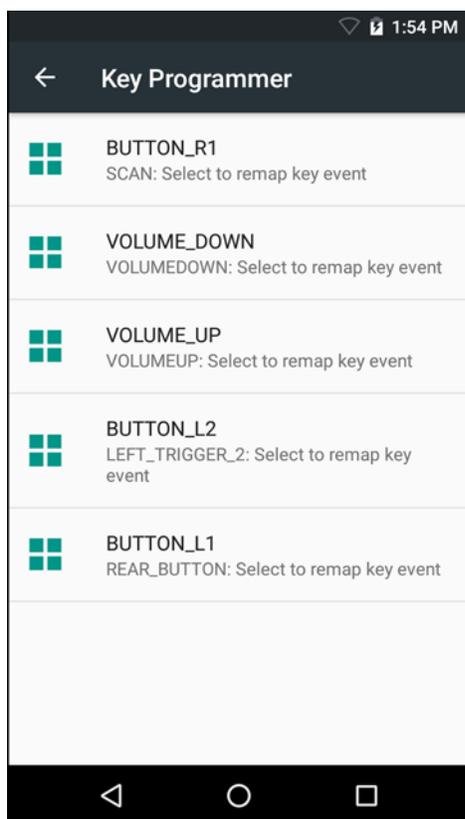
Figure 5-11 *Key Programmer Screen*

3. Select the button to remap.
4. Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.
5. Touch a function or application shortcut to map to the button.

NOTE If you select an application shortcut, the application icon appears next to the button on the Key Programmer screen.
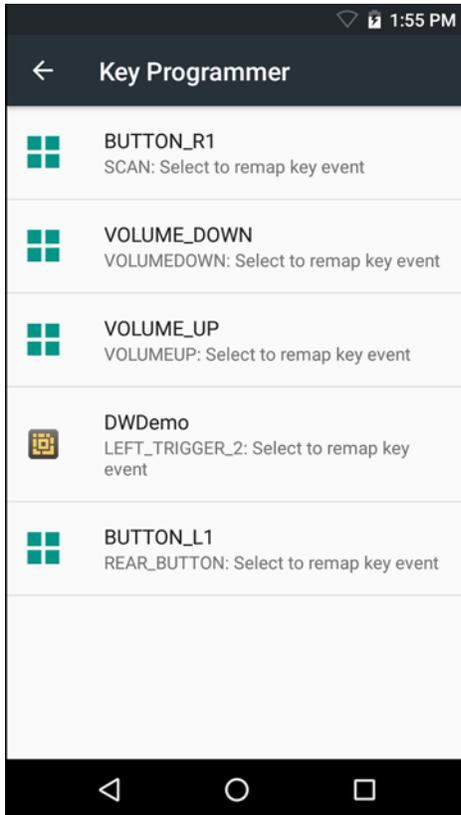
Figure 5-12 *Remapped Button*

6. Touch ○.

Accounts

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

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

Language Usage

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

Changing the Language Setting

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🌐 **Language & input**.

3. Touch **Language**, select a language from the list of available languages.

   The operating system text changes to the selected language.

Adding Words to the Dictionary

1. In the **Language & input** screen, touch **Personal dictionary**.

2. If prompted, select the language that this word or phase is stored.

3. Touch **+** to add a new word or phrase to the dictionary.

4. Enter the word or phrase.

5. In the **Shortcut** text box, enter a shortcut for the word or phrase.

6. Touch ◁.

Keyboard Settings

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

- Android Keyboard
- Enterprise keyboard.

PTT Express Configuration

Refer to the *PTT Express User Guide* at http://www.zebra.com/support for information on configuring the PTT Express Client application.

RxLogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics. It allows for custom plug-ins to be created and work seamlessly with this tool. RxLogger is used to diagnose device and application issues. Its information tracking includes the following: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging, cellular logging, TCP dumps, Bluetooth logging, GPS logging, logcat, FTP push/pull, ANR dumps, etc. All logs and files generated are saved onto flash storage on the device (internal or external).
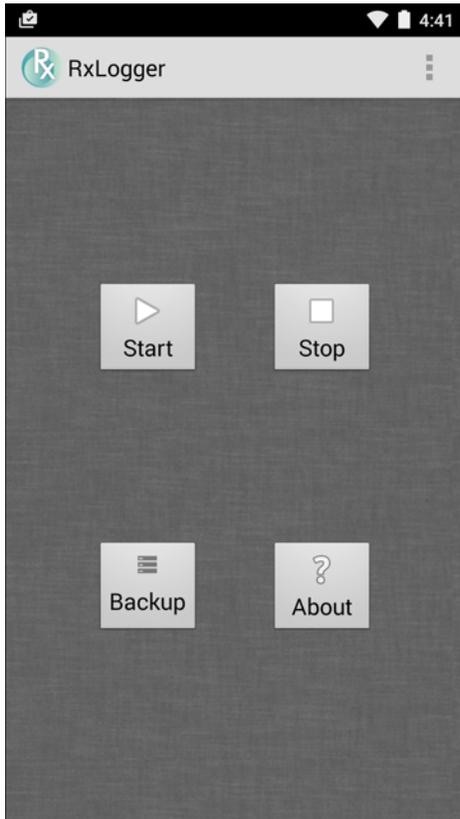
Figure 5-13 *RxLogger*

RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plug-ins already built-in. The included plug-ins are described below. Touch ⋮ > **Settings** to open the configuration screen.
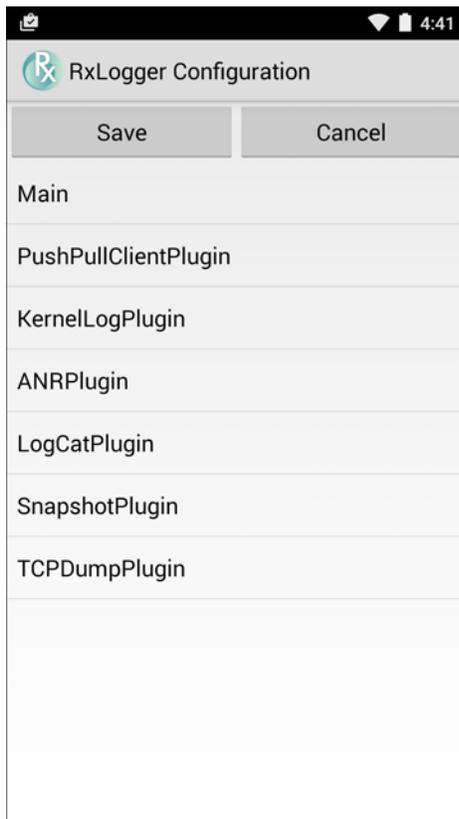
Figure 5-14 *RxLogger Configuration Screen*

Main Log Plug-in

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

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

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

Snapshot Plug-in

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the base path to use to store the snapshot files
- **Log filename** - Specifies the base filename for all the snapshot files. This file number will be appended to this base filename when saving the snapshot.
- **Log interval** - Specifies the interval, in milliseconds, on which to invoke a detailed snapshot.
- **Time to keep** - Specifies the interval, in milliseconds, to keep snapshot files on the file system.
- **CPU Info** - Enables detailed per process CPU logging in the snapshot.
- **Memory Info** - Enables logging of detailed per process memory usage in the snapshot.
- **Battery Info** - Enables logging of detailed power information including battery life, on time, charging, and wake locks.
- **Processes** - Enables dumping the complete process list in the snapshot.
- **Threads** - Enables dumping all processes and their threads in the snapshot.
- **Properties** - Enables dumping of all system properties on the device. This includes build/version information as well as state information.
- **Network Usage** - Enables dumping of all available network interfaces and the routing table.
- **Filesystems** - Enables dumping of the available volumes on the file system and the free storage space for each.
- **Usage stats** - Enables dumping of detailed usage information for each package on the device. This includes the number of starts and duration of each run.

Logcat Plug-in

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

- **Enable Plugin** - Enables logging for this plug-in.
- **Log path** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.

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

PushPullClient Plug-in

The PushPullClient plug-in is designed to automatically push log files to a remote FTP server on a regular basis. It also has the capability to pull a remote file from the FTP server to a local directory on the device to automatically

pull down a new configuration file so that the configuration of the tool can be set and updated remotely. The tool uses a flag file on the FTP site (based on device serial number) to ensure the file is only pulled once. By removing the flag file for a particular device you can force it to download the file again.

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

TCPDump Plug-in

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

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

ANR Plugin

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

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

Kernal Plug-in

- **Enable Plugin** - Enables logging for this kernal buffer.

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

Configuration File

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

Enabling Logging

To enable logging:

1. Touch ⊞ > ℞ .
2. Touch **Start**.
3. Touch ○.

Disabling Logging

To disable logging:

1. Touch ⊞ > ℞ .
2. Touch **Stop**.
3. Touch ○.

Extracting Log Files

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

About Phone

Use About phone settings to view information about the TC51. Touch ⊞ > ⚙ > ⓘ **About phone**.

- **Status** - Touch to display the following:
  - **Battery status** - Indicates if the battery is charging (on AC power) or discharging (on battery power).
  - **Battery level** - Indicates the battery charge level.
  - **IP address** - Displays the IP address of the device.
  - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
  - **Ethernet MAC address** - Displays the Ethernet driver MAC address.
  - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
  - **Serial number** - Displays the serial number of the device.
  - **Up time** - Displays the time that the TC51 has been running since being turned on.
- **Battery Information** - Displays information about the battery.
- **SW components** - Lists filenames and versions for various software on the TC51.
- **Legal information** - Opens a screen to view legal information about the software included on the TC51.
- **Model number** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Android security patch level** - Displays the security patch level date.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

CHAPTER 6 APPLICATION DEPLOYMENT

Introduction

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

Security

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

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

Secure Certificates

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

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

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

Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the microSD card. See *Chapter 4, USB Communication* for information about connecting the device to a host computer and copying files.

2. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

3. Touch 🔒 **Security**.

4. Touch **Install from storage**.

5. Navigate to the location of the certificate file.

6. Touch the filename of the certificate to install.

7. If prompted, enter the password for credential storage. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

8. If prompted, enter the certificate's password and touch **OK**.

9. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.
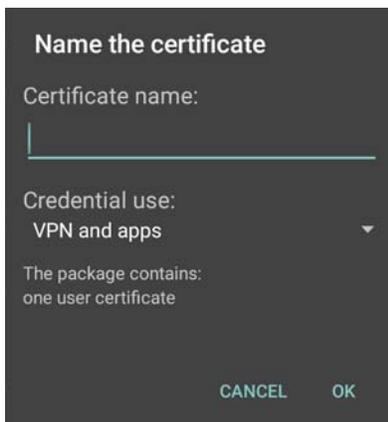
Figure 6-1   *Name the Certificate Dialog Box*

10. 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

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🔒 **Security**.

    - **Trusted credentials** - Touch to display the trusted system and user credentials.

    - **Install from storage** - Touch to install a secure certificate from the microSD card.

    - **Clear credentials** - Deletes all secure certificates and related credentials.

Development Tools

Android

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

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

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

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

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

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

By default, the Developer Options are hidden. To un-hide the developer options, swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

Touch ⓘ. **About device**. Scroll down to **Build number**. Tap **Build number** seven times until **You are now a developer** appears.

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

EMDK for Android

EMDK for Android provides developers with a comprehensive set of tools to easily create powerful line-of-business applications for enterprise mobile computing devices. It's designed for Google™ Android SDK and Android Studio, and includes class libraries, sample applications with source code, and all associated documentation to help your applications take full advantage of what Zebra devices have to offer.

The kit also delivers Profile Manager, a GUI-based device configuration tool providing exclusive access to the Zebra MX device management framework. This allows developers to configure Zebra devices from within their applications in less time, with fewer lines of code and with fewer errors.

For more information go to: techdocs.zebra.com.

StageNow

StageNow is Zebra's next-generation Android Staging Solution, supporting Android Lollipop, KitKat®, and Jelly Bean operating systems, and built on the MX 4.3/4.4/5.x/6.0 platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a bar code, reading a tag, or playing an audio file.

The StageNow Staging Solution includes the following components:

- The StageNow Workstation tool installs on the staging workstation (host computer) and lets the administrator easily create staging profiles for configuring device components, and perform other staging actions such as checking the condition of a target device to determine suitability for software upgrades or other activities. The StageNow Workstation stores profiles and other created content for later use.
- The StageNow Client resides on the device and provides a user interface for the staging operator to initiate staging. The operator uses one or more of the desired staging methods (print and scan a bar code, read an NFC tag or play an audio file) to deliver staging material to the device.

For more information go to: techdocs.zebra.com.

ADB USB Setup

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

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

Enabling USB Debugging

By default, USB debugging is disabled. To enable USB debugging:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ⓘ **About phone**.

3. Scroll down to **Build number**.

4. Tap **Build number** seven time. The message **You are now a developer!** appears.

5. Touch ◁.

6. Touch { } **Developer options**.

7. Slide the **USB debugging** switch to the **ON** position.

8. Touch **OK**.

9. Connect the device to the host computer using the Rugged Charge/USB Cable.

   The **Allow USB debugging?** dialog box appears on the device.

10. On the device, touch **OK**.

11. On the host computer, navigate to the `platform-tools` folder.

12. Type `adb devices`.

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

> **NOTE** If device number does not appear, ensure that ADB drivers are installed properly.

13. Touch ○.

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 6-5*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 6-7*.
- microSD Card, see *Installing Applications Using a microSD Card on page 6-8*
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

Installing Applications Using the USB Connection

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

1. Connect the device to a host computer using the Rugged Charge/USB cable.

2. Pull down the Notification panel and touch **USB for Charging**.

Use USB for

◉ Charging
Just charge this device

○ File transfers
Transfer files to Windows or Mac (MTP)

○ Photo transfer (PTP)
Transfer photos or files if MTP is not
supported (PTP)

○ MIDI
Use device for MIDI input

CANCEL
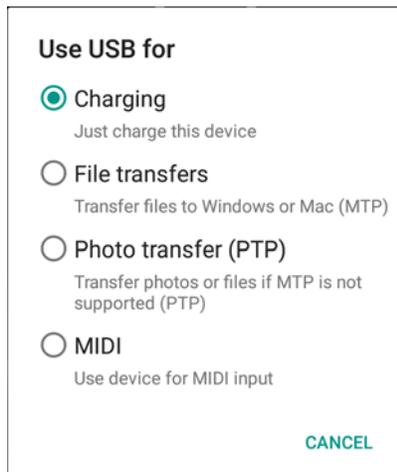
Figure 6-2   *Use USB Dialog Box*

3. Touch **File transfers**.

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

5. On the host computer, copy the application *.apk* file from the host computer to the device.

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

6. Disconnect the device from the host computer.

7. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

8. Touch 🔒 **Security**.

9. Slide the **Unknown sources** switch to the **ON** position.

10. Touch **OK**.

11. Touch ○.

12. Touch ⊞ > 📁 to view files on the microSD card or Internal Storage.

13. Locate the application *.apk* file.

14. Touch the application file to begin the installation process.

15. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
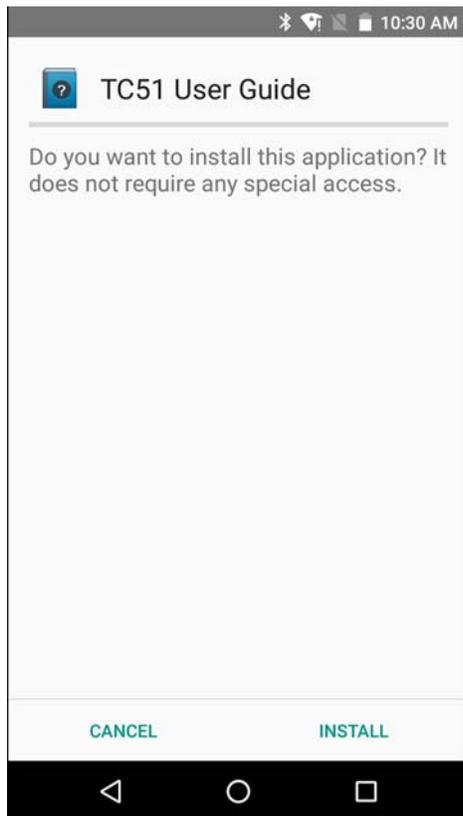
Figure 6-3   *Accept Installation Screen*

16. 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.

Ensure that the ADB drivers are installed on the host computer. See *ADB USB Setup on page 6-4*.

1. Connect the device to a host computer using USB. See *Chapter 4, USB Communication*.

2. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

3. Touch { } **Developer options**.

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

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

6. Touch **OK**.

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

```
adb install <application>
```

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

8. Disconnect the device from the host computer. See *Chapter 4, USB Communication*.

Installing Applications Using a microSD Card

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

1. Connect the device to a host computer using USB. See *Chapter 4, USB Communication*.
2. Copy the application APK file from the host computer to the microSD card.
3. Remove the microSD card from the host computer.
4. Press and hold the Power button until the menu appears.
5. Touch **Power off**.
6. Press the two battery latches in.
7. Lift the battery from the device.
8. Lift the access door.
9. Insert the microSD card.
10. Replace the access door.
11. Insert the battery, bottom first, into the battery compartment in the back of the device.
12. Press the battery down until the battery release latch snaps into place.
13. Press and hold the Power button to turn on the device.
14. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙️.
15. Touch 🔒 **Security**.
16. Slide the **Unknown sources** switch to the **ON** position.
17. Touch **OK**.
18. Touch ○.
19. Touch ⦙⦙⦙.

✓ **NOTE** In **File Browser**, the microSD card path is `/storage/sdcard1`.

20. Touch 📁 to view files on the microSD card.
21. Locate the application APK file.
22. Touch the application file to begin the installation process.
23. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
24. Touch **Open** to open the application or **Close** to exit the installation process. The application appears in the App list.

Uninstalling an Application

To uninstall an application:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch 🤖 **Apps**.

3. Scroll through the list to the application.
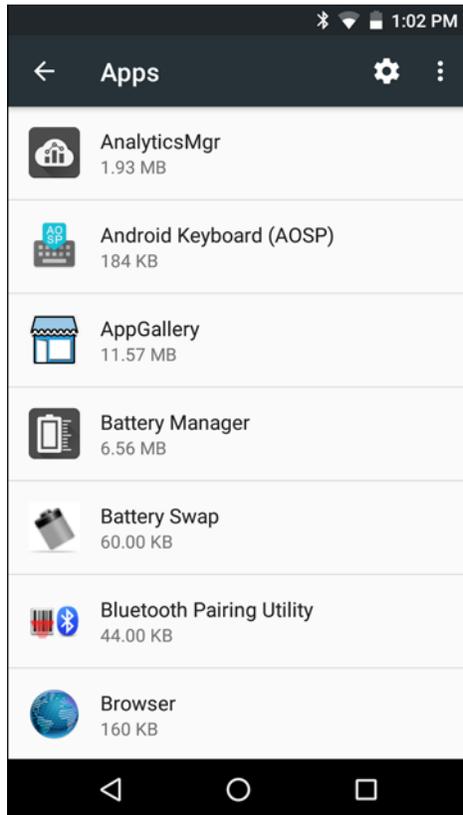
Figure 6-4   *Downloaded Screen*

4. Touch the application to uninstall.

5. Touch **Uninstall**.

6. Touch **OK** to confirm.

Performing a System Update

System Update packages can contain either partial or complete updates for the operating system. Zebra distributes the System Update packages on the Zebra Support & Downloads web site. Perform system update using either a microSD card or using ADB.

Download the System Update Package

Download the system update package:

1. Go to the Zebra Support & Downloads web site, http://www.zebra.com/support.

2. Download the appropriate System Update package (GMS - T51N0M3XCPUEFyyyyy.zip or Non-GMS - T51N0M3X0PUEFyyyyy.zip) to a host computer.

Using microSD Card

1. Copy the System Update zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see *Chapter 4, USB Communication* for more information) and then installing the microSD card into the device (see *Replacing the microSD Card on page 1-7* for more information).
   - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See *Chapter 4, USB Communication* for more information. Disconnect the device from the host computer.

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

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

Figure 6-5 *System Recovery Screen*

6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.

7. Press the Power button.

8. Use the Volume Up and Volume Down buttons to navigate to the T51N0MXXXRExxyyyyy.zip (GMS) or T51N0MXXXREyyyyy.zip (Non-GMS) file.

9. Press the Power button. The System Update installs and then the device returns to the Recovery screen.

10. Press the Power button to reboot the device.

> ✓ **NOTE** If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Using ADB

To update the system using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down with two fingers from the status bar to open the quick access panel and then 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 devices
   ```

   The following displays:

   ```
   List of devices attached
   ```

   ```
   XXXXXXXXXXXXXXX device
   ```
   (where XXXXXXXXXXXXXXX is the device number).

   ✓ **NOTE** If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:

   ```
   adb reboot recovery
   ```

10. Press Enter. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

12. Press the Power button.

13. On the host computer command prompt window type:

    ```
    adb sideload <file>
    ```

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

14. Press Enter. The System Update installs (progress appears as percentage in the Command Prompt window) and then the Recovery screen appears.

15. Press the Power button to reboot the device.

   ✓ **NOTE** If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Verify System Update Installation

To check that the system update installed properly:

1. On the device, swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ⓘ **About**.

3. Scroll down to **Build number**.

    4. Ensure that the build number matches the new system update package file number.

Performing an Enterprise Reset

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

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

Perform Enterprise Reset using either a microSD card or using ADB.

Download the Enterprise Reset Package

Download the system update package:

1. Go to the Zebra Support & Downloads web site, http://www.zebra.com/support.

2. Download the Enterprise Reset file (T51N0MXXXRExxyyyyy.zip) to a host computer.

Using microSD Card

1. Copy the Enterprise Reset zip file to the root of the microSD card.

- Copy the zip file to a microSD card using a host computer (see *Chapter 4, USB Communication* for more information) and then installing the microSD card into the device (see *Replacing the microSD Card on page 1-7* for more information).

- Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See *Chapter 4, USB Communication* for more information. Disconnect the device from the host computer.

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

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

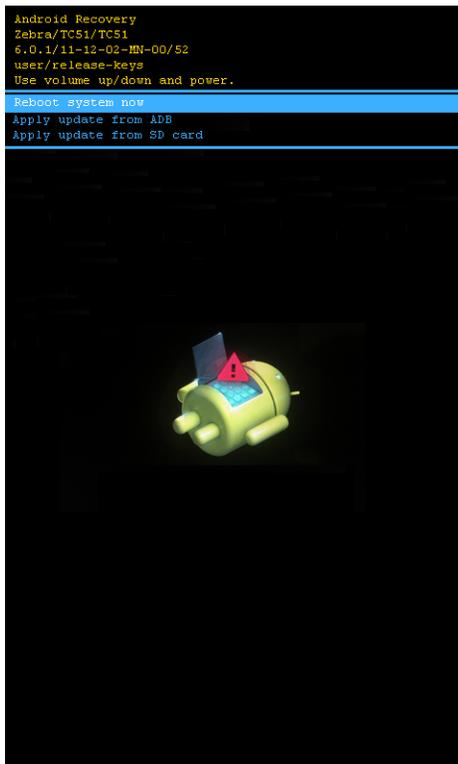**5.** Press and hold the PTT button until the device vibrates. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

6. Press the Up and Down Volume buttons to navigate to the **apply update from sdcard**.

7. Press the Power button.

8. Press the Up and Down Volume buttons to navigate to the T51N0MXXXRExxyyyyy.zip file.

9. Press the Power button. The Enterprise Reset occurs and then the device returns to the Recovery screen.

10. Press the Power button.

Using ADB

To perform an Enterprise Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down with two fingers from the status bar to open the quick access panel and then 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 type:

   `adb devices.`

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

   ✓ ***NOTE*** If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:

   `adb reboot recovery`

10. Press Enter. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

12. Press the Power button.

13. On the host computer command prompt window type:

    `adb sideload <file>`

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

14. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.

15. Press the Power button to reboot the device.

Performing a Factory Reset

A Factory Reset erases all data in the **/cache**, **/data** and **/enterprise** partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See *Performing a System Update on page 6-9* for more information.

Download the Factory Reset Package

Download the Factory Reset package:

1. Go to the Zebra Support & Downloads web site, http://www.zebra.com/support.

2. Download the appropriate Factory Reset file (T51N0MXXXRFxxyyyyy.zip) to a host computer.

Using microSD Card

1. Copy the Factory Reset zip file to the root of the microSD card.

- Copy the zip file to a microSD card using a host computer (see *Chapter 4, USB Communication* for more information) and then installing the microSD card into the device (see *Replacing the microSD Card on page 1-7* for more information).

- Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See *Chapter 4, USB Communication* for more information. Disconnect the device from the host computer.

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

3. Touch **Reboot**.

4. Touch **OK**. The device resets.

5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

6. Press the Up and Down Volume buttons to navigate to the **apply update from sdcard**.

7. Press the Power button.

8. Press the Up and Down Volume buttons to navigate to the T51N0MXXXRFxxyyyyy.zip file.

9. Press the Power button. The Factory Reset occurs and then the device returns to the Recovery screen.

10. Press the Power button.

Using ADB

To perform an Factory Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.

2. Connect the cable or cradle to the host computer.

3. On the device, swipe down with two fingers from the status bar to open the quick access panel and then 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 reboot recovery
   ```

9. Press Enter. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

10. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

11. Press the Power button.

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

    ```
    adb devices.
    ```

    The following displays:

    ```
    List of devices attached
    XXXXXXXXXXXXXXX device
    ```
    (where XXXXXXXXXXXXXXX is the device number).

    ✓ **NOTE** If device number does not appear, ensure that ADB drivers are installed properly.

13. Type:

```
adb reboot recovery
```

14. Press Enter. The System Recovery screen appears. See *Figure 6-5 on page 6-10*.

15. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.

16. Press the Power button.

17. On the host computer command prompt window type:

```
adb sideload <file>
```

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

18. Press Enter. The Factory Reset package installs and then the Recovery screen appears.

19. Press the Power button to reboot the device.

Storage

The device contains four types of file storage:

- Random Access Memory (RAM)
- Internal storage
- External storage (microSD card)
- 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 ⚙ > ▦ **Memory**.
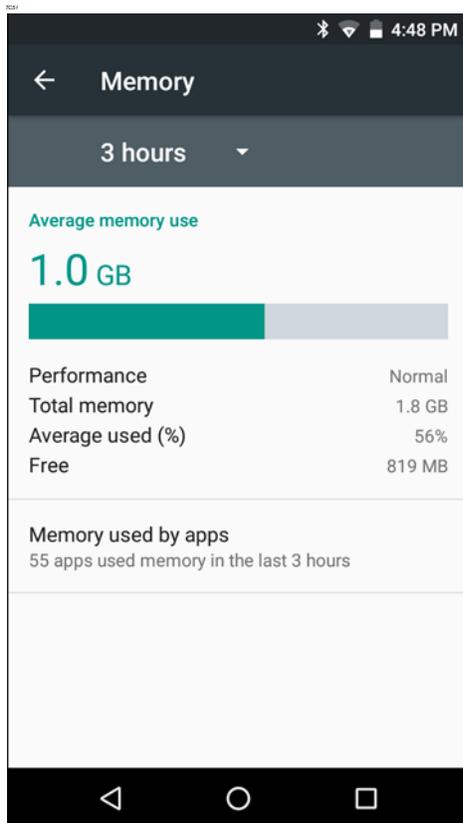
Figure 6-6 *Memory Screen*

The screen displays the amount of used and free RAM.

Internal Storage

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

To view the used and available space on the internal storage:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.
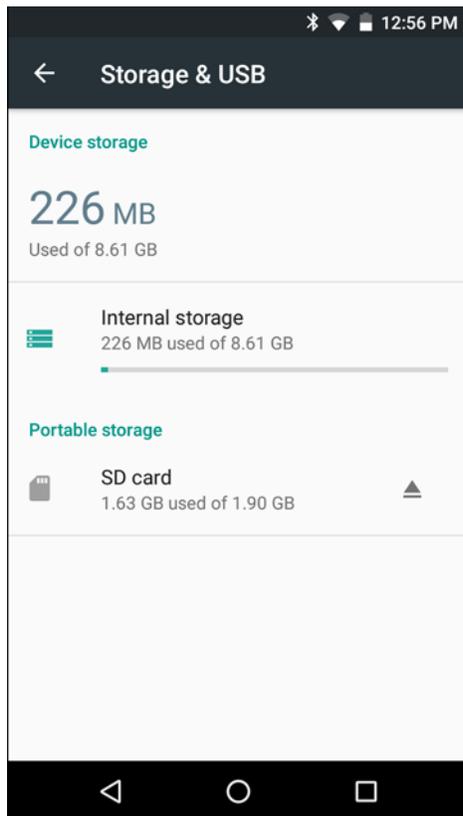
2. Touch ▤ **Storage & USB**.

Figure 6-7   *Storage Screen*

- **Internal Storage** - Displays the total amount of space on internal storage and amount used.

Touch **Internal storage** to display a the amount of storage used by apps, photos, videos, audio and other files.
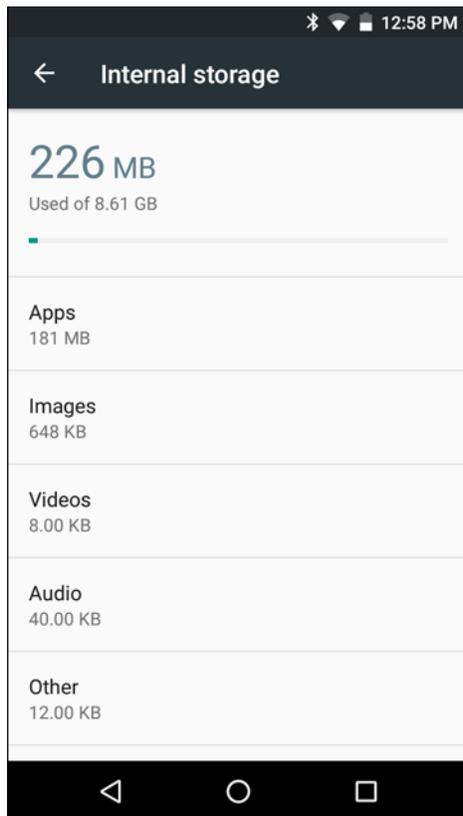
Figure 6-8 *Internal Storage Screen*

External Storage

The TC51 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the TC51 is connected to a host computer.

To view the used and available space on the microSD card:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2. Touch ☰ **Storage & USB**.
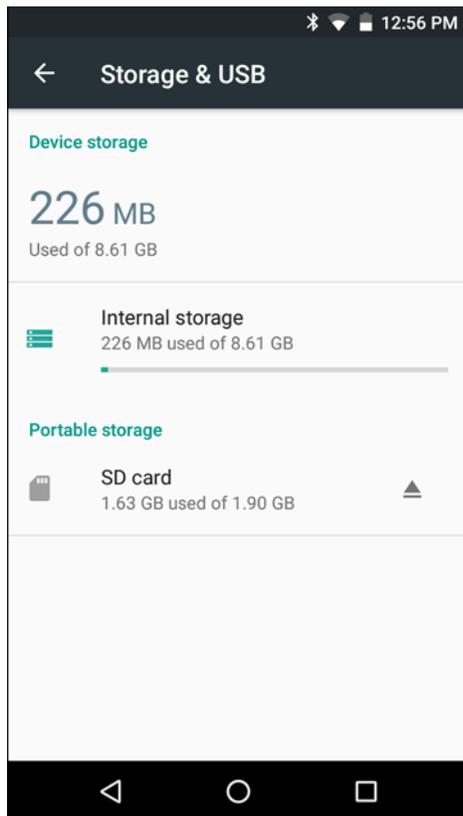
Figure 6-9   *Storage Screen*

Portable storage displays the total amount of space on the installed microSD card and the amount used.

To unmount the microSD card, touch ▲.

Touch **SD card** to view the contents of the card.
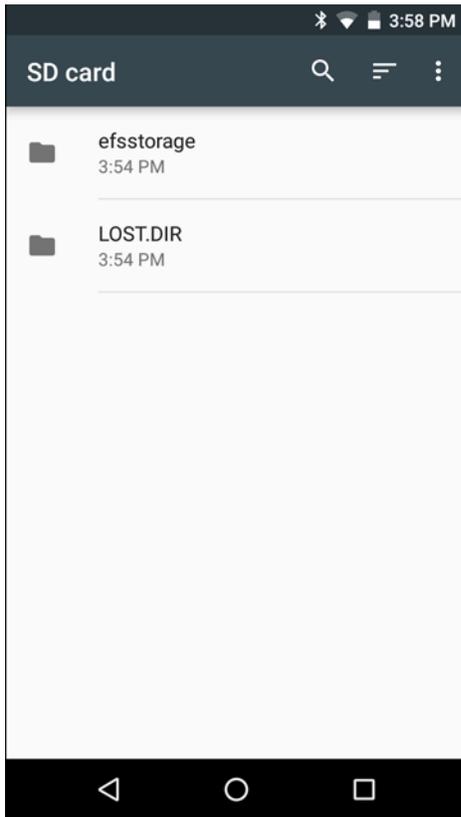
Figure 6-10   *SD Card Contents List*

Formatting a microSD Card

To format an installed microSD card as portable storage:

1. Touch **SD card**.

2. Touch **⋮** > **Settings**.
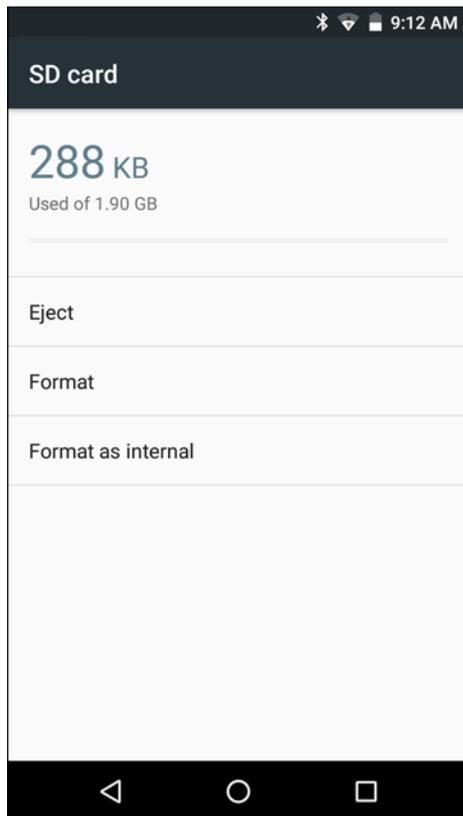
Figure 6-11   *SD Card Settings Screen*

3.   Touch **Format**.
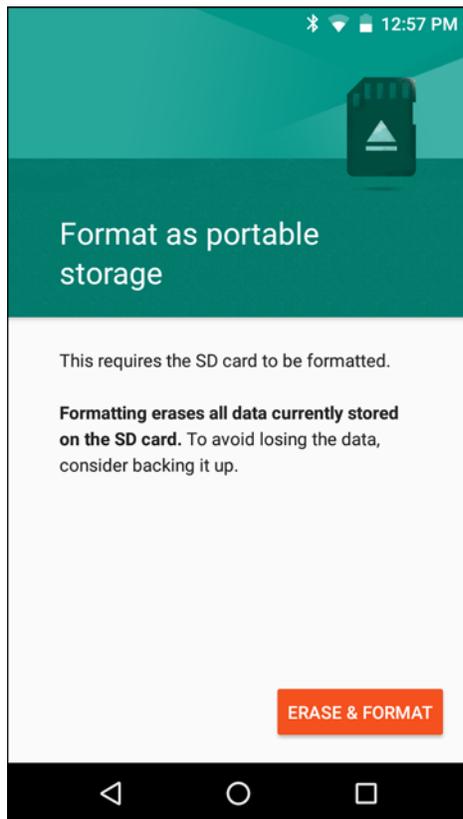
Figure 6-12 *Format Screen*

4. Touch **ERASE & FORMAT**.

5. Touch **DONE**.

Format as Internal Memory

You can format a microSD card as internal memory to increase the actual amount of the device's internal memory. Once formatted, the microSD card can only be read by this device. To format an installed microSD card as internal memory:

1. Touch **SD card**.

2. Touch ⋮ > **Settings**.
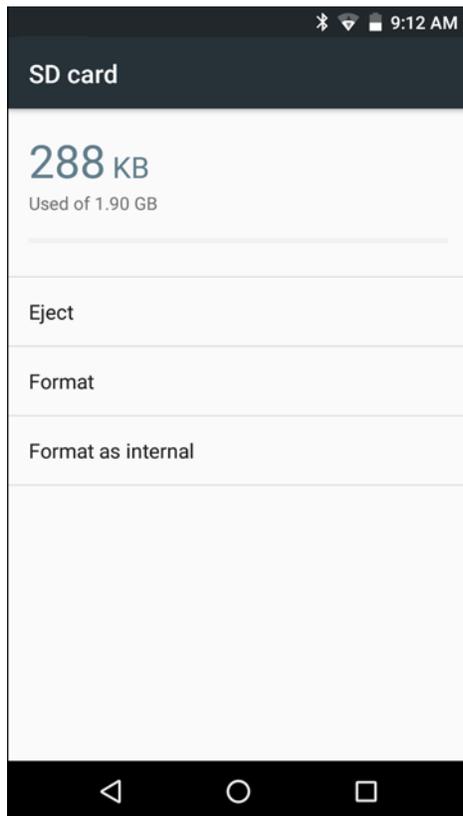
Figure 6-13   *SD Card Settings Screen*

3. Touch **Format as internal**.
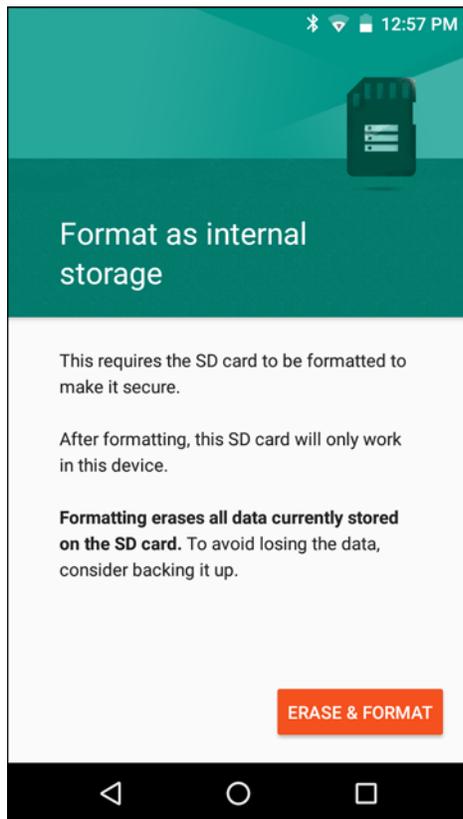
Figure 6-14   *Format Screen*

4.   Touch **ERASE & FORMAT**.

5.   Touch **DONE**.

Enterprise Folder

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

Application Management

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

1.   Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙.

2.   Touch 🤖 **Apps**.
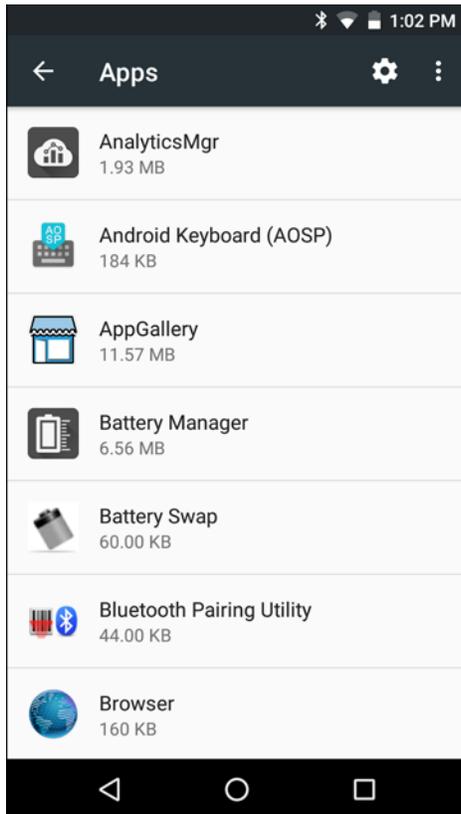
Figure 6-15 *Apps Screen*

Touch ⋮ > **Show system** to include system processes in the list.

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

Viewing Application Details

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

- **Force stop** - stop an application.
- **Uninstall** - remove the application and all of its data and settings from the device. See *Uninstalling an Application on page 6-8* for information about uninstalling applications.
- **Storage** - lists how much information is stored, and includes a button for clearing it.
- **Permissions** - lists the areas on the device that the application has access to.
- **Notification** - set the application notification settings.
- **Open by default** - clears If you have configured an application to launch certain file types by default, you can clear that setting here.
- **Battery** - lists the amount of computing power used by the application.
- **Memory** - lists the average application memory usage.

Managing Downloads

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

1. Touch ⊞ > ⬇ .

2. Touch an item to open it.

3. Touch headings for earlier downloads to view them.

4. Touch and hold an item, select items to delete and touch 🗑 . The item is deleted from storage.

5. Touch ☰ > **By name** or **By date modified** or **By size** to switch between them.

    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 7 MAINTENANCE AND TROUBLESHOOTING

Introduction

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

Maintaining the TC51

For trouble-free service, observe the following tips when using the TC51:

- Do not scratch the screen of the TC51. When working with the TC51, use the optional stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the TC51 screen.

- The touch-sensitive screen of the TC51 is glass. Do not to drop the TC51 or subject it to strong impact.

- Protect the TC51 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 TC51 in any location that is dusty, damp, or wet.

- Use a soft lens cloth to clean the TC51. If the surface of the TC51 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.

- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.

Display Best Practices

Image Retention

Image retention may occur when a static image continuously displays for extended periods of time. A user may see a faint remnant of the image even after a new image displays. To prevent image retention:

- set the display to turn off after a few minutes of idle time.
- rotate background images on a periodic basis.
- turn off the display when the device in not in use.
- use a screen saver with the following characteristics:
  - background color set to black
  - use a small moving image (approximately 2% of the display size).
  - move the image randomly across the screen
  - screen saver should be active as long as the static image is used.
  - Link to Zebra Screen Sample?

Battery Safety Guidelines

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Follow battery usage, storage, and charging guidelines found in this guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between +32°F and +104°F (0°C and +40°C)
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact the Global Customer Support Center.
- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- To enable authentication of an approved battery, as required by IEEE1725 clause 10.2.1, all batteries will carry a hologram. Do not fit any battery without checking it has the authentication hologram.
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.

- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, contact the 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 the Global Customer Support Center for more information.

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

Approved Cleanser Active Ingredients

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

Harmful Ingredients

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

Cleaning Instructions

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

Special Cleaning Notes

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

Cleaning Materials Required

- Alcohol wipes
- Lens tissue

- Cotton-tipped applicators
- Isopropyl alcohol
- Can of compressed air with a tube.

Cleaning Frequency

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

Cleaning the TC51

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:

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 pointed away from your face.

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

Cleaning Cradle Connectors

To clean the connectors on a cradle:

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

> ⚠️ **CAUTION** Do not point nozzle at yourself and others, ensure the nozzle or tube is 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.

TC51

Table 7-1   *Troubleshooting the TC51*

Problem	Cause	Solution
When pressing the power button the TC51 does not turn on.	Battery not charged.	Charge or replace the battery in the TC51.
	Battery not installed properly.	Install the battery properly.
	System crash.	Perform a reset.
When pressing the power button the TC51 does not turn on but two LEDs blink.	Battery charge is at a level where data is maintained but battery should be re-charged.	Charge or replace the battery in the TC51.
Battery did not charge.	Battery failed.	Replace battery. If the TC51 still does not operate, perform a reset.
	TC51 removed from cradle while battery was charging.	Insert TC51 in cradle. The 4,300 mAh battery charges to 90% in less than 2.5 hours at room temperature.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0°C (32°F) or above 40°C (104°F).
Cannot see characters on display.	TC51 not powered on.	Press the **Power** button.
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	TC51 removed from cradle or disconnected from host computer during communication.	Replace the TC51 in the cradle, or reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software was incorrectly installed or configured.	Perform setup.
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 closer to an access point.

Table 7-1   *Troubleshooting the TC51 (Continued)*

Problem	Cause	Solution
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 within 10 meters (32.8 feet) of the other device.
	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.
No sound.	Volume setting is low or turned off.	Adjust the volume.
TC51 shuts off.	TC51 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.	Replace the battery.
Tapping the window buttons or icons does not activate the corresponding feature.	The device is not responding.	Reset the device. See *Resetting the TC51 on page 1-8*.
A message appears stating that the TC51 memory is full.	Too many files stored on the TC51.	Delete unused memos and records. If necessary, save these records on the host computer (or use an SD card for additional memory).
	Too many applications installed on the TC51.	Remove user-installed applications on the TC51 to recover memory. Select (icon) > (icon) > (icon) **Apps** > **Downloaded**. Select the unused program and tap **Uninstall**.

Table 7-1   *Troubleshooting the TC51 (Continued)*

Problem	Cause	Solution
The TC51 does not decode with reading bar code.	Scanning application is not loaded.	Load a scanning application on the TC51 or enable DataWedge. See the system administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Place the TC51 within proper scanning range.
	TC51 is not programmed for the bar code.	Program the TC51 to accept the type of bar code being scanned. Refer to the EMDK or DataWedge application.
	TC51 is not programmed to generate a beep.	If the TC51 does not beep on a good decode, set the application to generate a beep on good decode.
	Battery is low.	If the scanner stops emitting a laser beam upon a trigger press, check the battery level. When the battery is low, the scanner shuts off before the TC51 low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or the Global Customer Support Center.
Cannot unlock TC51.	User enters incorrect password.	If the user enters an incorrect password eight times, the user is requested to enter a code before trying again.
		If the user forgot the password, contact system administrator.

1-Slot Charge Only Cradle

Table 7-2   *Troubleshooting the 1-Slot Charge Only Cradle*

Symptom	Possible Cause	Action
LEDs do not light when TC51 or spare battery is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	TC51 is not seated firmly in the cradle.	Remove and re-insert the TC51 into the cradle, ensuring it is firmly seated.
	Spare battery is not seated firmly in the cradle.	Remove and re-insert the spare battery into the charging slot, ensuring it is firmly seated.

Table 7-2   *Troubleshooting the 1-Slot Charge Only Cradle (Continued)*

Symptom	Possible Cause	Action
TC51 battery is not charging.	TC51 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure TC51 is seated correctly. Confirm main battery is charging. The 4,620 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The TC51 is not fully seated in the cradle.	Remove and re-insert the TC51 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
Spare battery is not charging.	Battery not fully seated in charging slot.	Remove and re-insert the spare battery in the cradle, ensuring it is firmly seated. The 4,620 mAh battery fully charges in less than six hours.
	Battery inserted incorrectly.	Re-insert the battery so the charging contacts on the battery align with the contacts on the cradle.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

4-Slot Charge Only Cradle with Battery Charger Troubleshooting

Table 7-3   *Troubleshooting the 4-Slot Charge Only Cradle with Battery Charger*

Problem	Cause	Solution
Battery is not charging.	TC51 removed from the cradle too soon.	Replace the TC51 in the cradle. The battery fully charges in approximately six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	TC51 is not inserted correctly in the cradle.	Remove the TC51 and reinsert it correctly. Verify charging is active. Touch ⊞ > ⚙ > ⓘ **About phone** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

5-Slot Charge Only Cradle Troubleshooting

Table 7-4 *Troubleshooting the 5-Slot Charge Only Cradle*

Problem	Cause	Solution
Battery is not charging.	TC51 removed from the cradle too soon.	Replace the TC51 in the cradle. The battery fully charges in approximately six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	TC51 is not inserted correctly in the cradle.	Remove the TC51 and reinsert it correctly. Verify charging is active. Touch ⊞ > ⚙ > ⓘ **About phone** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

5-Slot Ethernet Cradle Troubleshooting

Table 7-5 *Troubleshooting the 5-Slot Ethernet Cradle*

Problem	Cause	Solution
During communication, no data transmits, or transmitted data was incomplete.	TC51 removed from cradle during communications.	Replace TC51 in cradle and retransmit.
	Incorrect cable configuration.	Ensure that the correct cable configuration.
	TC51 has no active connection.	An icon is visible in the status bar if a connection is currently active.
Battery is not charging.	TC51 removed from the cradle too soon.	Replace the TC51 in the cradle. The battery fully charges in approximately six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	TC51 is not inserted correctly in the cradle.	Remove the TC51 and reinsert it correctly. Verify charging is active. Touch ⊞ > ⚙ > ⓘ **About phone** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

4-Slot Battery Charger Troubleshooting

Table 7-6 *Troubleshooting the 4-Slot Battery Charger*

Problem	Cause	Solution
Spare Battery Charging LED does not light when spare battery is inserted.	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charging slot, ensuring it is correctly seated.

Table 7-6 *Troubleshooting the 4-Slot Battery Charger (Continued)*

Problem	Cause	Solution
Spare Battery not charging.	Charger is not receiving power.	Ensure the power cable is connected securely to both the charger and to AC power.
	Spare battery is not correctly seated.	Remove and re-insert the battery into the battery adapter, ensuring it is correctly seated.
	Battery adapter is not seated properly.	Remove and re-insert the battery adapter into the charger, ensuring it is correctly seated.
	Battery was removed from the charger or charger was unplugged from AC power too soon.	Ensure charger is receiving power. Ensure the spare battery is seated correctly. If a battery is fully depleted, it can take up to five hours to fully recharge a Standard Battery and it can take up to eight hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

APPENDIX A TECHNICAL SPECIFICATIONS

This chapter provides technical specification for the TC51.

TC51

Table A-1 *TC51 Technical Specifications*

Item	Description
Physical Characteristics	
Dimensions	Height: 155 mm (6.1 in.) Width: 75.5 mm (2.9 in.) Depth: 18.6 mm (0.73 in.)
Weight	249 g (8.8 oz)
Display	5.0 in. High Definition (1280 x 720); exceptionally bright, outdoor viewable; optically bonded to touch panel
Touch Panel	Dual mode capacitive touch with stylus or bare or gloved fingertip input (conductive stylus sold separately); Corning Gorilla Glass 4
Backlight	Light Emitting Diode (LED) backlight
Battery	Rechargeable 4,300 mAh Li-Ion, Power Precision+; Improved battery technology for longer cycle times and real-time visibility into battery metrics for better battery management; Fast charging (2.4 mA)
Expansion Slot	User accessible microSD up to 32 GB SDHC and up to 128 GB SDXC support
Connection Interface	Universal Serial Bus (USB) 2.0 High Speed (host and client)
Notification	Audible tone; multi-color LEDs, vibration
Voice and Audio	Two microphones support with noise cancellation; vibrate alert; speaker; Bluetooth wireless headset support. High quality speaker phone; PTT headset support; Cellular circuit switch voice; HD Voice

Table A-1   *TC51 Technical Specifications (Continued)*

Item	Description
Performance Characteristics	
CPU	Snapdragon 650 64-bit Hexa-Core 1.8GHz ARM Cortex A72, power optimization
Operating System	Android 6.0.1 Marshmallow with Zebra's Mobility Extensions (Mx) (pre-installed on both AOSP and GMS options)
Memory	Standard: 2 GB RAM/16 GB Flash Optional: 4 GB RAM/32 GB Flash
Output Power	USB - 5 VDC @ 500 mA max
User Environment	
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)
Relative Humidity	Operating: 5 to 95% non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) to tile over concrete over operating temperature range. Multiple 1.5 m (5 ft.) to concrete with Rugged Boot over operating temperature range.
Tumble	500 0.5 m (1.6 ft.) tumbles; meets and exceeds IEC tumble specifications
Electrostatic Discharge (ESD)	+/-15 kVDC air discharge, +/-10 kVDC direct discharge, +/- 10 kVDC indirect discharge
Vibration	4 g's PK Sine (5 Hz to 2 kHz); 0.04g2/Hz Random (20 Hz to 2 kHz); 60 minute duration per axis, 3 axis
Thermal Shock	-40°C to 70°C (-40°F to 158°F) rapid transition
Interactive Sensor Technology (IST)	
Motion Sensor	3-axis accelerometer Gyro; 3-axis accelerometer
Light Sensor	Ambient light sensor to auto adjust display backlight brightness
Proximity Sensor	Automatically detects when the user places the handset against head during a phone call to disable display output and touch input.
Wireless LAN Data and Voice Communications	
Radio	IEEE 802.11 a/b/g/n/ac/d/h/i/r; Wi-Fi™ certified; IPv4, IPv6; 2X2 MIMO
Data Rates Supported	5GHz: 802.11a/n/ac - up to 866.7 Mbps 2.4GHz: 802.11b/g/n - up to 144.4 Mbps

Table A-1   *TC51 Technical Specifications (Continued)*

Item	Description
Operating Channels	Chan 1 - 13 (2412 - 2472 MHz) Chan 36 - 165 (5180 - 5825 MHz) Channel Bandwidth: 20, 40, 80 MHz– Rest of the World Actual operating channels/frequencies depend on regulatory rules and certification agency
Security and Encryption	WEP (40 or 104 bit); WPA/WPA2 Personal (TKIP, and AES); WPA/WPA2 Enterprise (TKIP and AES) — EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0-MSCHAPv2, PEAPv1-EAP-GTC3, EAP Fast3 and LEAP
Certifications	WFA (802.11n, WMM-PS)
Fast Roam	PMKID caching; Cisco CCKM; 802.11r; OKC
Wireless PAN Data and Voice Communications	
Bluetooth	Class 2, Bluetooth v4.1 (Bluetooth Smart technology); Bluetooth Wideband support HFPv1.6; Bluetooth v4.1 Low Energy (LE)
Data Capture Specifications	
2D Imager	SE4710 imager (1D and 2D) with LED aimer.
Camera	Rear — 13 MP autofocus; f/2.4 aperture; rear camera flash LED generates balanced white light; supports Torch mode.
Near Field Communications (NFC)	ISO 14443 Type A and B; F; FeliCa and ISO 15693 cards; P2P mode and Card Emulation via UICC and Host
2D Imager Engine (SE4710) Specifications	
Field of View	Horizontal - 48.0° Vertical - 36.7°
Image Resolution	1280 horizontal X 960 vertical pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles (107,639 lux)
Focal Distance	From front of engine: 17.7 cm (7.0 in.)
Laser Aiming Element	Visible Laser Diode (VLD): 655 nm +/- 10 nm Central Dot Optical Power: 0.6 mW (typical) Pattern Angle: 48.0º horizontal, 38.0º vertical
Illumination System	LEDs: Warm white LED Pattern Angle: 80° at 505 intensity

Table A-2   *Data Capture Supported Symbologies*

Item	Description
1D Bar Codes	Code 128, EAN-8, EAN-13, GS1 DataBar Expanded, GS1 128, GS1 DataBar Coupon, UPCA, Interleaved 2 of 5, UPC Coupon Code
2D Bar Codes	PDF-417, QR Code

Decode Distances

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

Table A-3   *SE4710 Decode Distances*

| Symbol Density/ Bar Code Type | Typical Working Ranges | |
	Near	Far
4 mil Code 39	3.3 in. 8.4 cm	8.8 in. 22.4 cm
5.0 mil Code 128	2.8 in. 7.1 cm	8.2 in. 20.8 cm
5 mil Code 39	2.0 in. 5.08 cm	13.5 in. 34.3 cm
5 mil PDF417	3.1 in. 7.9 cm	8.4 in. 21.3 cm
10 mil Data Matrix	2.9 in. 7.4 cm	10.1 in. 25.7 cm
100% UPCA	1.8 in. 4.6 cm*	26.0 in. 66.0 cm
20 mil Code 39	2.0 in. 5.08 cm*	30.0 in. 76.2 cm
20 mil QR Code	3.2 in. 8.1 cm	15.8 in. 40.1 cm

*Limited by width of bar code in field of view.

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

    Distances measured from front edge of scan engine chassis.
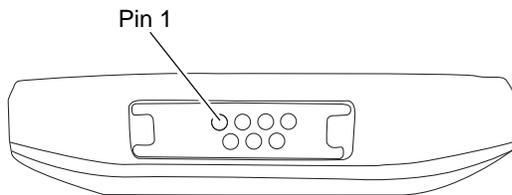
I/O Connector Pin-Outs

Figure A-1   *I/O Connector*

Table A-4   *I/O Connector Pin-Outs*

Pin	Signal	Description
1	VBUS	USB Power Input
2	D-	USB Data-
3	CC	USB Type C Control
4	GND	Ground
5	D+	USB Data+
6	Not Used	Not Used
7	ID	Cradle ID

1-Slot Charge Only Cradle Technical Specifications

Table A-5   *1-Slot Charge Only Cradle Technical Specifications*

Item	Description
Dimensions	Height: 9.9 cm (3.9 in.) Width: 9.8 cm (3.86 in.) Depth: 13.3 cm (5.24 in.)
Weight	378 g (13.3 oz.)
Input Voltage	12 VDC
Power Consumption	up to 15 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)

Table A-5   *1-Slot Charge Only Cradle Technical Specifications*

Item	Description
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10 kV contact +/- 10 kV indirect discharge

4-Slot Charge Only Cradle with Battery Charger Technical Specifications

Table A-6   *5-Slot Charge Only Cradle Technical Specifications*

Item	Description
Dimensions	Height: 10.6 cm (4.17 in.) Width: 48.9 cm (19.25 in.) Depth: 13.3 cm (5.24 in.)
Weight	2020 g (71.3 oz.)
Input Voltage	12 VDC
Power Consumption	up to 95 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)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

5-Slot Charge Only Cradle Technical Specifications

Table A-7   *5-Slot Charge Only Cradle Technical Specifications*

Item	Description
Dimensions	Height: 10.6 cm (4.17 in.) Width: 48.9 cm (19.25 in.) Depth: 13.3 cm (5.24 in.)
Weight	1937 g (68 oz.)
Input Voltage	12 VDC
Power Consumption	up to 65 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)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

5-Slot Ethernet Cradle Technical Specifications

Table A-8   *5-Slot Ethernet Cradle Technical Specifications*

Item	Description
Dimensions	Height: 10.6 cm (4.17 in.) Width: 48.9 cm (19.25 in.) Depth: 13.3 cm (5.24 in.)
Weight	2010 g (71 oz.)
Input Voltage	12 VDC
Power Consumption	up to 70 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)

Table A-8   *5-Slot Ethernet Cradle Technical Specifications*

Item	Description
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

4-Slot Battery Charger Technical Specifications

Table A-9   *4–Slot Battery Charger Technical Specifications*

Item	Description
Dimensions	Height: 9.7 cm (3.82 in.) Width: 9.8 cm (3.86 in.) Depth: 13.3 cm (5.24 in.)
Weight	450 g (15.9 oz.)
Input Voltage	12 VDC
Power Consumption	up to 48 watts
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

Trigger Handle Technical Specifications

Table A-10   *Trigger Handle Technical Specifications*

Item	Description
Dimensions	Height: 11.5 cm (4.53 in.) Width: 13.2 cm (5.19 in.) Depth: 8.0 cm (3.15 in.)
Weight	114 g (4.0 oz.)
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	10% to 95% non-condensing
Drop	1.8 m (6 feet) drops to concrete over temperature range.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

Rugged Charge/USB Cable Technical Specifications

Table A-11   *Rugged Charge/USB Cable Technical Specifications*

Item	Description
Length	164 +/- 6 cm (64.6 +/- 2.4 in.)
Input Voltage	5.0 VDC
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

INDEX

T

ZEBRA