TC70
INTEGRATOR GUIDE

Copyrights

Disclaimer

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

Trademarks

Revision History

Changes to the original guide are listed below:

Change	Date	Description
A01 Rev. A	10/2014	Initial release.
A02 Rev. A	04/2015	Zebra rebranding.
A02 Rev. B	02/2016	Correct mounting bracket part number.
A03 Rev. A	03/2018	Update approved cleanser active ingredients.

Contents

About This Guide

Introduction

This guide provides information about using the TC70 mobile computer and accessories.

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

Documentation Set

The documentation set for the TC70 provides information for specific user needs, and includes:

- *TC70 Quick Start Guide* - describes how to get the TC70 up and running.
- *TC70 User Guide* - describes how to use the TC70.
- *TC70 Integrator Guide* - describes how to set up the TC70 and accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
TC70	WLAN: 802.11 a/b/g/n WPAN: Bluetooth v4.0 Low Energy	4.7" High Definition (1280 x 720) LCD	1 GB RAM / 8 GB Flash (SLC High Reliability Flash)	2D imager and integrated NFC	Android-based, Android Open-Source Project 4.4.2.

Software Versions

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

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

Chapter Descriptions

Topics covered in this guide are as follows:

- *Getting Started on page 17* provides information on getting the TC70 up and running for the first time.
- *Accessories on page 27* describes the available accessories and how to use them with the TC70.

- *USB Communication on page 65* describes how to connect the TC70 to a host computer using USB.
- *DataWedge Configuration on page 67* describes how to use and configure the DataWedge application.
- *Administrator Utilities on page 101* provides information for using the suite of administrative tools for configuring the TC70.
- *Settings on page 123* provides the settings for configuring the TC70.
- *Application Deployment on page 133* provides information for developing and managing applications.
- *Maintenance and Troubleshooting on page 151* includes instructions on cleaning and storing the TC70, and provides troubleshooting solutions for potential problems during TC70 operation.
- *Technical Specifications on page 161* provides the technical specifications for the TC70.

Notational Conventions

The following conventions are used in this document:

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

Icon Conventions

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

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

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

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

Related Documents

- *TC70 Quick Start Guide*, p/n MN000976Axx.
- *TC70 Regulatory Guide*, p/n MN000977Axx.

- *TC70 User Guide*, p/n MN001120Axx.

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 Global 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

Figure 1: Manufacturing Label
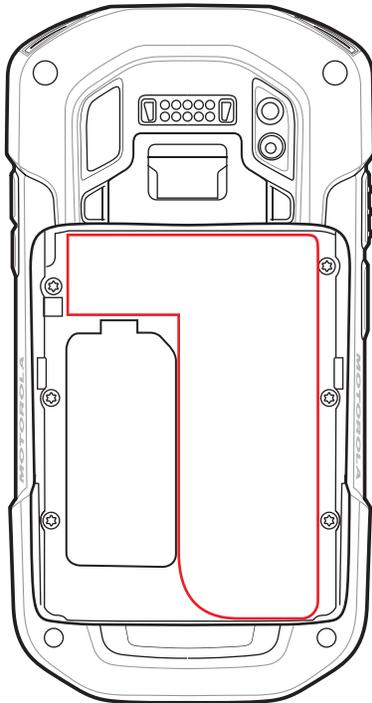
Customer Support responds to calls by email or telephone within the time limits set forth in support agreements.

If the problem cannot be solved by Global 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

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

Setup

When and where to use: Perform this procedure to start using the TC70 for the first time.

Procedure:

1 Install a micro secure digital (SD) card (optional).
2 Install hand strap (optional).
3 Install the battery.
4 Charge the TC70.
5 Power on the TC70.

Installing a microSD Card

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

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

Procedure:

1 Remove the hand strap, if installed.
2 Lift the access door.

Figure 2: Lift Access Door
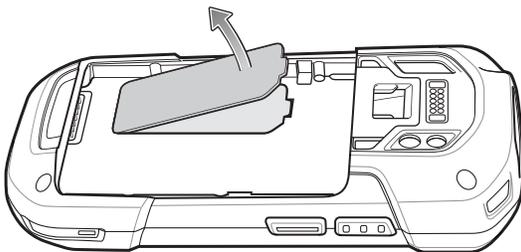
3 Insert the microSD card into the card holder door ensuring that the card slides into the holding tabs on each side of the door.

4 Re-install the access door.

Installing the Hand Strap and Battery

Note: Installation of the hand strap is optional. Skip this section if not installing the hand strap.

Procedure:

1 Remove the hand strap filler from the hand strap slot.

Figure 3: Remove Filler
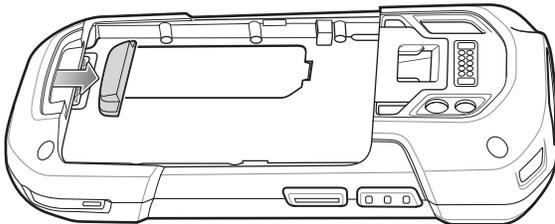
2 Insert the hand strap plate into the hand strap slot.

Figure 4: Insert Hand Strap
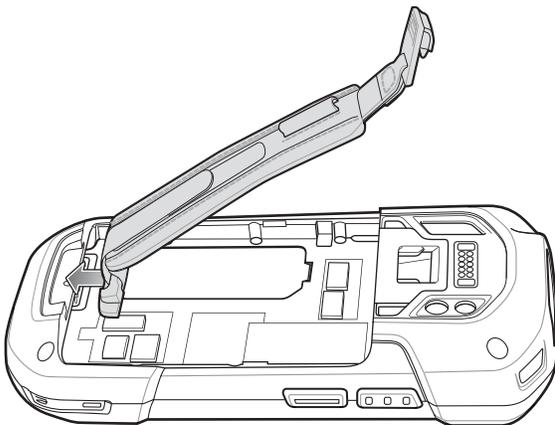
3 Insert the battery, bottom first, into the battery compartment in the back of the TC70.

Figure 5: Insert Bottom of Battery into Battery Compartment
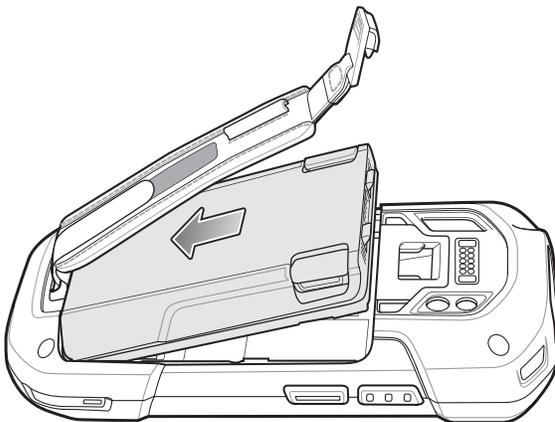
4 Rotate the top of the battery into the battery compartment.
5 Press the battery down into the battery compartment until the battery release latches snap into place.

Figure 6: Press Down on Battery
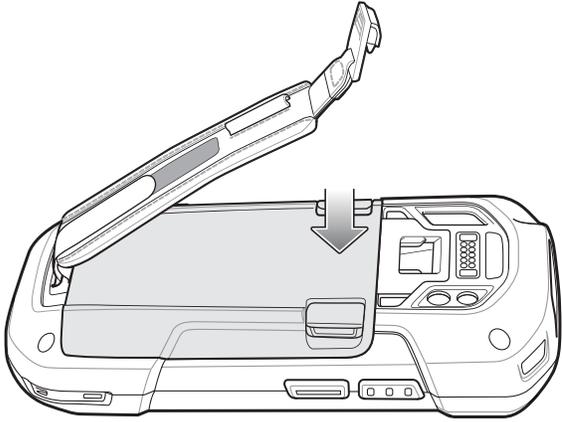
6 Place hand strap clip into hand strap mounting slot and pull down until it snaps into place.

Figure 7: Secure Hand Strap Clip
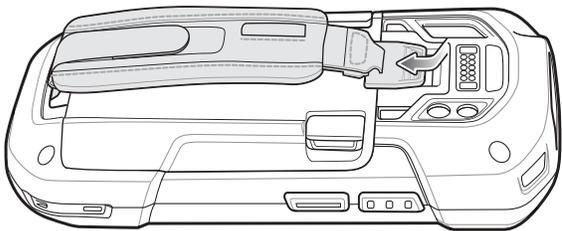
Installing the Battery

Procedure:

1 Insert the battery, bottom first, into the battery compartment in the back of the TC70.

Figure 8: Insert Bottom of Battery into Battery Compartment
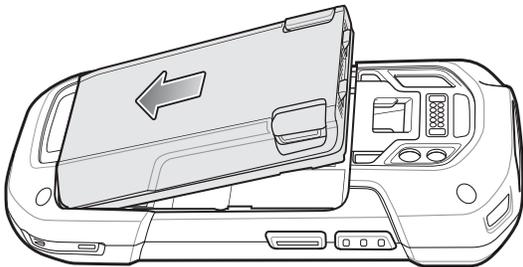
2 Rotate the top of the battery into the battery compartment.

Figure 9: Rotate Battery into Battery Compartment
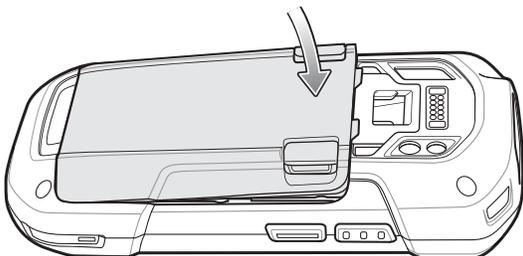
3 Press the battery down into the battery compartment until the battery release latches snap into place.

Figure 10: Press Down on Battery
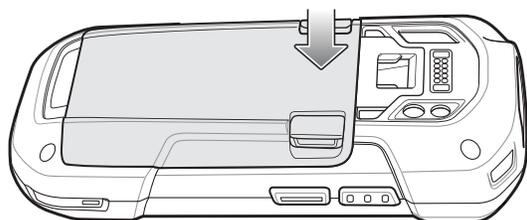
Charging the Battery

Before using the TC70 for the first time, charge the main battery until the green Charging/Notification light emitting diode (LED) remains lit. To charge the TC70, use a cable or a cradle with the appropriate power supply. For information about the accessories available for the TC70, see *Accessories on page 27* for more information.

- Snap-On USB Cable
- Charging Cable Cup
- 2-Slot Charge Only Cradle
- 2-Slot USB/Ethernet Cradle
- 5-Slot Charge Only Cradle
- 5-Slot Ethernet Cradle.

The 4,620 mAh battery fully charges in approximately six hours at room temperature.

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC70 or accessory always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC70 or accessory may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC70 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

Procedure:

1 To charge the main battery, connect the charging accessory to the appropriate power source.

2 Insert the TC70 into a cradle or attach to a cable. The TC70 turns on and begins charging. The Charging/ Notification LED blinks amber while charging, then turns solid green when fully charged.

Charging Indicators

Table 1: Charging/Notification LED Charging Indicators

State	Indication
Off	TC70 is not charging. TC70 is not inserted correctly in the cradle or connected to a power source. Charger/cradle is not powered.
Slow Blinking Amber (1 blink every 2 seconds)	TC70 is charging.
Solid Green	Charging complete.
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).

State	Indication
Slow Blinking Red (1 blink every 2 seconds)	TC70 is charging and battery is at end of useful life.
Solid Red	Charging complete and battery is at end of useful life.
Fast Blinking Red (2 blinks/second)	Charging error and 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

Procedure:

1 Press and hold the Power button until the menu appears.
2 Touch **Power off**.
3 If hand strap is attached, slide the hand strap clip up toward the top of the TC70 and then lift.

Figure 11: Remove Hand Strap Clip
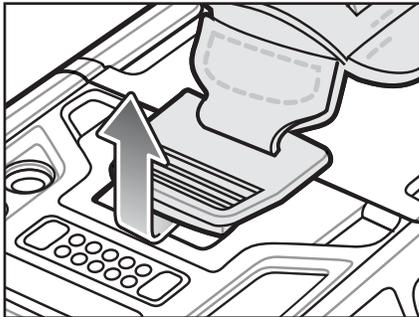
4 Press the two battery latches in.

Figure 12: Press Battery Latches

5   Lift the battery from the TC70.

Figure 13: Lift the Battery
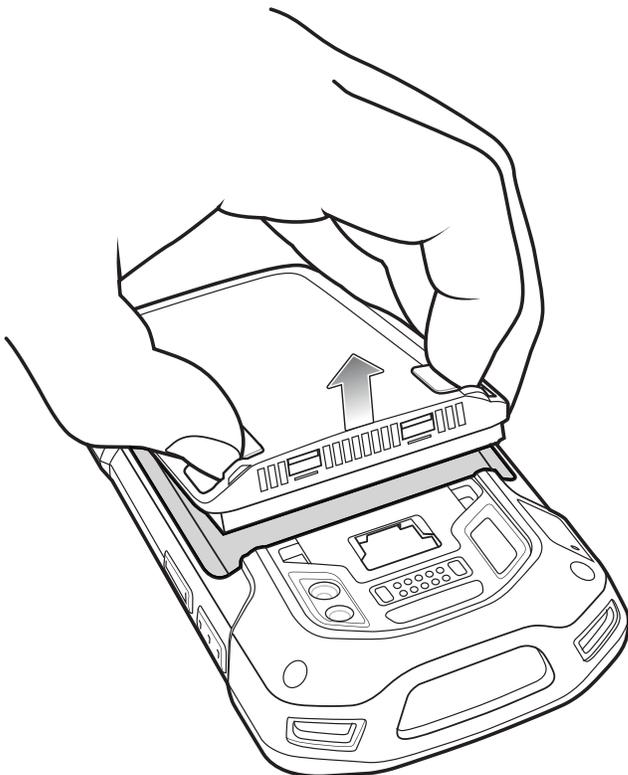
6   Insert the replacement battery, bottom first, into the battery compartment in the back of the TC70.

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

8   Replace the hand strap, if required.

9 Press and hold the Power button to turn on the TC70.

Replacing the microSD Card

Procedure:

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

2 Touch **Power off**.

3 If hand strap is attached, slide the hand strap clip up toward the top of the TC70 and then lift.

Figure 14: Remove Hand Strap Clip
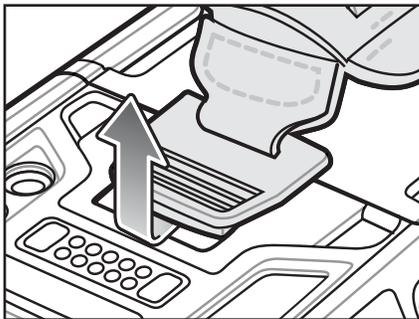
4 Press the two battery latches in.

5 Lift the battery from the TC70.

6 Lift the access door.

Figure 15: Remove Access Door
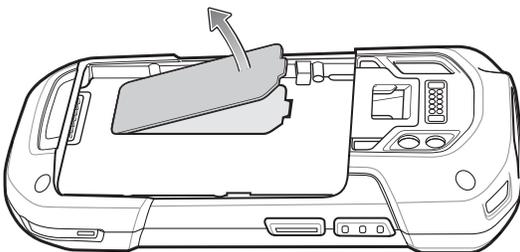
7 Remove microSD card from holder.

8 Insert the replacement microSD card.

9 Replace the access door.

Figure 16: Replace Access Door
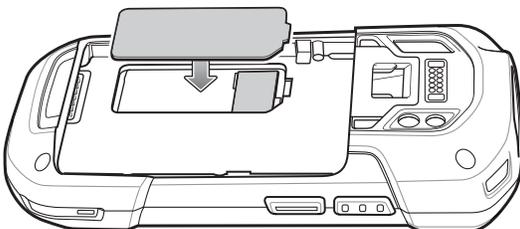
10 Insert the replacement battery, bottom first, into the battery compartment in the back of the TC70.

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

12 Replace the hand strap, if required.

13 Press and hold the Power button to turn on the TC70.

Resetting the TC70

There are four reset functions:

- Soft reset
- Hard reset
- Enterprise reset
- Factory reset.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

Procedure:

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

2 Touch **Reset**.

3 The device reboots.

Performing a Hard Reset

> **Caution:** Performing a hard reset with a SD card installed in the TC70 may cause damage or data corruption to the SD card.

Perform a hard reset if the TC70 stops responding.

Procedure:

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

Figure 17: Three Button Reset
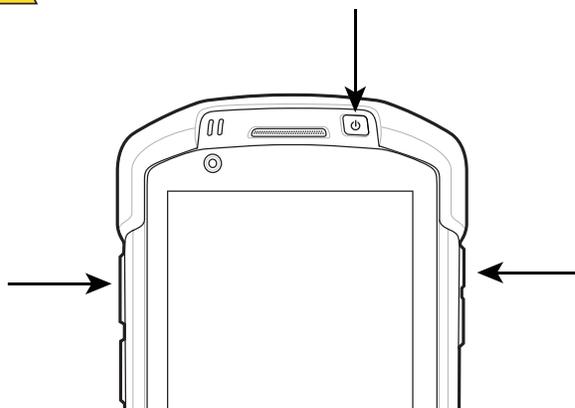
2 When the screen turns off, release the buttons.

3 The TC70 reboots.

Performing an Enterprise Reset

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

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

Procedure:

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

2   Copy the T700HKXXXREENxyyzz.zip file to the root of the microSD card or the root of the Internal Storage. See *USB Communication on page 65*.

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

4   Touch **Reset**.

5   Touch **OK**. The TC70 resets.

6   Press and hold the Scan button.

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

Figure 18: System Recovery Screen
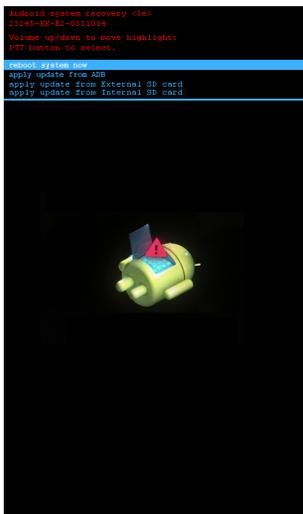
8   Press the Up and Down Volume buttons to navigate to the **apply update from sdcard** or **apply from Internal SD card** option.

9   Press the PTT button.

10 Press the Up and Down Volume buttons to navigate to the T700HKXXXREENxyyzz.zip file.

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

Performing a Factory Reset

A Factory Reset erases all data in the /cache, /data and /enterprise partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See *TC70 System Update on page 138* for more information.

Procedure:

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

2   Copy the TC700HKXXXRFENxyyzz file to the root of the microSD card or the root of Internal Storage. See *USB Communication on page 65*.

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

4   Touch **Reset**.

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

6   Press and hold the Scan button.

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

Figure 19: System Recovery Screen
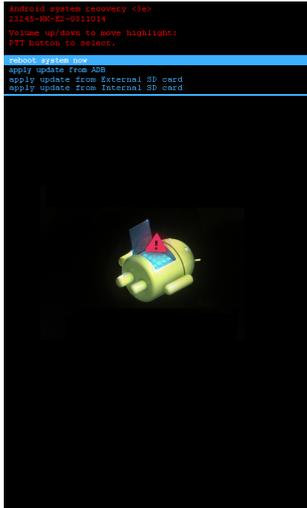
8 Press the Up and Down volume buttons to navigate to the **apply update from sdcard** or **apply from Internal SD card** option.

9 Press the PTT button.

10 Press the Up and Down Volume buttons to navigate to the `TC700HKXXXRFENxyyzz` file.

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

Chapter

2

Accessories

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

Accessories

This table lists the accessories available for the TC70.

Table 2: TC70 Accessories

Accessory	Part Number	Description
Cradles		
2-Slot Charge Only Cradle	CRD-TC7X-SEC2U1–01	Provides device and spare battery charging. Use with power supply, p/n PWRS-14000-148R.
2-Slot USB/Ethernet Cradle	CRD-TC7X-SE2EU1–01	Provides device and spare battery charging and USB communication with a host computer and Ethernet communication with a network. Use with power supply, p/n PWRS-14000-148R.
5-Slot Charge Only Cradle	CRD-TC7X-SE5C1-01	Charges up to five devices. Use with power supply, p/n PWRS-14000-241R and DC line cord, p/n 50-16002-029R. Can accommodate one 4-Slot Battery Charger using the Battery Adapter Cup.
5-Slot Ethernet Cradle	CRD-TC7X-SE5EU1–01	Provides device charging and provides Ethernet communication for up to five devices. Use with power supply, p/n PWRS-14000-241R and DC line cord, p/n 50-16002-029R.
Chargers		
4-Slot Spare Battery Charger	SAC-TC7X-4BTYC1-01	Charges up to four battery packs. Use with power supply, p/n PWRS-14000-148R.
Power Supply	PWRS-14000-249R	Provides power to the device using the Snap-On USB Cable or Snap-On Charging Cable Cup.
Power Supply	PWRS-14000-148R	Provides power to the 4-Slot Spare Battery Charger.
Power Supply	PWRS-14000-241R	Provides power to the 5-Slot Charge Only cradle and the 5-Slot Ethernet Cradle. Requires DC Line Cord, p/n 50–16002–029R.
Snap-On USB Cable	CBL-TC7X-CBL1-01	Provides power to the device and USB communication with a host computer. Use with power supply, p/n PWRS-14000-249R.

Table continued…

Accessory	Part Number	Description
Charging Cable Cup	CHG-TC7X-CBL1-01	Provide power to the device. Use with power supply, p/n PWRS-14000-249R.
DC Line Cord	50-16002-029R	Provides power from the power supply to the 5-Slot Charge Only Cradle and 5-Slot Ethernet Cradle.
Miscellaneous		
4,620 mAh battery	BTRY-TC7X-46MA2-01	Replacement battery (single pack).
	BTRY-TC7X-46MA2-10	Replacement battery (10–pack).
Magnetic Stripe Reader	MSR-TC7X-SNP1-01	Captures data from magnetic stripe cards.
Audio Adapter	ADP-TC7X-AUDIO1–01	Snaps onto the device and provides audio to a wired headset with 2.5 mm plug.
Hand Strap	SG-TC7X-HSTRP1-03	Replacement hand strap with hand strap mounting clip (3–pack).
Stylus	SG-TC7X-STYLUS1–03	Stylus for use with device. (3–pack).
Holster	SG-TC7X-HLSTR1–01	Soft holster for added protection.
Mounting Bracket	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.
Battery Adapter Cup	CUP-SE-BTYADP1–01	Provides mounting for the 4-Slot Battery Charger on the 5-Slot Charge Only Cradle and 5-Slot Ethernet Cradle.
Screen Protector	SG-TC7X-SCRNP-01	Provides additional protection for the screen (3–pack).
Trigger Handle	TRG-TC7X-SNP1-01	Add a gun-style handle with a scanning trigger for comfortable and productive data capture.

2-Slot Charge Only Cradle

The 2-Slot Charge Only Cradle:

- Provides 5 VDC power for operating the device.
- Charges the device's battery.
- Charges a spare battery.

Figure 20: 2–Slot Charge Only Cradle
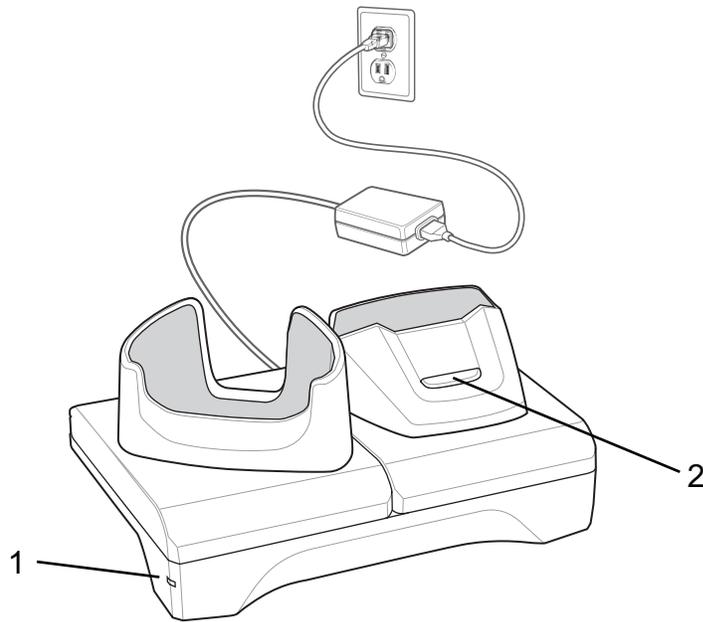
1	Power LED – Lights green indicating that the cradle is receiving power.
2	Spare battery Charging LED

Setup

Figure 21: 2–Slot Charge Only Cradle
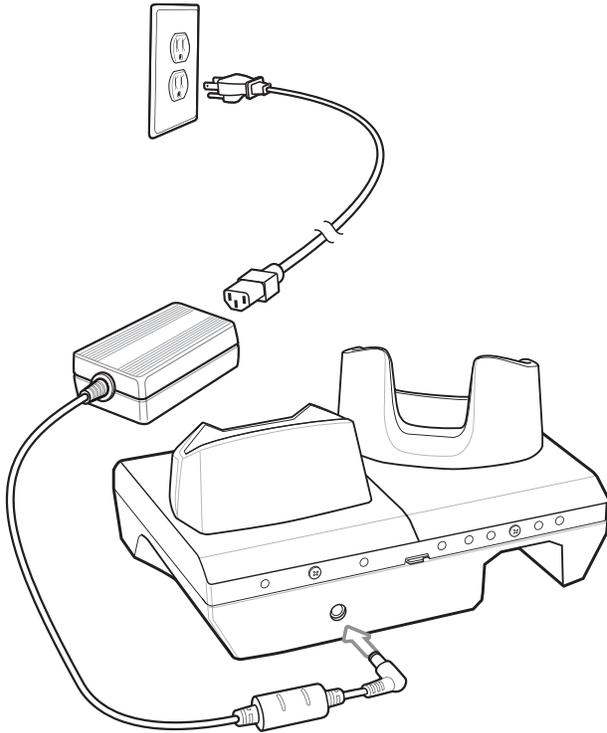
Charging the Device

Procedure:

1 Insert the device into the slot to begin charging.

Figure 22: Battery Charging
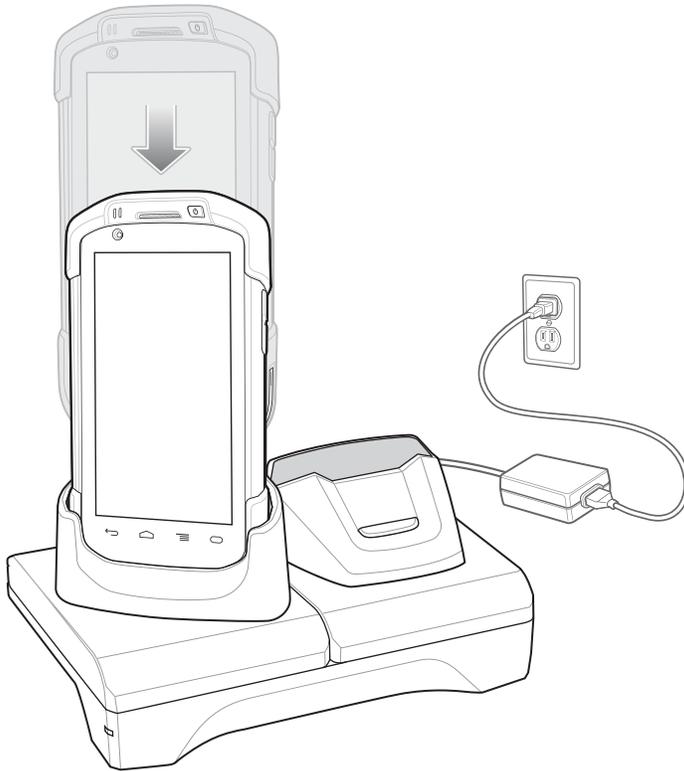
2 Ensure the device is seated properly.

Charging the Spare Battery

Procedure:

1 Insert the battery into the right slot to begin charging.

Figure 23: Spare Battery Charging
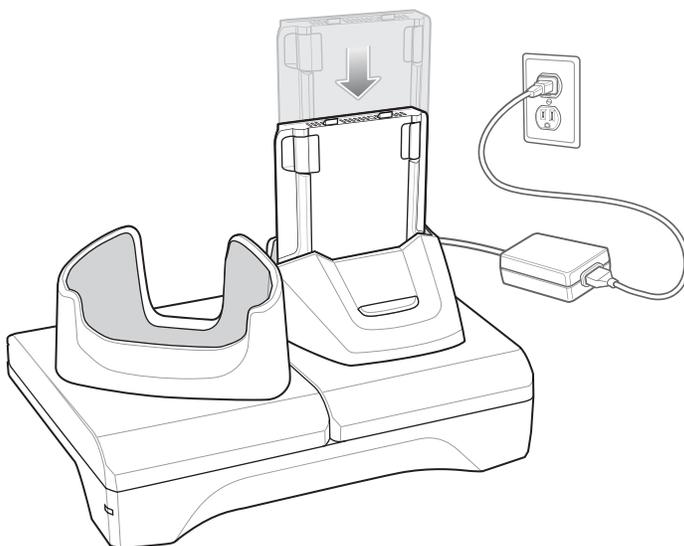
2 Ensure the battery is seated properly.

Battery Charging

Main Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device.

The 4,620 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 4,620 mAh battery fully charges in less than six hours at room temperature.

Table 3: Spare Battery Charging LED Indicators

LED	Indication
Slow Blinking Amber	Spare battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Slow Blinking Red	Spare battery is charging and battery is at the end of useful life.
Solid Red	Charging complete and battery is at the end of useful life.
Fast Blinking Red	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.

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.

2-Slot USB/Ethernet Cradle

The 2-Slot USB/Ethernet Cradle:

- Provides 5.0 VDC power for operating the device.
- Charges the device's battery.
- Charges a spare battery.
- Connects the device to an Ethernet network.
- Provides communication to a host computer using a USB cable.

Note: Remove all attachments on the device, except the hand strap, before place onto the cradle.

Figure 24: 2-Slot USB/Ethernet Cradle
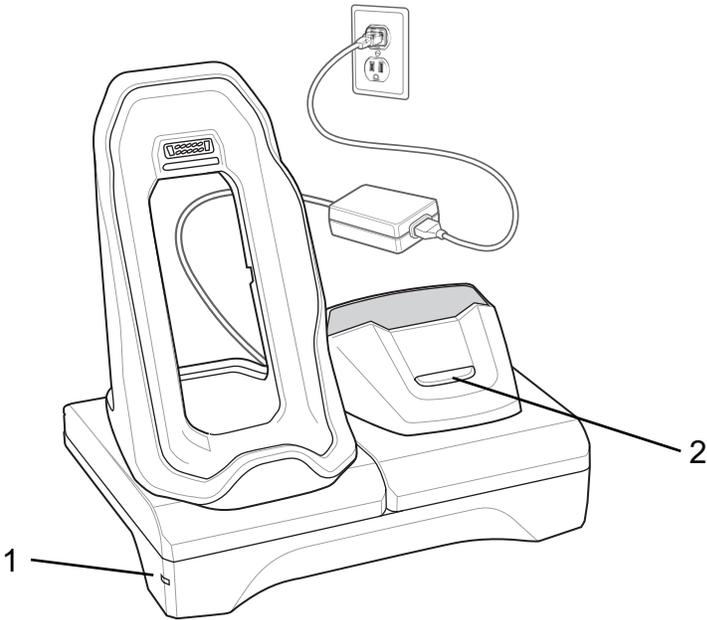
1	Power LED – Lights green indicating that the cradle is receiving power.
2	Spare Battery Charging LED

Setup

Figure 25: 2–Slot USB/Ethernet Cradle
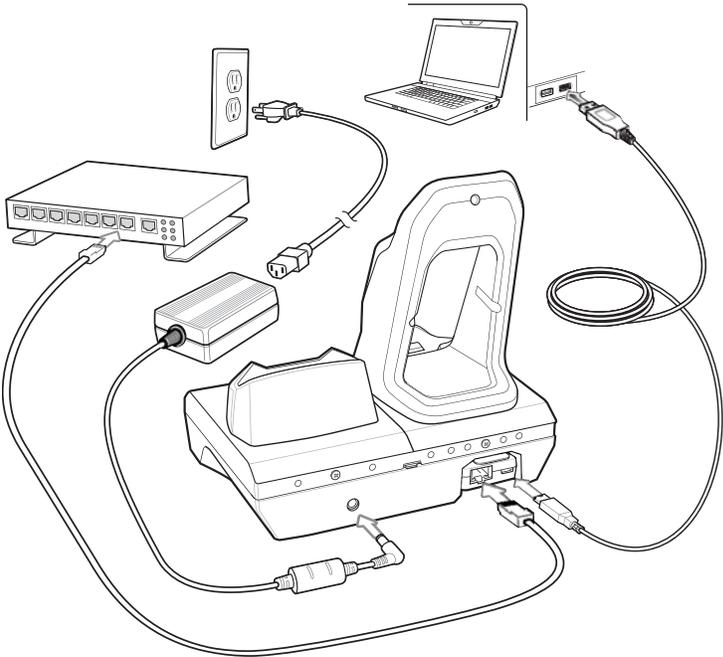
Charging the Device

Procedure:

1 Place the bottom of the device into the base.

   Figure 26: Battery Charging
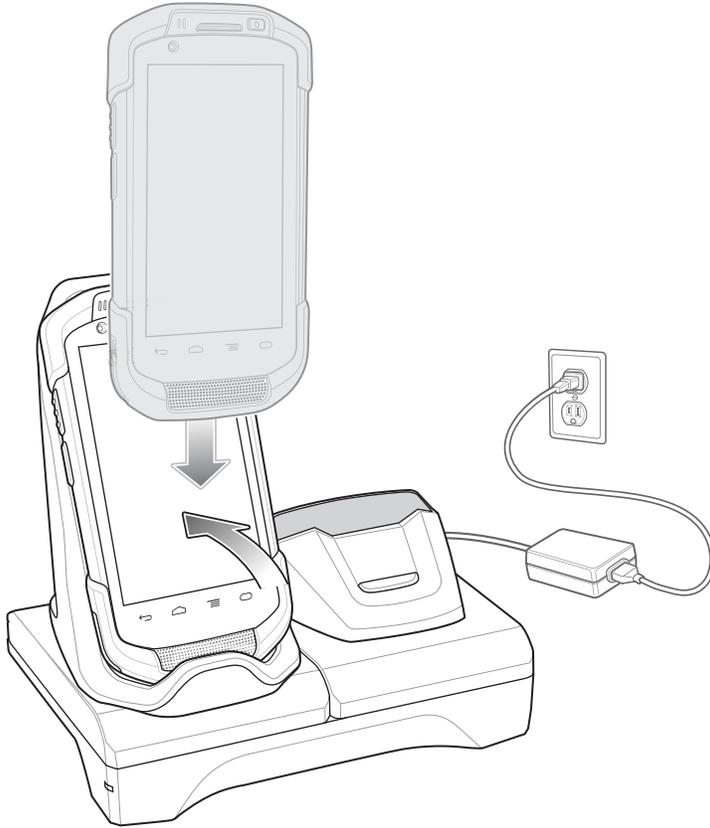
2 Rotate the top of the device until the connector on the back of the device mates with the connector on the cradle.

3 Ensure the device is connected properly. The charging Charging/Notification LED on the device begins blinking amber indicating that the device is charging.

Charging the Spare Battery

Procedure:

1 Insert the battery into the right slot to begin charging.

Figure 27: Spare Battery Charging

2   Ensure the battery is seated properly.

Battery Charging

Main Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device.

The 4,620 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 4,620 mAh battery fully charges in less than six hours at room temperature.

Table 4: Spare Battery Charging LED Indicators

LED	Indication
Slow Blinking Amber	Spare battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Slow Blinking Red	Spare battery is charging and battery is at the end of useful life.
Solid Red	Charging complete and battery is at the end of useful life.
Fast Blinking Red	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.

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.

USB/Ethernet Communication

The 2–Slot USB/Ethernet Cradle provides both Ethernet communication with a network and USB communication with a host computer. Prior to using the cradle for Ethernet or USB communication. Ensure that the switch on the USB/Ethernet module is set properly.

Turn the cradle over to view the module.

Figure 28: 2–Slot USB/Ethernet Cradle Module Switch
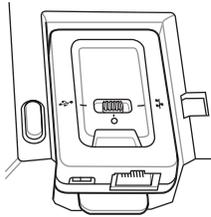
For Ethernet communication, slide the switch to the position.

For USB communication, slide the switch to the position.

Place the switch in the center position ⬤ to disable communications.

Ethernet LED Indicators

There are two LEDs on the USB/Ethernet Module RJ-45 connector. The green LED lights to indicate that the transfer rate is 100 Mbps. When the LED is not lit the transfer rate is 10 Mbps. The yellow LED blinks to indicate activity, or stays lit to indicate that a link is established. When it is not lit it indicates that there is no link.

Figure 29: LED Indicators
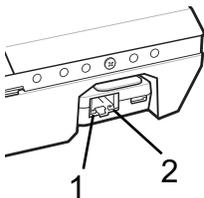
Table 5: USB/Ethernet Module LED Data Rate Indicators

Data Rate	(1) Yellow LED	(2) Green LED
100 Mbps	On/Blink	On
10 Mbps	On/Blink	Off

Ethernet Settings

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The TC70 includes Ethernet cradle drivers. After the TC70, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch **Ethernet**.

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

5 Place the TC70 into the Ethernet cradle slot.

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

7 Touch **Modify Proxy**.

Figure 30: Ethernet Proxy Settings

8 Touch the **Proxy settings** drop-down list and select **Manual**.

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

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

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

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

12 Touch **Modify**.

13 Touch ⌂.

Configuring Ethernet Static IP Address

The TC70 includes Ethernet cradle drivers. After the TC70, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch **Ethernet**.

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

5 Place the TC70 into the Ethernet cradle slot.

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

7   Touch **Disconnect**.

Figure 31: Ethernet Proxy Settings
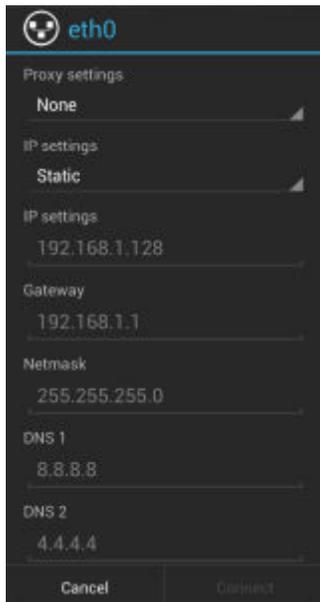
eth0

Proxy settings

None

IP settings

Static

IP settings

192.168.1.128

Gateway

192.168.1.1

Netmask

255.255.255.0

DNS 1

8.8.8.8

DNS 2

4.4.4.4

Cancel   Connect

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

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

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

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

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

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

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

15 Touch **Connect**.

16 Touch ⌂.

5-Slot Charge Only Cradle

The 5-Slot Charge Only Cradle:

• Provides 5 VDC power for operating the TC70.

• Simultaneously charges up to five TC70s and up to four TC70s and on 4-Slot Battery Charger using the Battery Charger Adapter.

• Consists of a cradle base and cups that can be configured for various charging requirements.

Figure 32: 5-Slot Charge Only Cradle
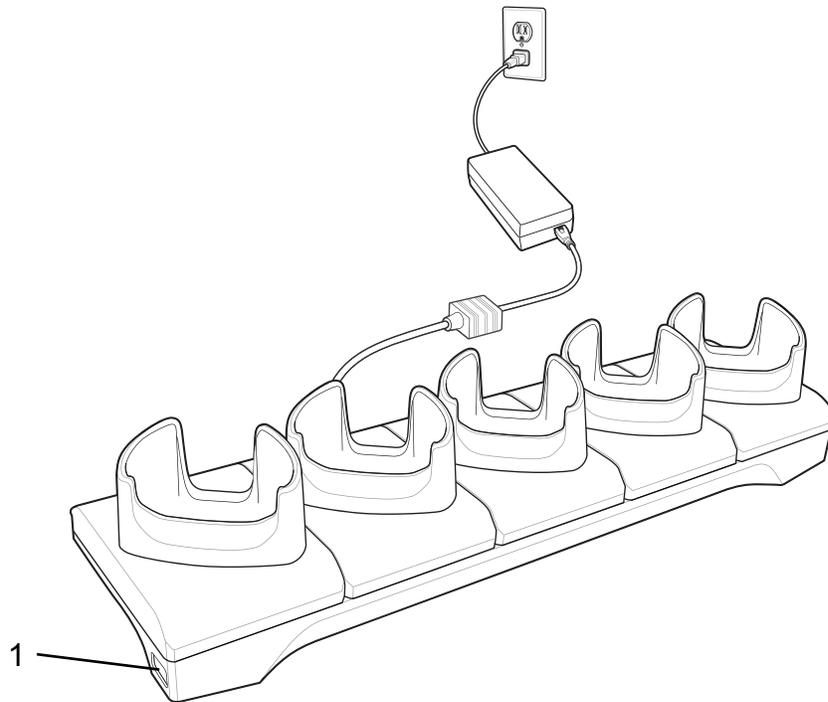
1	Power LED – Lights green when power is applied to cradle.

Setup

Figure 33: 5-Slot Charge Only Cradle
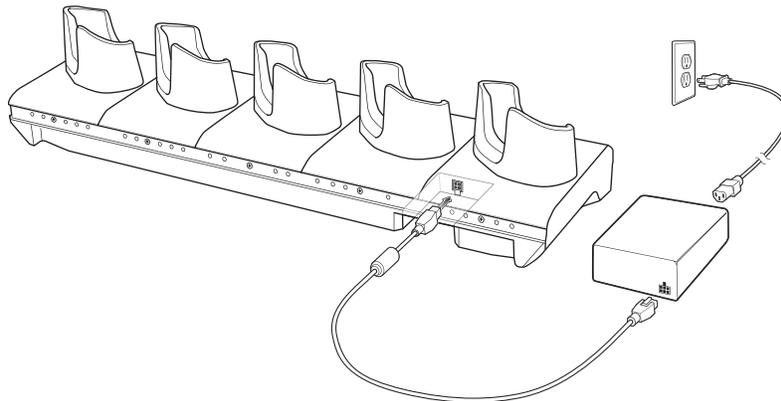
Charging the TC70

Procedure:

1 Insert the TC70 into a slot to begin charging.

Figure 34: TC70 Battery Charging
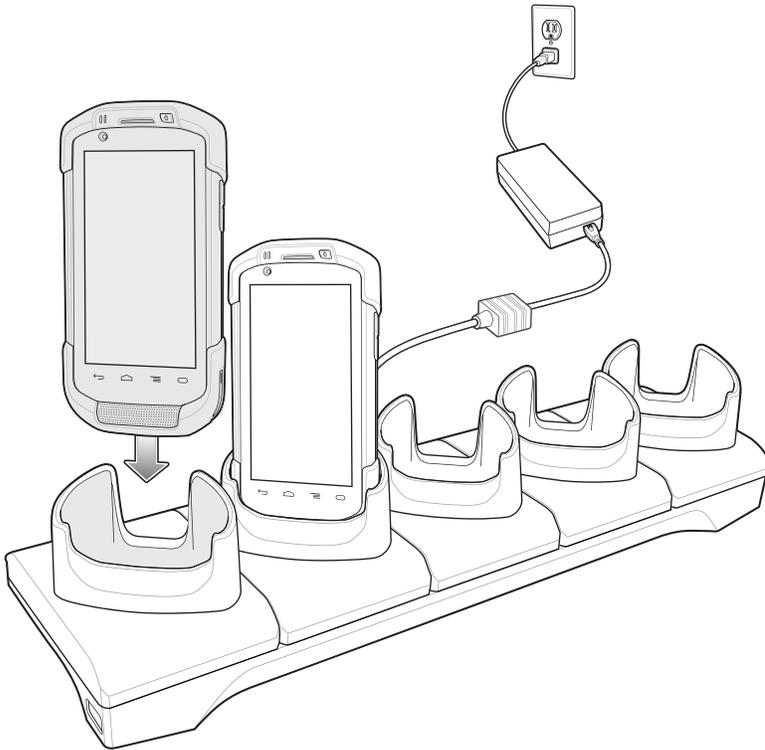
Figure 35: 5-Slot Charge Only Cradle with Four Slot Battery Charger
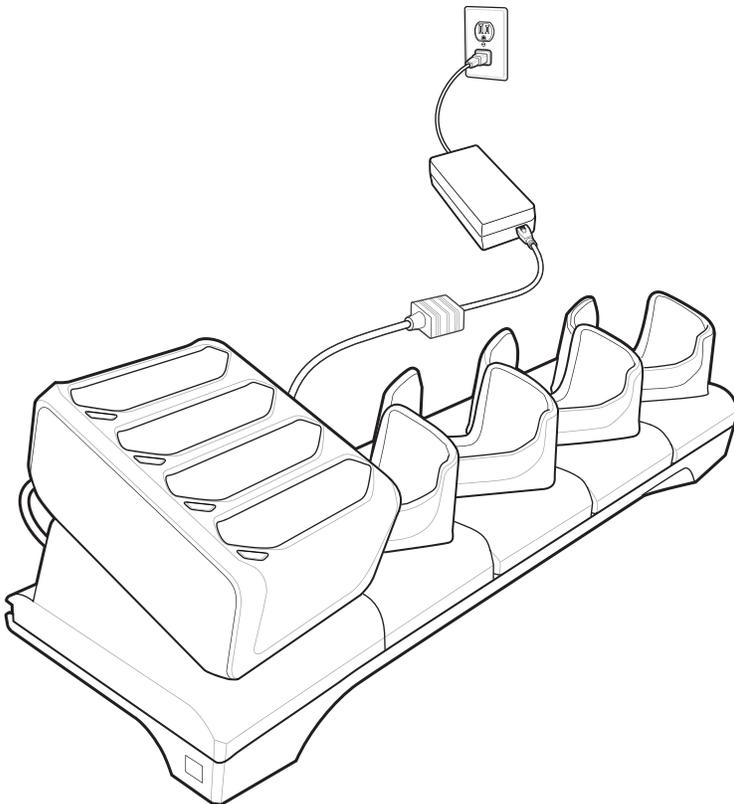
2 Ensure the TC70 is seated properly.

Battery Charging

Main Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device.

The 4,620 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 always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the device may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device indicates when charging is disabled due to abnormal temperatures via its LED.

Installing the Four Slot Battery Charger

Note: The Battery Charger must be installed in the first slot only.

Procedure:

1 Remove power from the cradle.

Figure 36: Remove Power from Cradle
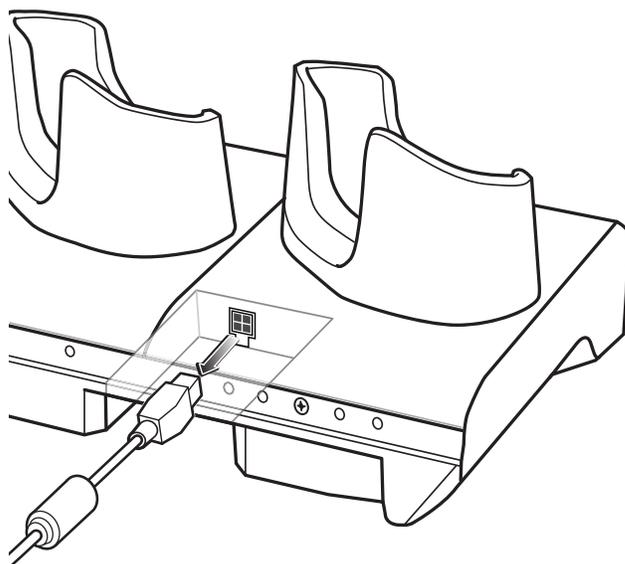
2 Using a Phillips screwdriver, remove the screw securing the cup to the cradle base.

Figure 37: Remove Screw
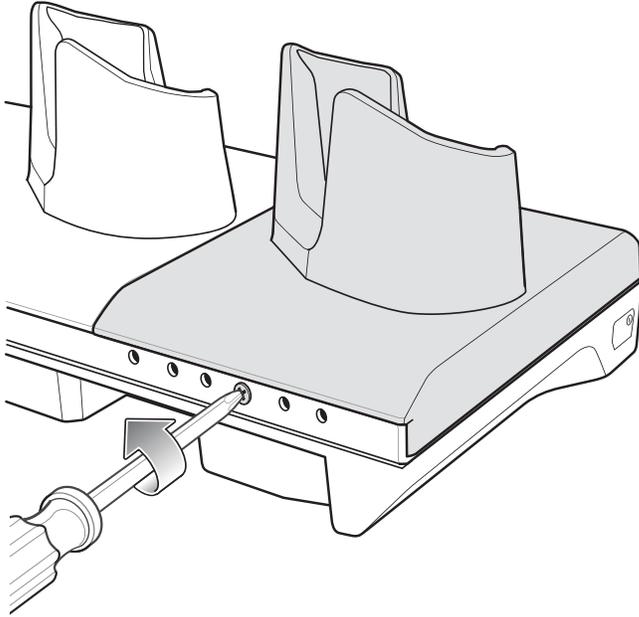
3 Slide the cup to the front of the cradle.

Figure 38: Remove Cup
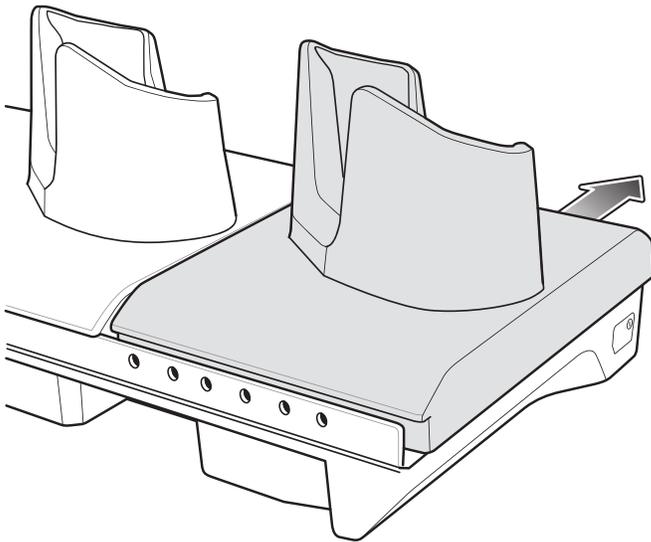
4 Carefully lift the cup up to expose the cup power cable.

5 Disconnect the cup power cable.

Figure 39: Disconnect Cup Power Cable
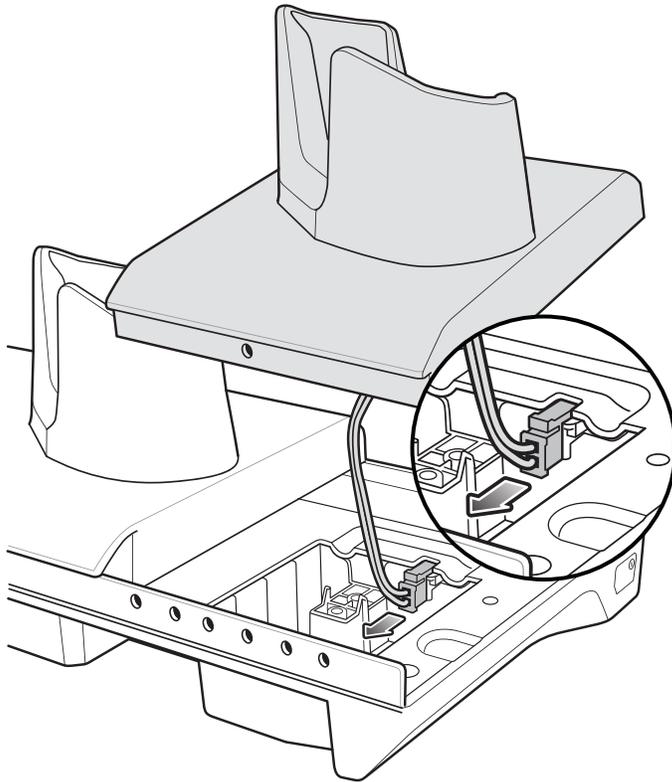
6   **Note:** Place power cable into adapter to avoid pinching cable.

Connect the Battery Adapter power cable to the connector on the cradle.

Figure 40: Connect Adapter Power Cable
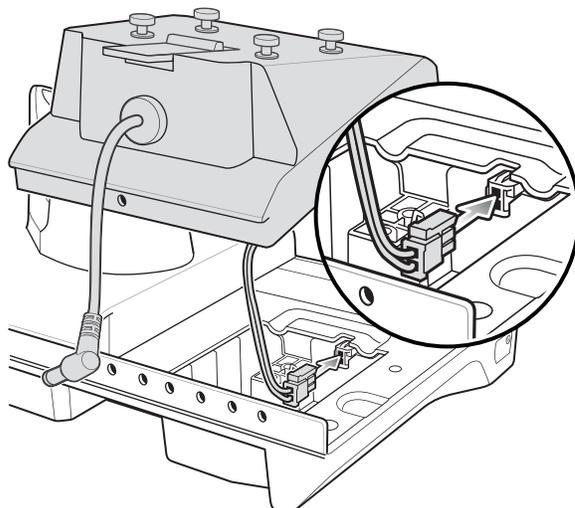
7 Place adapter onto cradle base and slide toward rear of cradle.

Figure 41: Install Adapter
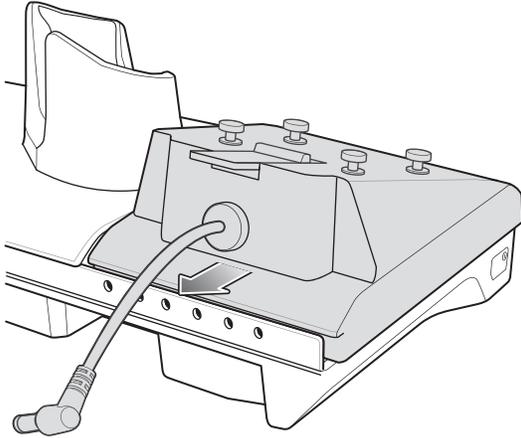
8 Using a Phillips screwdriver, secure adapter to cradle base with screw.

Figure 42: Secure adapter to Cradle
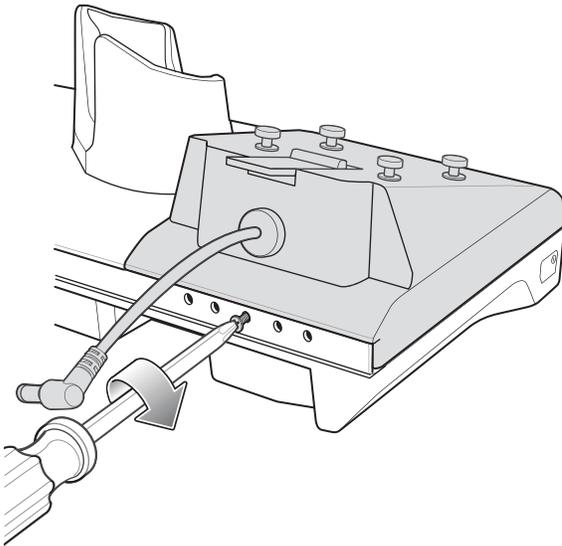
9 Align mounting holes on the bottom of the Four Slot Battery Charger with the stubs on the Battery Adapter.

Figure 43: Install Four Slot Battery Charger
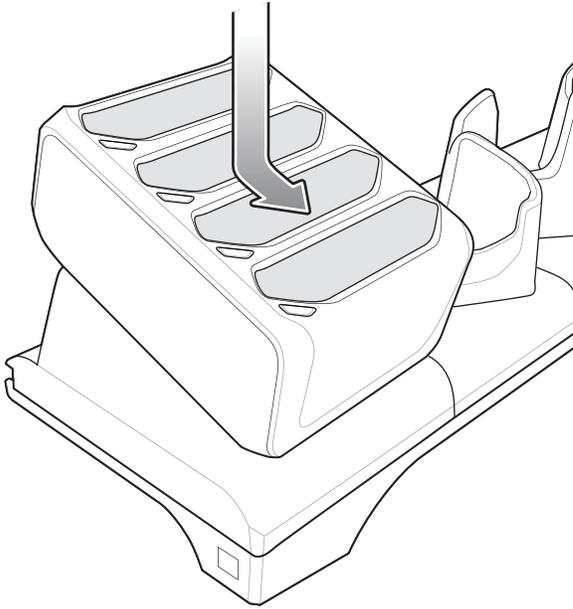
10 Slide the Four Slot battery Charger down toward the front of the cradle.

11 Connect the output power plug into the power port on the Four Slot Battery Charger.

Figure 44: Connect Adapter Power Cable
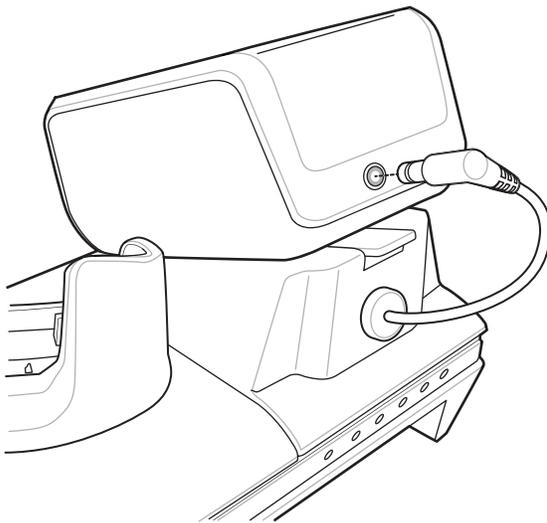
Removing the 4-Slot Battery Charger

Procedure:

1 Disconnect the output power plug from the 4-Slot Battery Charger.

2 At the back of the cup, press down on the release latch.

Figure 45: Press Release Latch
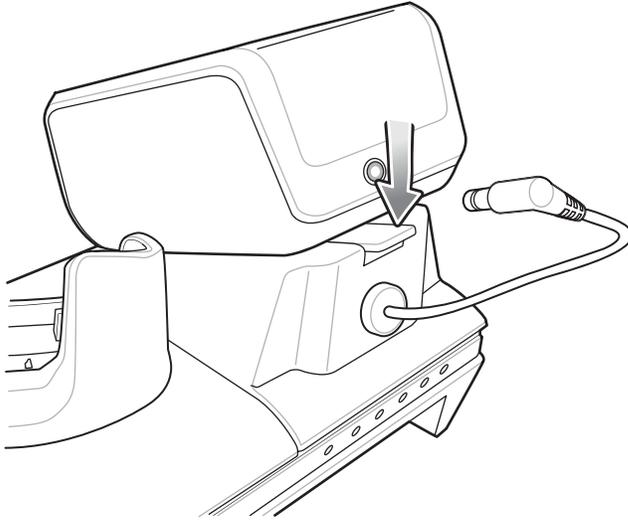
3 Slide the 4-Slot Battery Charger toward the front of the cradle.

4 Lift the 4-Slot off the cradle cup.

5-Slot Ethernet Cradle

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 151*.

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 TC70s and up to fourTC70s and on 4-Slot Battery Charger using the Battery Charger Adapter.

Figure 46: 5-Slot Ethernet Cradle
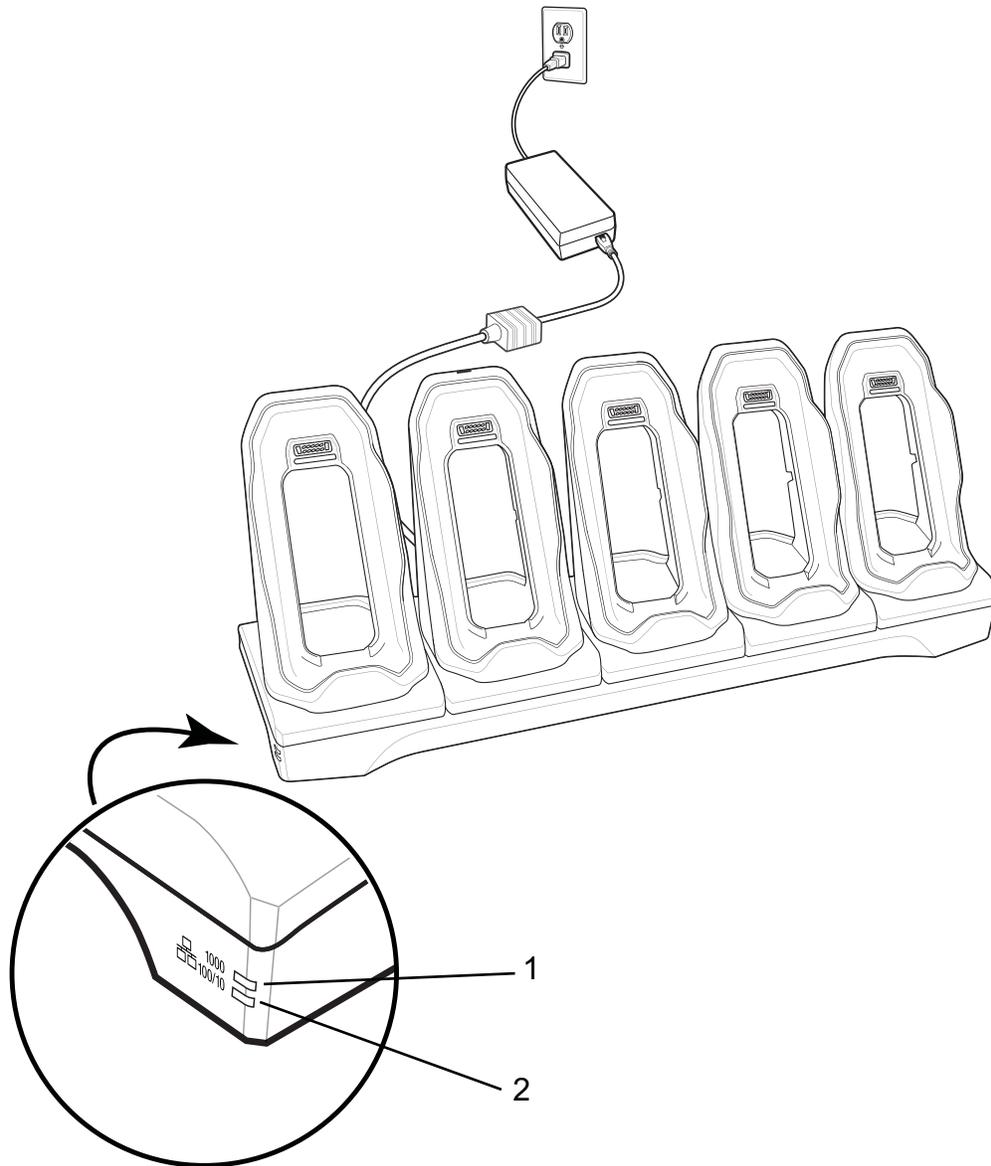
1	1000 LED – Indicates 1 Gbps data rate.
2	100/10 LED – Indicates 100 Mbps or 10 Mbps data rate.

Setup

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

Figure 47: 5-Slot Ethernet Cradle Setup
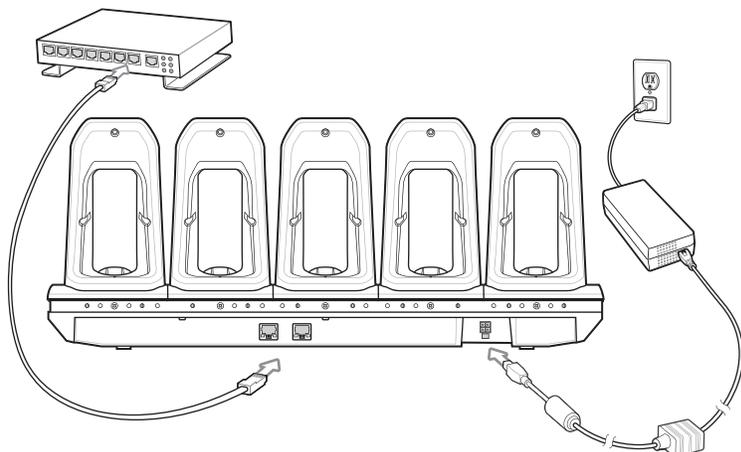
Daisy-chaining Ethernet Cradles

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:

Procedure:

1 Connect power to each 5-Slot Ethernet cradle.
2 Connect an Ethernet cable to the one of the ports on the back of the first cradle and to the Ethernet switch.
3 Connect the other end of the Ethernet cable to one of the ports of the back of the second 5-Slot Ethernet cradle.

Figure 48: Daisy-chaining 5-Slot Ethernet Cradles
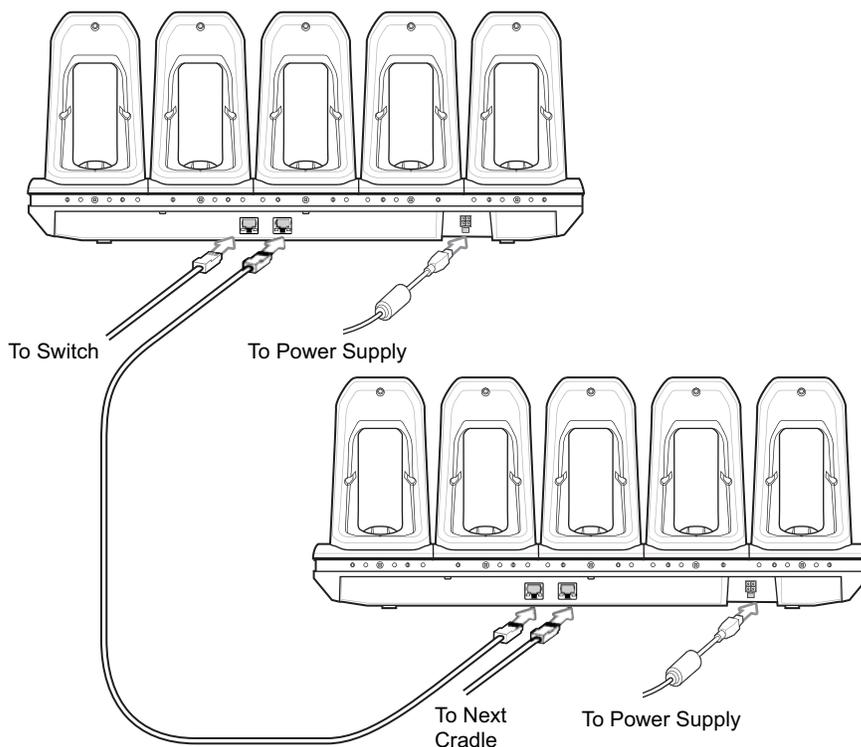
4 Connect additional cradles as described in step 2 and 3.

Ethernet Settings

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The TC70 includes Ethernet cradle drivers. After the TC70, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch **Ethernet**.

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

5 Place the TC70 into the Ethernet cradle slot.

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

7 Touch **Modify Proxy**.

Figure 49: Ethernet Proxy Settings

8 Touch the **Proxy settings** drop-down list and select **Manual**.

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

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

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

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

12 Touch **Modify**.

13 Touch ⌂.

Configuring Ethernet Static IP Address

The TC70 includes Ethernet cradle drivers. After the TC70, configure the Ethernet connection:

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch **Ethernet**.

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

5 Place the TC70 into the Ethernet cradle slot.

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

7 Touch **Disconnect**.

Figure 50: Ethernet Proxy Settings
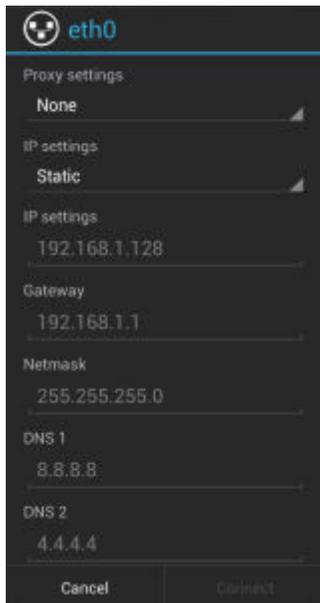
8 Touch and hold **Eth0** until the menu appears.

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

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

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

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

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

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

15 Touch **Connect**.

16 Touch ⌂.

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 6: 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

Charging the TC70

Procedure:

1   Insert the TC70 into a slot to begin charging.

Figure 51: TC70 Battery Charging
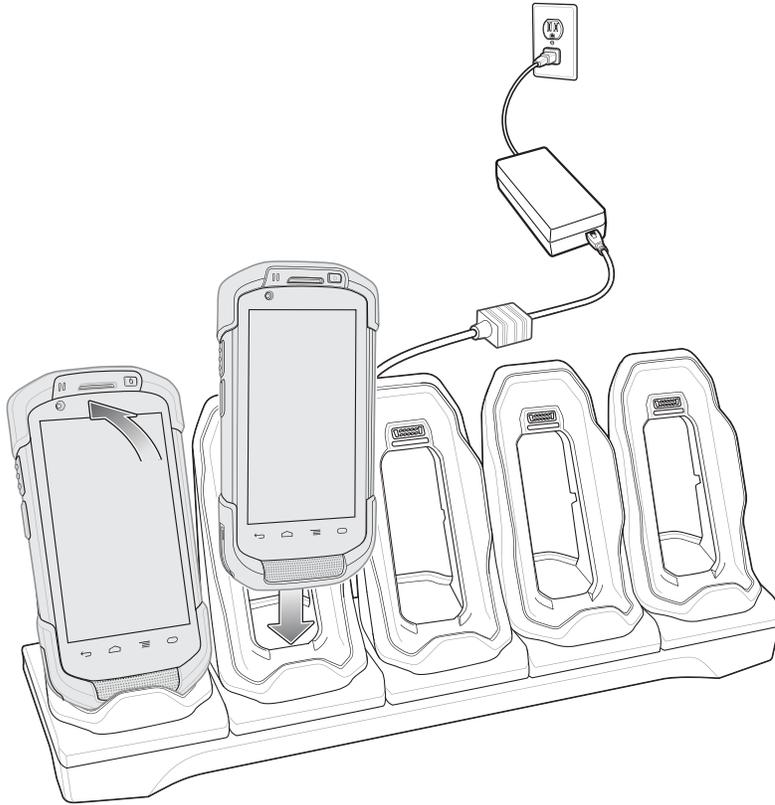
2   Ensure the TC70 is seated properly.

Figure 52: 5-Slot Ethernet Cradle with 4-Slot Battery Charger
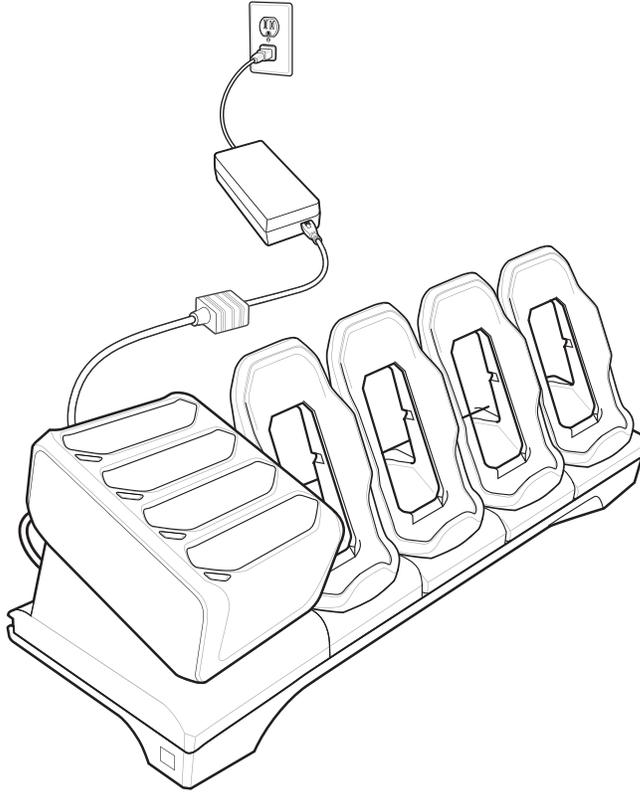
Battery Charging

Main Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device.

The 4,620 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 4,620 mAh battery fully charges in less than six hours at room temperature.

Table 7: Spare Battery Charging LED Indicators

LED	Indication
Slow Blinking Amber	Spare battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Slow Blinking Red	Spare battery is charging and battery is at the end of useful life.
Solid Red	Charging complete and battery is at the end of useful life.
Fast Blinking Red	Error in charging; check placement of spare battery and battery is at the end of useful life.

Table continued…

LED	Indication
Off	No spare battery in slot; spare battery not placed correctly; cradle is not powered.

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

Procedure:

1 Touch [icon].

2 Touch [icon].

3 Touch **Ethernet**.

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

5 Insert the device into a slot.

The [icon] icon appears in the Status bar.

6 Touch **Eth0** to view Ethernet connection details.

Installing the 4-Slot Battery Charger

Note: The Battery Charger must be installed in the first slot only.

Procedure:

1 Remove power from the cradle.

Figure 53: Remove Power from Cradle
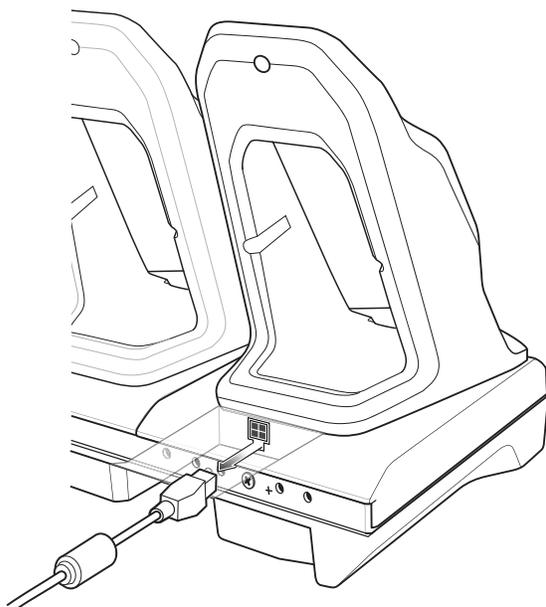
2 Using a Phillips screwdriver, remove the screw securing the cup to the cradle base.

Figure 54: Remove Screw
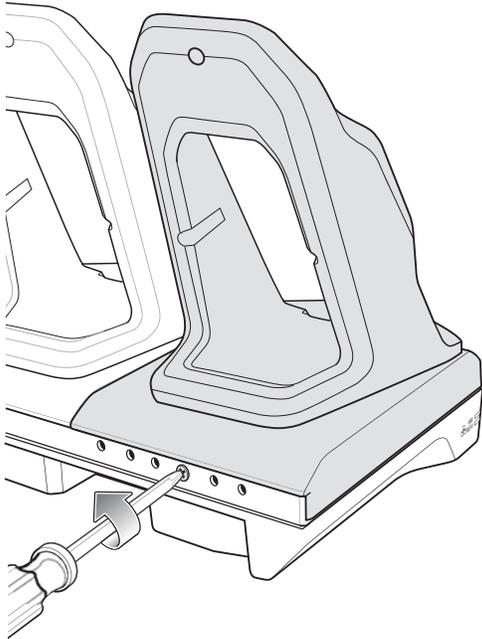
3 Slide the cup to the front of the cradle.

Figure 55: Remove Cup
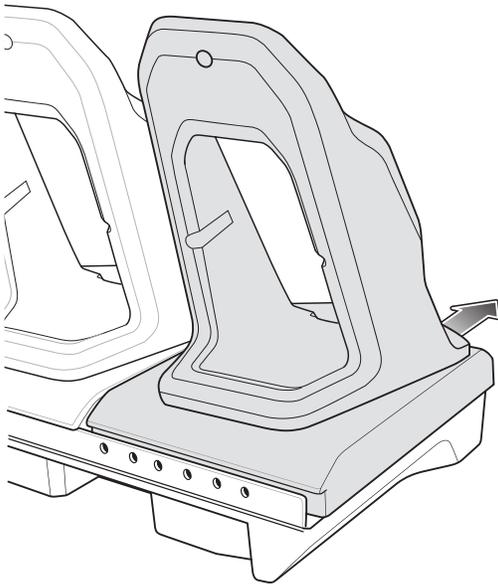
4 Carefully lift the cup up to expose the cup power cable.
5 Disconnect the cup power cable and USB cable.

Figure 56: Disconnect Cup Cables
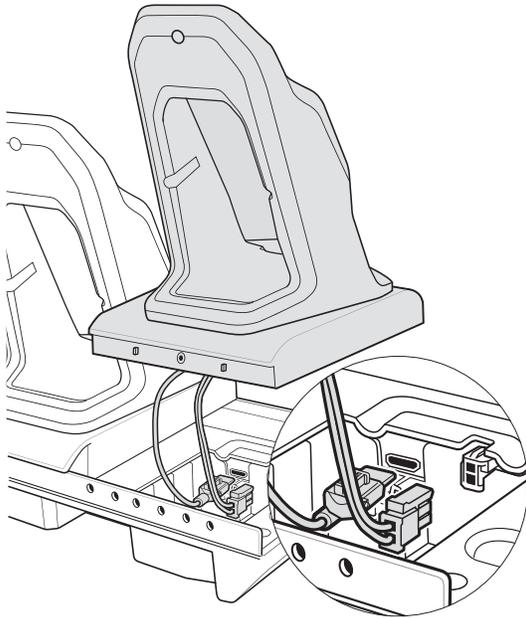
6 **Note:** Place power cable into adapter to avoid pinching cable.

Connect the Battery Adapter power cable to the connector on the cradle.

Figure 57: Connect Adapter Power Cable
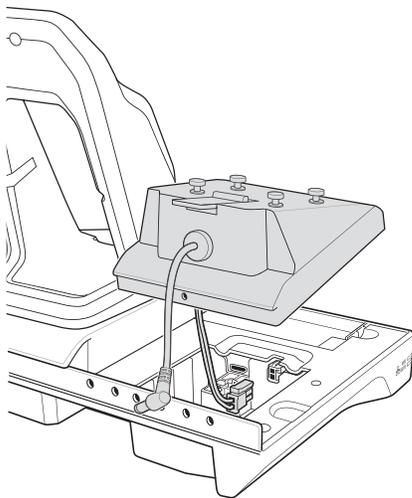
7 Place adapter onto cradle base and slide toward rear of cradle.

Figure 58: Install Adapter
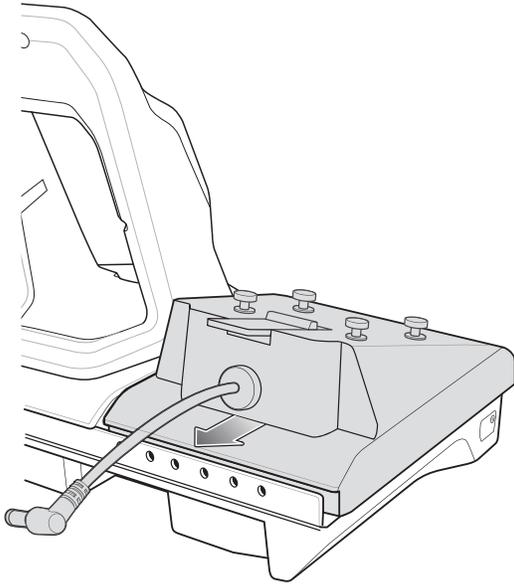
8 Using a Phillips screwdriver, secure adapter to cradle base with screw.

Figure 59: Secure adapter to Cradle
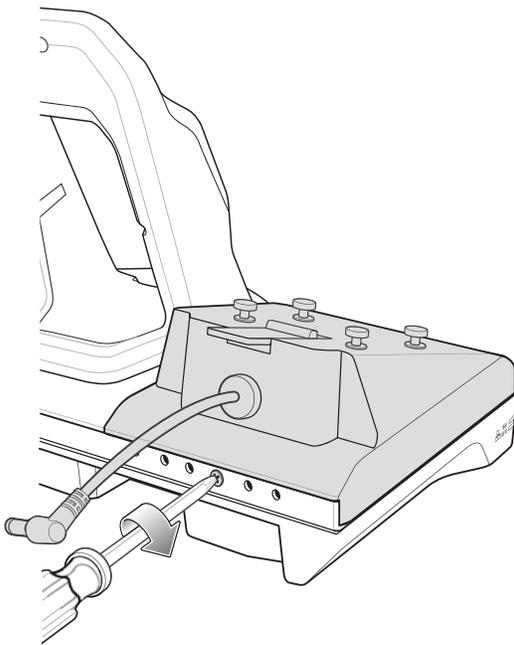
9 Align mounting holes on the bottom of the 4-Slot Battery Charger with the stubs on the Battery Adapter.

Figure 60: Install 4-Slot Battery Charger
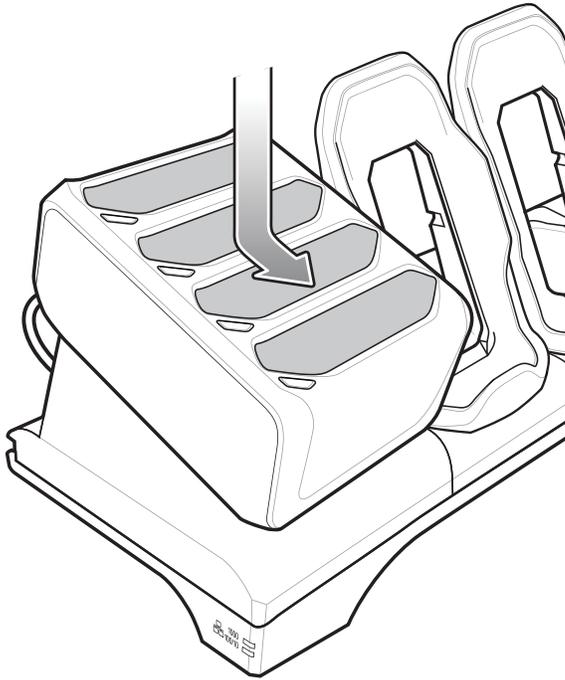
10 Slide the 4-Slot battery Charger down toward the front of the cradle.

11 Connect the output power plug into the power port on the 4-Slot Battery Charger.

Figure 61: Connect Adapter Power Cable
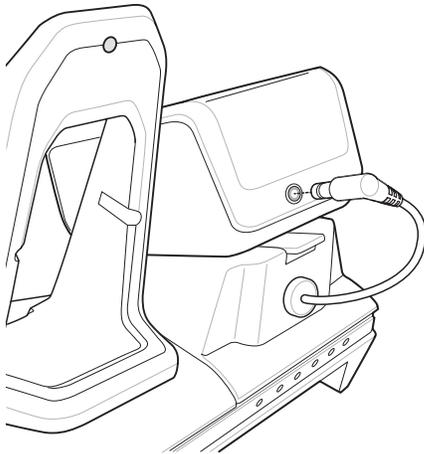
Removing the 4-Slot Battery Charger

Procedure:

1 Disconnect the output power plug from the 4-Slot Battery Charger.

2 At the back of the cup, press down on the release latch.

Figure 62: Press Release Latch
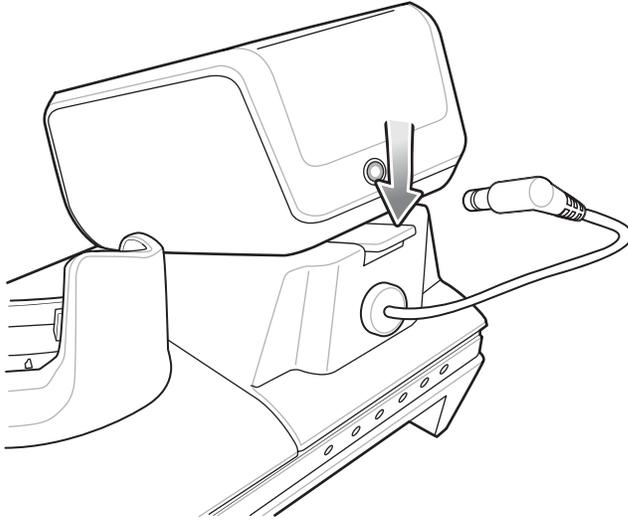
3   Slide the 4-Slot Battery Charger toward the front of the cradle.

4   Lift the 4-Slot off the cradle cup.

4-Slot Battery Charger

This section describes how to use the 4-Slot Battery Charger to charge up to four TC70 batteries.

Setup

Figure 63: Four Slot Battery Charger Power Setup
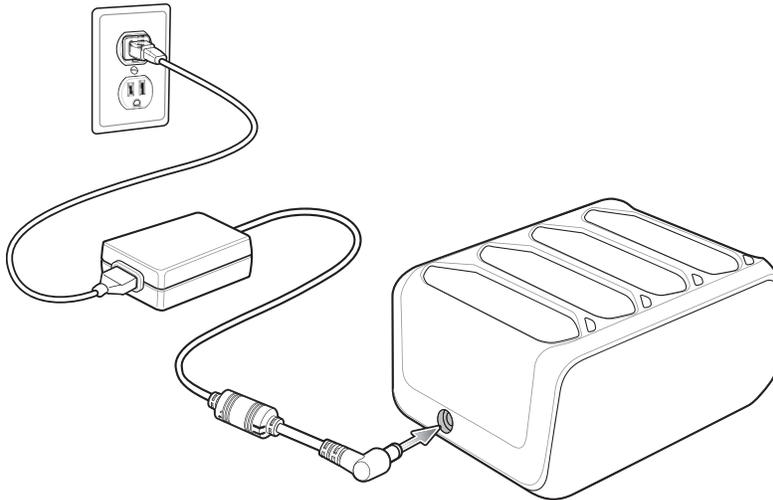
Charging Spare Batteries

Procedure:

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 64: Four Slot Battery Charger
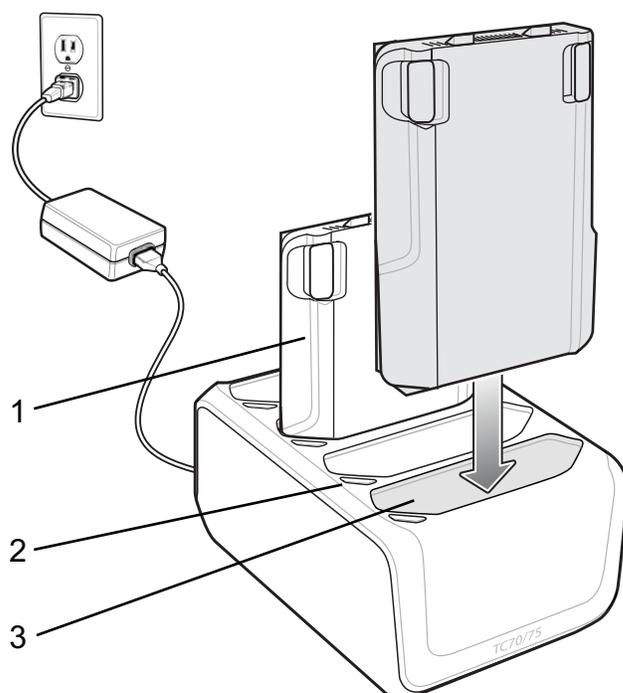
Item	Description
1	TC70 Battery
2	Battery Charge LED
3	Battery Slot

Battery Charging

Spare Battery Charging

Each Battery Charging LED indicates the status of the battery charging in each slot. The table below describes the Battery Charging LED status.

The 4,620 mAh battery fully charges in less than six hours at room temperature.

Table 8: Battery LED Charging Indicators

LED	Indication
Slow Blinking Amber	Spare battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Slow Blinking Red	Spare battery is charging and battery is at the end of useful life.
Solid Red	Charging complete and battery is at the end of useful life.
Fast Blinking Red	Error in charging; check placement of spare battery and battery is at the end of useful life.

Table continued…

LED	Indication
Off	No spare battery in slot; spare battery not placed correctly; cradle is not powered.

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.

Hand Strap Replacement

Caution: Close all running applications prior to replacing the hand strap.

Procedure:

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

2 Touch **Power Off**.

3 Touch **OK**.

4 Remove the hand strap clip from the hand strap mounting slot.

Figure 65: Remove Hand Strap Clip
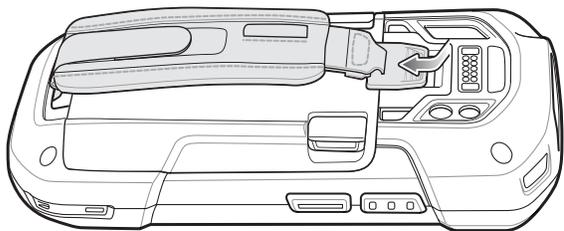
5 Press the two battery latches in.

Figure 66: Press Battery Latches

6   Lift the battery from the TC70.

Figure 67: Lift the Battery
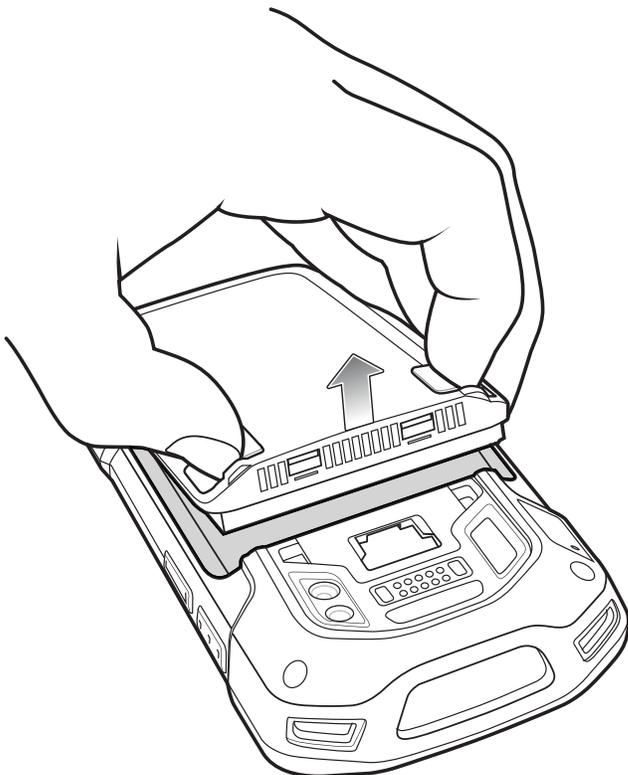
7   Remove the battery.
8   Remove the hand strap plate from the hand strap slot.
9   Insert the replacement hand strap plate into the hand strap slot.

Figure 68: Insert Hand Strap
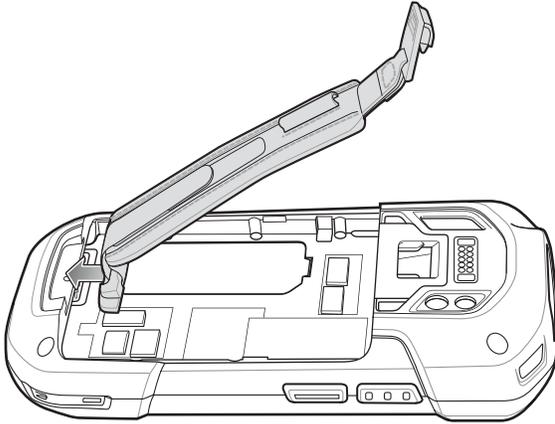
10 Insert the battery, bottom first, into the battery compartment in the back of the TC70.

Figure 69: Insert Bottom of Battery into Battery Compartment
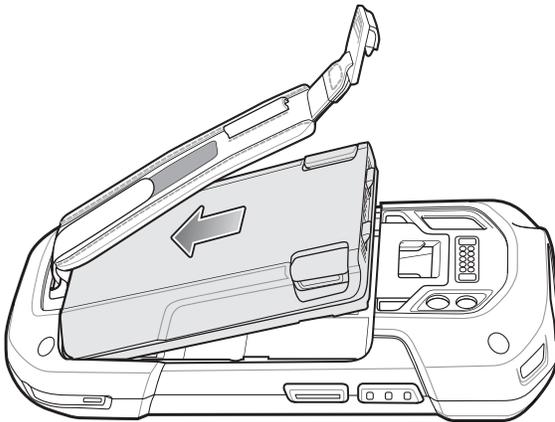
11 Rotate the top of the battery into the battery compartment.

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

Figure 70: Press Down on Battery
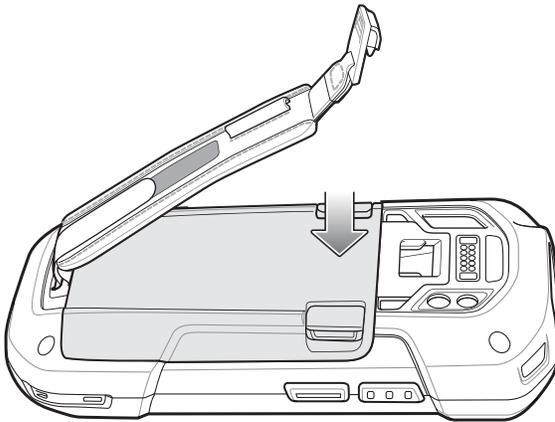
13 Place hand strap clip into hand strap mounting slot and pull down until it snaps into place.

Figure 71: Secure Hand Strap Clip
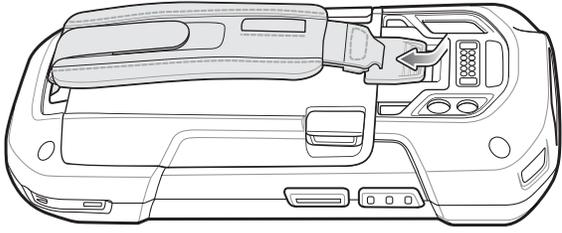
Chapter

3

USB Communication

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

Connecting to a Host Computer via USB

Connect the TC70 to a host computer using the USB Charging cable to transfer files between the TC70 and the host computer.

> **Caution:**
>
> When connecting the TC70 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Connecting to the TC70 as a Media Device

Note: Using Media Device, you can copy files to either the microUSB card or internal memory.

Procedure:

1 Connect the USB Charge cable to the TC70 and then to the host computer.
   Connected as a media device, **Connected as an installer** or **Connected as a camera** appears on the Status bar.

2 If **Connected as an installer** or **Connected as a camera** appears, pull down the Notification shade and touch **Connected as an installer** or **Connected as a camera** and then touch **Media device (MTP)**.

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

4 Locate the **TC70** as a portable device.

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

6 Copy or delete files as required.

Connecting to the TC70 as an Installer

Procedure:

1 Connect the USB Charge cable to the TC70 and then to the host computer.
   Connected as a media device, **Connected as an installer** or **Connected as a camera** appears on the Status bar.

2 If **Connected as media device** or **Connected as a camera** appears, pull down the Notification shade and touch **Connected as media device** or **Connected as a camera** and then touch **USB mass storage (UMS)**.

3 Touch **Turn on USB Storage**.

4 On the host computer, open a file explorer application.
   The TC70 storage appears as Removable Disk.

5 Locate the TC70 as a devices within Removable Storage.

6 Open the **Removable Disk**.

7   Copy or delete files as required.

8   On the TC70, touch **Turn off USB storage**.

Connecting to the TC70 as a Camera

Note: Using Camera, you can copy files to either the microUSB card or internal memory.

Procedure:

1   Connect the USB Charge cable to the TC70 and then to the host computer.
Connected as a media device, **Connected as an installer Connected as a camera** or appears on the Status bar.

2   If **Connected as an installer** or **Connected as a media device** appears, pull down the Notification shade and touch **Connected as an installer** or **Connected as a media device** and then touch **Camera (PTP)**.

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

4   Locate the **TC70** as a portable device.

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.

Procedure:

1   On the host computer, unmount the device.

2   Remove the USB Charging cable from the device.

Chapter

4

DataWedge Configuration

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

Basic Scanning

Scanning can be performed using the imager.

Using the Imager

To capture bar code data:

Procedure:

1 Ensure that an application is open on the TC70 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 72: TC70 Data Capture
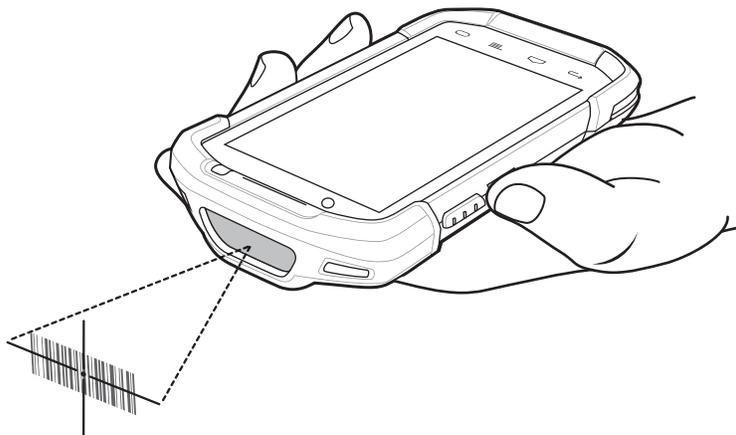
4 The green, a beep sounds and the TC70 vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

Profiles

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

Profile information consists of:

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

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

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

- Visible profiles:

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

    - **RD Client** - provides support for MSP.
    - **MSP Agent** - provides support for MSP.
    - **MspUserAttribute** - provides support for MSP.
    - **Camera** - disables scanning when the default camera application is in foreground.
    - **RhoElements** - disables scanning when RhoElements is in foreground.

Profile0

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

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

Plug-ins

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

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

Input Plug-ins

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

- **Bar Code Scanner Input Plug-in** – The Bar Code Scanner Input Plug-in is responsible for reading data from the integrated bar code scanner and supports different types of bar code readers including laser, imager and internal camera. Raw data read from the bar code scanner can be processed or formatted using Process Plug-ins as

required. **DataWedge** has built-in feedback functionality for the bar code scanner to issue user alerts. The feedback settings can be configured according to user requirement.
• **MSR Input Plug-in** – The Magnetic Stripe Reader (MSR) Input Plug-in is responsible for reading data from an MSR. Raw data read from the MSR can be processed or formatted using Process Plug-ins as required. **DataWedge** has built-in feedback functionality for the MSR to issue user alerts. The feedback settings can be configured according to user requirement.

Process Plug-ins

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

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

Output Plug-ins

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

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

Profiles Screen

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

• **Profile0**
• **Launcher**
• **DWDemo**.

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

Figure 73: DataWedge Profiles Screen
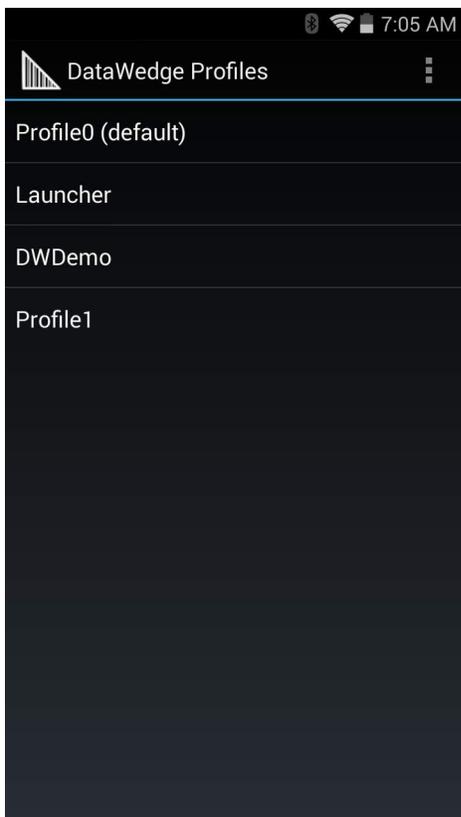
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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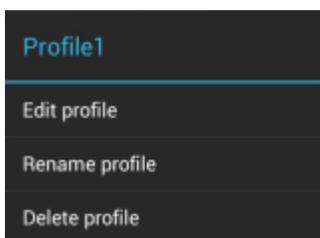
The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

Options Menu

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

Disabling DataWedge

Procedure:

1 Touch ⊞.

2 Touch ▥.

3 Touch ☰.

4 Touch **Settings**.

5 Touch **DataWedge enabled**.
The blue check disappears from the checkbox indicating that DataWedge is disabled.

Creating a New Profile

Procedure:

1 Touch ⊞.

2 Touch ▥.

3 Touch ☰.

4 Touch **New profile**.

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

Figure 75: New Profile Name Dialog Box
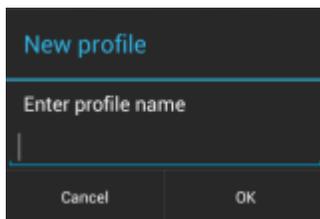
6 Touch **OK**.
The new profile name appears in the **DataWedge profile** screen.

Profile Configuration

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

Figure 76: Profile Configuration Screen
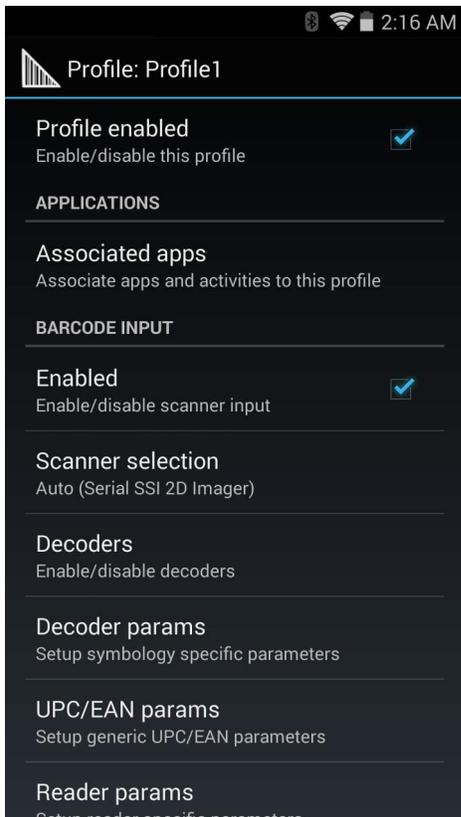
The configuration screen lists the following sections:

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

Bar Code Input

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

Enabled

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

Scanner Selection

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

- **Auto** - The software automatically selects the 2D Imager.
- **Serial SSI 2D Image** - Scanning is performed using the 2D Imager.

Decoders

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

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

Note: DataWedge supports the decoders listed below but not all are validated on this device.

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

⬅ to return to the previous screen.

Decoder Params

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

- **UPCA**

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

    There are three options for transmitting a UPCA preamble:

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

- **UPCE0**

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

    There are three options for transmitting a UPCE0 preamble:

    - **Preamble Sys Char** - Transmit System Character only.
    - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).

+ **Preamble None** - Transmit no preamble (default).
- **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).

- **Code128**

  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 77* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 77* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Enable Plain Code 128** - Flag to enable other 128 sub types (besides GS1-128 and ISBT-128).
  - **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
  - **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
  - **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:

    + **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
    + **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
    + **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
  - **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.

    + **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
    + **Security Level 1** - This setting eliminates most misdecodes (default).
    + **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
    + **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.

- **Code39**

  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 77* for more information.
  - **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 77* for more information.
  - **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).
  - **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
  - **Full ASCII** - Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled),
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

- **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
- **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character "A" to all Code 32 bar codes (default - disabled).
- **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).

- **Interleaved 2 of 5**

  - **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 77* for more information.
  - **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 77* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **Check Digit**

    + **No Check Digit** - A check digit is not used. (default)
    + **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
    + **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
  - **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).
  - **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
  - **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).

- **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).

- **US Postnet**

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

- **US Planet**

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

- **UK Postal**

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

- **Codabar**

  - **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 77* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 77* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).

- **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).

- **MSI**

    - **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 77* for more information.
    - **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 77* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
    - **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.

        + **One Check Digit** - Verify one check digit (default).
        + **Two Check Digits** - Verify two check digits.

    - **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.

        + **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
        + **Mod-10-10** - Both check digits are MOD 10.

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

- **Code93**

    - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 77* for more information.
    - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 77* 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).

- **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).

- **Discrete 2 of 5**

    - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 77* for more information.
    - **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 77* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

- **Code 11**

    - **Length1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 77* for more information.
    - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 77* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
    - **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code.

        + **No Check Digit** - Do not verify check digit.
        + **1 Check Digit** - Bar code contains one check digit (default).
        + **2 Check Digits** - Bar code contains two check digits.

    - **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).

- **Matrix 2 of 5**

    - **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 77* for more information.
    - **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 77* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

- **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
- **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).

• **UPCE1**

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

  There are three options for transmitting a UPCE1 preamble:

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

Decode Lengths

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

• Variable length: Decode symbols containing any number of characters.

- Set both **Length1** and **Length2** to 0.

• Range: Decode a symbol with a specific length range (from a to b, including a and b).

- Set **Length1** to a and set **Length2** to b.

• Two Discrete Lengths: Decode only symbols containing either of two selected lengths.

- Set both **Length1** or **Length2** to the specific lengths. **Length1** must be greater than **Length2**.

• One Discrete Length: Decode only symbols containing a specific length.

- Set both **Length1** and **Length2** to the specific length.

UPC EAN Params

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

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

- **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding "in-spec" UPC/EAN bar codes (default).
- **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
- **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
- **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.

• **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
• **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.

- **Supplemental Mode**
  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
  - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).
- **Linear Decode** -
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled.
- **Coupon Repost 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.
- **Bookland Format** - If Bookland is enabled, select one of the following formats for Bookland data:
  - **Bookland ISBN-10** - The scanner reports Bookland data starting with 978 in tranditional 10–digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode.
  - **Bookland ISBNN-13** - The scanner reports Bookland data (starting with either 978 or 979) as EAN-13 in 13–digit format to meet the 2007 ISBN-13 protocol.

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.

Reader Params

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

- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -15000).
- **Linear Security Level** - Sets the number of times a bar code is read to confirm an accurate decode.

  - **Security Short or Codabar** - Two times read redundancy if short bar code or Codabar.
  - **Security All Twice** - Two times read redundancy for all bar codes (default).
  - **Security Long and Short** - Two times read redundancy for long bar codes, three times for short bar codes.
  - **Security All Thrice** - Three times read redundancy for all bar codes.

- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.

  - **Disable** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Enabled** – Enables Picklist mode. Only the bar code in the center of the image is decoded.

- **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.

    Note: When using the LCD mode, a degradation in performance may be observed and the aiming crosshair may blink until the bar code is decoded.

- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D bar codes.

  - **Disable** - Disables decoding of inverse 1D bar codes (default).
  - **Enable** - Enables decoding of only inverse 1D bar codes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D bar codes.

Scan Params

Allows the configuration of Code ID and decode feedback options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned bar code. This is useful when the reader is decoding more than one code type. Select a code ID character to insert between the prefix and the decoded symbol.

  - **Code ID Type None** - No prefix (default).
  - **Code ID Type Aim** - A standards based three character prefix.
  - **Code ID Type Symbol** - A Symbol defined single character prefix.

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

- **Volume Type** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.

  - **Ringer and Notifications** - Set the good decode beep to the ringer and notifications sound.(default)
  - **Music and media** - Set the good decode beep to the music and media sound
  - **Alarms** - Set the good decode beep to the alarm sound

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

- **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.)
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).

MSR Input

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

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

Keystroke Output

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

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code or MSR data for use in native Android applications. This feature is helpful when populating or executing a form.

  - **None** - Action key character feature is disabled (default).
  - **Tab** - Tab character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.

- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.

  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 86* 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 86* for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
    - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
    - **Prefix to data** - Add characters to the beginning of the data when sent.
    - **Suffix to data** - Add characters to the end of the data when sent.
    - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
    - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
    - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
    - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Overview

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

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

```
<intent-filter . . . >

<action android:name="android.intent.action.DEFAULT" />

<category android:name="android.intent.category.MAIN" />

</intent-filter>
```

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

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

and the Intent category would be:

`android.intent.category.MAIN.`

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

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

- String LABEL_TYPE_TAG = "com.symbol.emdk.datawedge.label_type";

  - String contains the label type of the bar code.
- String DATA_STRING_TAG = "com.symbol.emdk.datawedge.data_string";

  - String contains the output data as a String. In the case of concatenated bar codes, the decode data is concatenated and sent out as a single string.
- String DECODE_DATA_TAG = "com.symbol.emdk.datawedge.decode_data";

  - Decode data is returned as a list of byte arrays. In most cases there will be one byte array per decode. For bar code symbologies that support concatenation e.g. Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per bar code). Clients can get data in each byte array by passing an index.

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

- String MSR_DATA_TAG = "com.symbol.emdk.datawedge.msr_data";

  - String contains the output data as a String. The data from the MSR tracks is concatenated and sent out as a single string.
- String MSR_TRACK1_TAG = "com.symbol.emdk.datawedge.msr_track1";

  - MSR track 1 data is returned as a byte array.
- String MSR_TRACK2_TAG = "com.symbol.emdk.datawedge.msr_track2";

  - MSR track 2 data is returned as a byte array.
- String MSR_TRACK3_TAG = "com.symbol.emdk.datawedge.msr_track3";

  - MSR track 3 data is returned as a byte array.
- String MSR_TRACK1_STATUS_TAG = "com.symbol.emdk.datawedge.msr_track1_status";

  - MSR track 1 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK2_STATUS_TAG = "com.symbol.emdk.datawedge.msr_track2_status";

  - MSR track 2 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK3_STATUS_TAG = "com.symbol.emdk.datawedge.msr_track3_status";

  - MSR track 3 decode status as an Integer where 0 indicates a successful decode.

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

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

IP Output

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

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.
- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.

    - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
    - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 86* 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 77: IP Output Screen
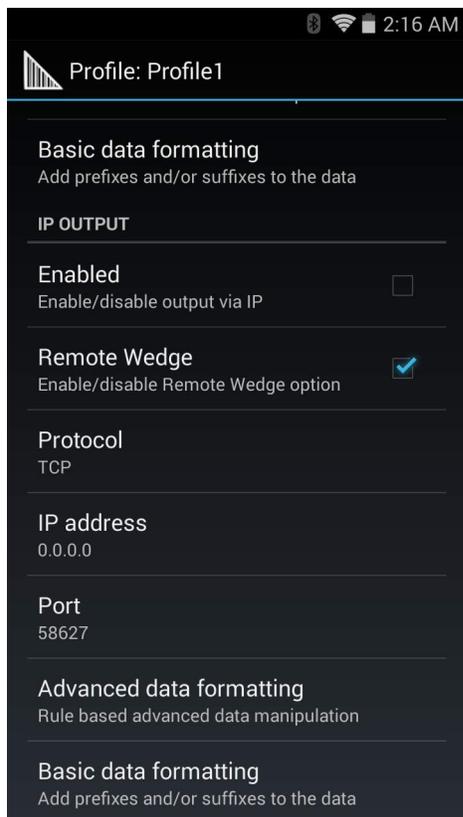
Using IP Output with IPWedge

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:

Procedure:

1   In **IP Output**, touch **Enabled**.
    A check appears in the checkbox.

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

3   Touch **Protocol**.

4   In the **Choose protocol** dialog box, touch the same protocol selected for the **IPWedge** computer application. (TCP is the default).

Figure 78: Protocol Selection
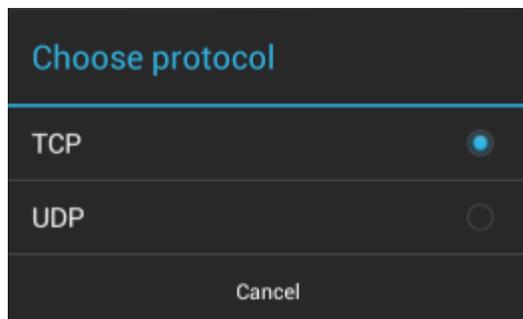
5 Touch **IP Address**.

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

Figure 79: IP Address Entry
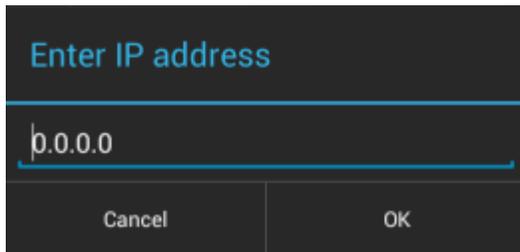
7 Touch **Port**.

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

Figure 80: Port Number Entry
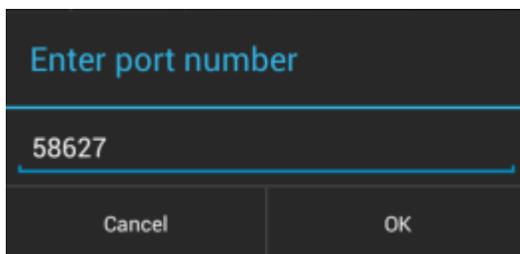
9 Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

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:

Procedure:

1 In **IP Output**, touch **Enabled**.
A check appears in the checkbox.

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

3 Touch **Protocol**.

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

Figure 81: Protocol Selection
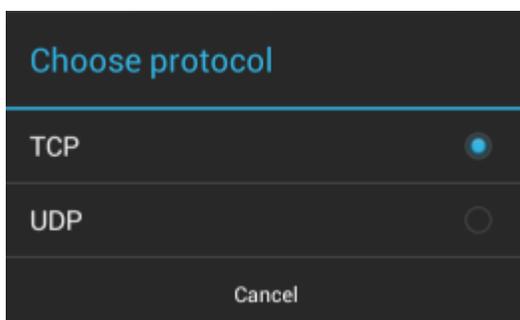
5   Touch **IP Address**.

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

Figure 82: IP Address Entry
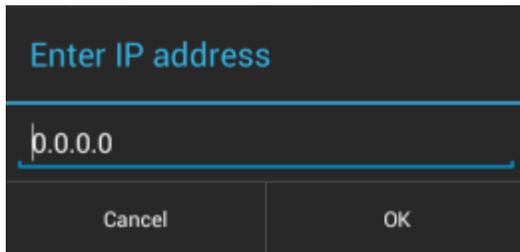
7   Touch **Port**.

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

Figure 83: Port Number Entry
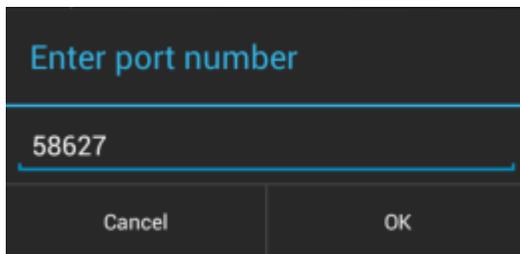
9   Configure **Advanced Data Formatting** and **Basic Data Formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

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.

Procedure:

1   Touch ⊞ .

2   Touch ▥ .

3 Touch a DataWedge profile.

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

Figure 84: Advanced Data Formatting Screen
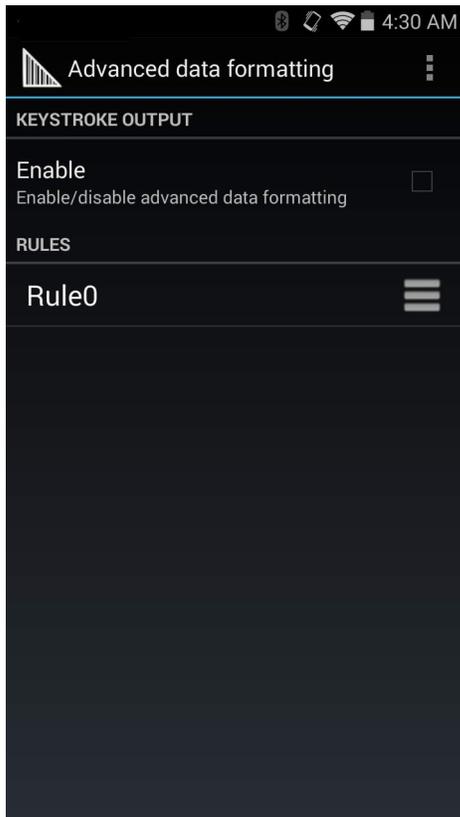
5 Touch the **Enable** checkbox to enable ADF.

Creating a Rule

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

Procedure:

1 Touch ≡.

2 Touch **New rule**.

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

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

5 Touch **Done**.

6 Touch **OK**.

Defining a Rule

Procedure:

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

Figure 85: Rule List Screen
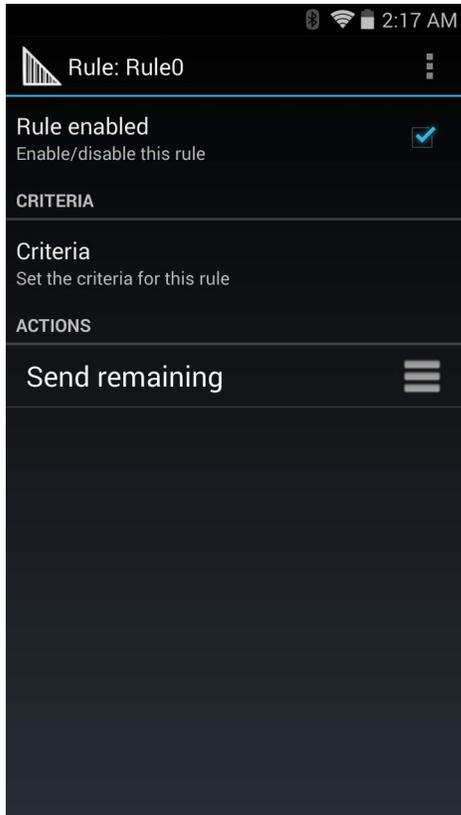
2 Touch the **Rule enabled** checkbox to enable the current rule.

Defining Criteria

Procedure:

1 Touch **Criteria**.

Figure 86: Criteria Screen
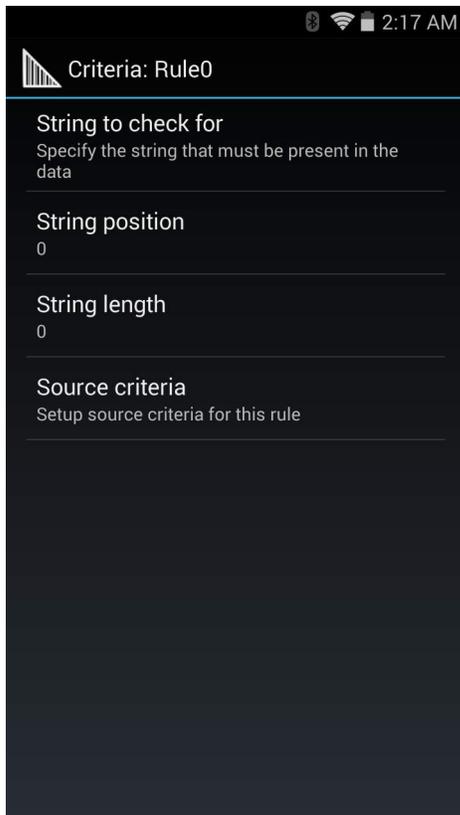
2 Touch **String to check for** option to specify the string that must be present in the data.

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

4 Touch **Done**.

5 Touch **OK**.

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

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

8 Touch **OK**.

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

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

11 Touch **OK**.

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

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

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

Figure 87: Barcode Input Screen
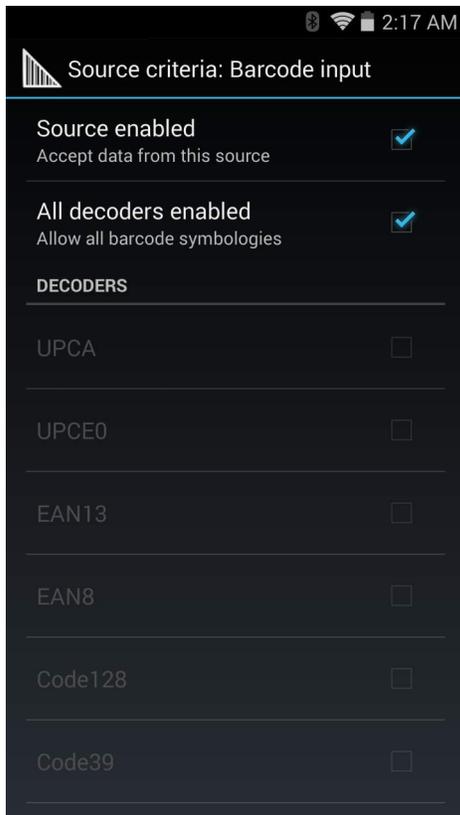
15 For **Barcode inputs**, touch the **All decoders enabled** checkbox to select all bar code symbologies. Deselect the **All decoders enabled** checkbox to individually select the symbologies.

16 Touch ⟵ until the **Rule** screen appears.

17 If required, repeat steps to create another rule.

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

Defining an Action

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

Procedure:

1 Touch ≡.

2 Touch **New action**.

3 In the **New action** menu, select an action to add to the **Actions** list. See *Table 9: ADF Supported Actions on page 91* for a list of supported ADF actions.

4 Some Actions require additional information. Touch the Action to display additional information fields.

5 Repeat steps to create more actions.

6 Touch ⟵.

7 Touch ⟵.

Deleting a Rule

Procedure:

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

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

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

Order Rules List

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

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

Table 9: ADF Supported Actions

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

Table continued…

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

Deleting an Action

Procedure:

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

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

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

Modify the data as follows:

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

To create an ADF rule for the above example:

Procedure:

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

10 Touch **String position**.

11 Change the value to 0.

12 Touch **OK**.

13 Touch **String length**.

14 Change value to 12.

15 Touch **OK**.

16 Touch **Source criteria**.

17 Touch **Barcode input**.

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

19 Touch **Code 39**.

20 Touch ↩ three times.

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

22 Touch **Delete action**.

23 Touch ≡ .

24 Touch **New action**.

25 Select **Pad with zeros**.

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

27 Touch **How many**.

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

29 Touch ↩ three times.

30 Touch ≡ .

31 Touch **New action**.

32 Select **Send up to**.

33 Touch **Send up to** rule.

34 Touch **String**.

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

36 Touch **OK**.

37 Touch ↩ three times.

38 Touch ≡ .

39 Touch **New action**.

40 Select **Send char**.

41 Touch **Send char** rule.

42 Touch **Character code**.

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

44 Touch **OK**.

45 Touch ↩.

Figure 88: ADF Sample Screen
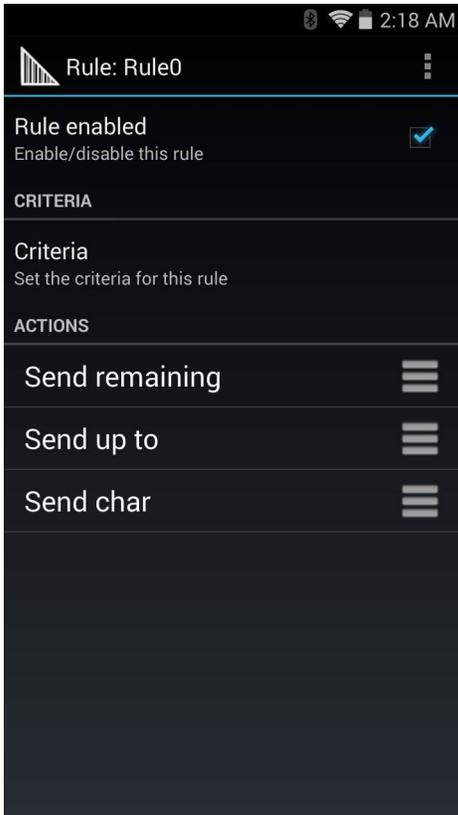
46 Ensure that an application is open on the device and a text field is in focus (text cursor in text field).

47 Aim the exit window at the bar code.

Figure 89: Sample Bar Code

1299X1559828

48 Press and hold the scan button.

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

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

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

Figure 90: Formatted Data
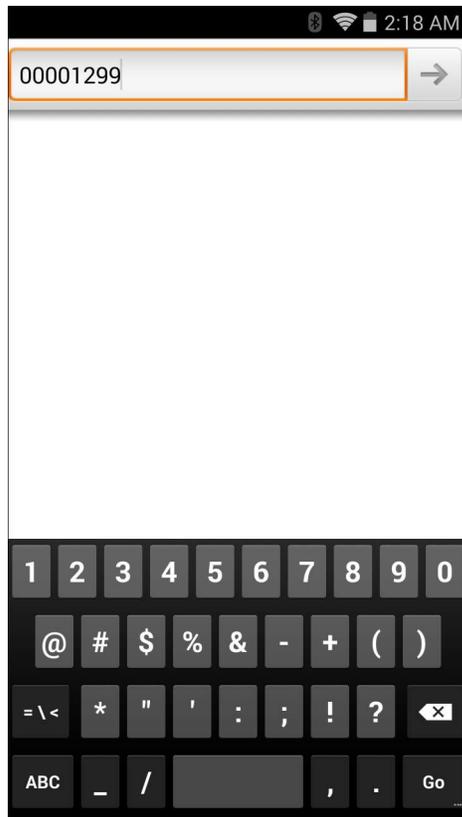
DataWedge Settings

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

Figure 91: DataWedge Settings Window
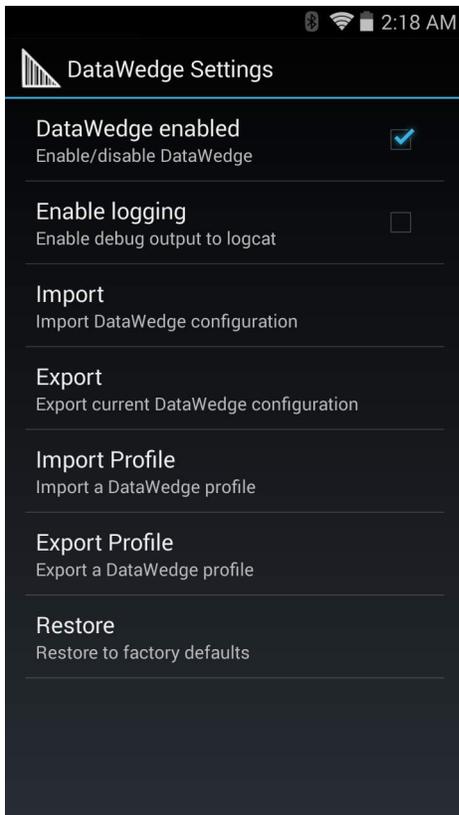
- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option.
- **Enable logging** - Enables or disables debug output file to logcat. To enable logging check this option.
- **Import** - allows import of a DataWedge configuration file. The imported configuration replaces the current configuration.
- **Export** - allows export of the current DataWedge configuration to the microSD card.
- **Import Profile** - allows import of a DataWedge profile file.
- **Export Profile** - allows export of a DataWedge profile.
- **Restore** - return the current configuration back to factory defaults.

Importing a Configuration File

Procedure:

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

Exporting a Configuration File

Procedure:

1 Touch ⊞.

2 Touch ▬.

3 Touch ≡.

4 Touch **Settings**.

5 Touch **Export**.

6 Touch **SD Card**.

7 Touch **Export**. The configuration file (`datawedge.db`) is saved to the root of the microSD card.

Importing a Profile File

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

Procedure:

1 Copy the profile file to the root of the microSD card.

2 Touch ⊞.

3 Touch ▬.

4 Touch ≡.

5 Touch **Settings**.

6 Touch **Import Profile**.

7 Touch the profile file to import.

8 Touch **Import**. The profile file (`dwprofile_x.db`, where x = the name of the profile) is imported and appears in the profile list.

Exporting a Profile

Procedure:

1 Touch ⊞.

2 Touch ▬.

3 Touch ≡.

4 Touch **Settings**.

5 Touch **Export Profile**.

6 Touch the profile to export.

7 Touch **Export**.

8 Touch **Export**. The profile file (`dwprofile_x.db`, where x = name of the profile) is saved to the root of the microSD card.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

Procedure:

1 Touch ⊕.

2 Touch ▟.

3 Touch ☰.

4 Touch **Settings**.

5 Touch **Restore**.

6 Touch **Yes**.

Configuration and Profile File Management

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

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

Enterprise Folder

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

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

Auto Import

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

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

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

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application

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

Capture Data and Taking a Photo in the Same Application

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

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

Soft Scan Feature

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

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

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

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

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

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

Sample

Intent sendIntent = new Intent();

sendIntent.setAction("com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER");

sendIntent.putExtra("com.symbol.emdk.datawedge.api.EXTRA_PARAMETER", "TOGGLE_SCANNING");

sendBroadcast(sendIntent);

Chapter
5

Administrator Utilities

We provide a suite of utilities that allow an administrator to manage the following features:

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

The following applications help the administrator configure these features.

*   On-device applications - reside on the device.

    -   MultiUser Administrator
    -   AppLock Administrator
    -   Secure Storage Administrator.
*   Host computer application - reside on a host computer.

    -   Enterprise Administrator.

Required Software

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

On-device Application Installation

See *Application Installation on page 135* for instruction on installing applications onto the device.

Multi-user/AppLock Configuration

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

Note: The administrator can also create the account information manually. See *Manual File Configuration on page 112* for more information.

Enterprise Administrator Application

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

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

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

Figure 92: Enterprise Administrator Window
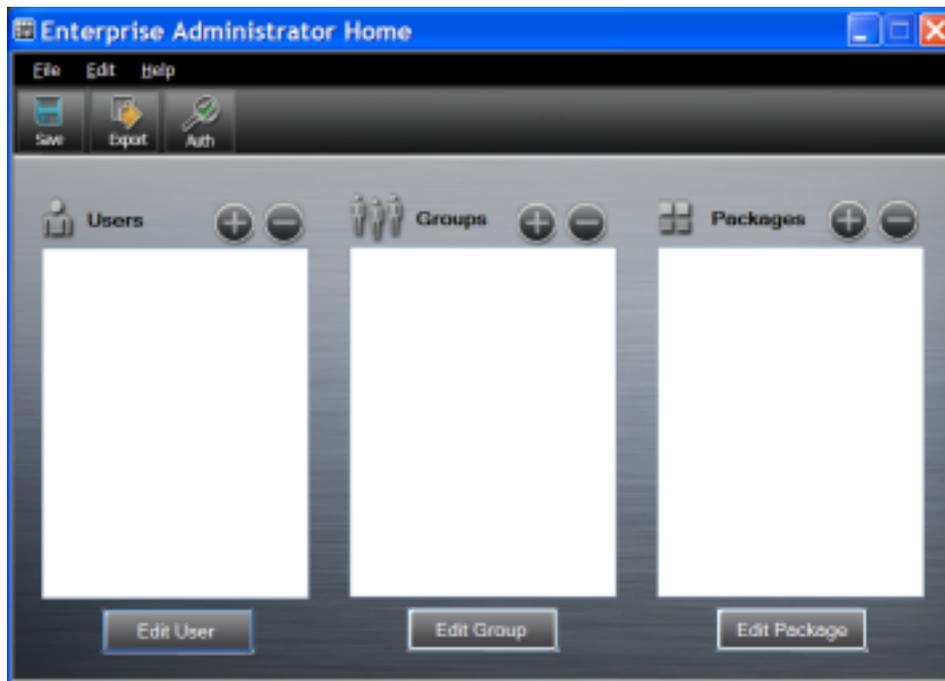
Creating Users

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

Procedure:

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

Figure 93: User Manager Window

2 In the **Username** text box, enter a user name. The text is case sensitive and required.

3 In the **Password** text box, enter a password for the user. The text is case sensitive and required.

4 In the **Retype Password** text box, re-enter the user password.

5 Select the **Admin** checkbox to set the user to have administrator rights.

6 Select the **Enabled** checkbox to enable the user.

7 Click **OK**.

8 Repeat steps 1 through 7 for each additional user.

Adding Packages

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

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

Procedure:

1 Click + next to **Packages**.

Note: To get a list of all the applications (packages) on the device see *Determining Applications Installed on the Device on page 115*.

Figure 94: Package Information Window

2 In the **Package name** text box, enter the name of an application.

3 Click **OK**.

4 Repeat steps 1 through 3 for each additional package.

Creating Groups

Create groups of users that have access to specific applications.

Procedure:

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

Figure 95: Group Manager Window

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

Creating Remote Authentication

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

Procedure:

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

Figure 96: Authentication Window

2 Select the **Remote** radio button.

3 In the **Server IP** text box, enter the address of the remote server.

4 In the **Port** text box, enter the port number of the remote server.

5 Select the **use SSL Encryption** check box if SSL encryption is required.

6 Click **OK**.

Save Data

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

Exporting File

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

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

Procedure:

1 Click **Export**.

2 In the **Browse For Folder** window, select a folder and then click **OK**.

3 Click **OK**.

4 Click **File → Export → Server Information**.
   The server file is saved in the `<user>\_APP_DATA` folder.

5 Copy all the files to the root of the microSD card. See *USB Communication on page 65* for information on copying files to the device.

Importing User List

Procedure:

1 Click **File → Import → User List**.

2   Navigate to the location when the *passwd* file is stored.

3   Select the `passwd` file.

4   Click **Open**.
The user information is populated into the **Users** list.

Importing Group List

Procedure:

1   Click **File → Import → Group List**.

2   Navigate to the location when the `group` file is stored.

3   Select the `group` file.

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

Importing Package List

To import a package list (see *Package List File on page 113* for instructions for creating a Package List file):

Procedure:

1   Click **File → Import → Package List**.

2   Navigate to the location when the package file is stored.

3   Select the package text file.

4   Click **Open**.
The package information is populated into the **Packages** list.

Editing a User

Procedure:

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

2   Click **Edit User**.

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

Deleting a User

Procedure:

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

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

Editing a Group

Procedure:

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

2   Click **Edit Group**.

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

Deleting a Group

Procedure:

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

2 Click **-**.

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

Editing a Package

Procedure:

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

2 Click **Edit Package**.

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

Deleting a Package

Procedure:

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

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

MultiUser Administrator

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

Importing a Password

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

Procedure:

1 Touch .

2 Touch .

Figure 97: MultiUser Administrator Screen
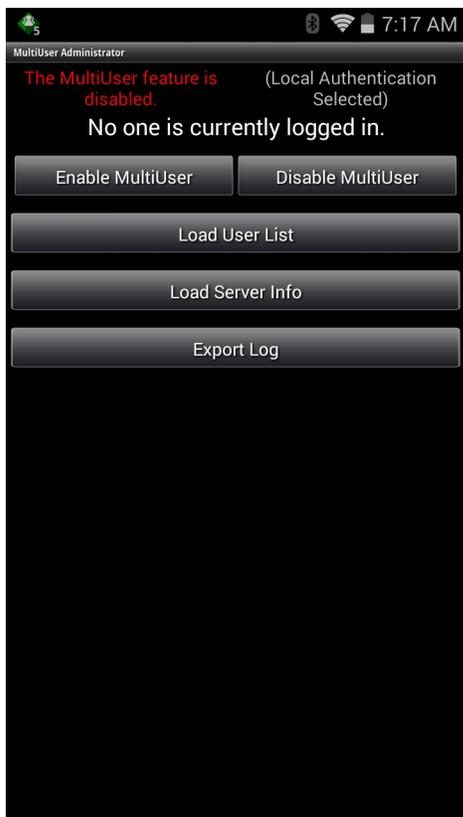
3   Touch **Load User List**. The application reads the data from the `passwd` file and configures the Multi-user Login feature.

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

Figure 98: MultiUser Login Screen
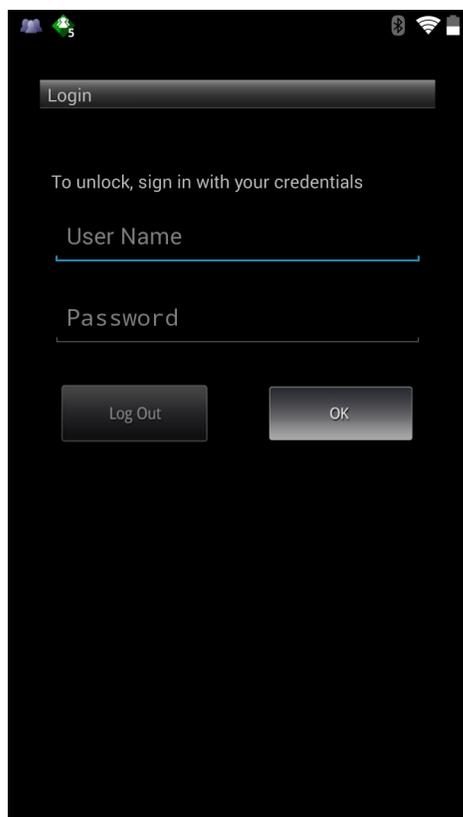
5   In the **Login** text box, enter the username.

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

7   Touch **OK**.

Disabling the Multi-user Feature

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

Procedure:

1   Touch 📱.

2   Touch 📱.

3   Touch **Disable MultiUser**.
    The Multi-user feature is disabled immediately.

Enabling Remote Authentication

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

Procedure:

1   Touch 📱.

2
   Touch .

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

4 Touch ☰.

5 Touch **Enable Remote Authentication**.
   The device accesses the remote server and then Login screen appears.

Disabling Remote Authentication

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

Procedure:

1
   Touch .

2
   Touch .

3 Touch ☰.

4 Touch **Disable Remote Authentication**.
   The remote authentication feature is disabled immediately. The device suspends. When resumed, the login screen appears.

Enabling Data Separation

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

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

Procedure:

1
   Touch .

2
   Touch .

3 Touch ☰.

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

Disabling Data Separation

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

Procedure:

1
   Touch .

2
   Touch .

3 Touch ☰.

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

Delete User Data

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

Procedure:

1 Touch ⊕.

2 Touch 👥.

3 Touch ≡.

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

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

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

Capturing a Log File

Procedure:

1 Touch ⊕.

2 Touch 👥.

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

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

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

AppLock Administrator

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

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

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

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

Enabling Application Lock

Procedure:

1 Touch ⊕.

2
Touch ▦ .

3 Touch **Enable Application Lock**.

Disabling Application Lock

Procedure:

1
Touch ⊞ .

2
Touch ▦ .

3 Touch **Disable Application Lock**.

Manual File Configuration

Groups File

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

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

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

where:

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

`<user1>` through `<userN>` = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 107* for more information.

> **Note:**
>
> If the same user is assigned to multiple groups, then that user's White List will be a logical union of the White Lists for all of the groups that user is assigned.
>
> A line starting with the # character is considered a comment and is ignored.

Examples:

- `AdminGroup:alpha`

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

  - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

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

`<package1name>`

`.`

`.`

`.`

`<packageNname>`

where:

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

Example:

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

`com.companyname.application`

`com.symbol.*` where:

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

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

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

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

> **Note:**
>
> The wildcard ".*" is allowed and indicates that this group is permitted to run any package.
>
> A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

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

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

Package List File

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

Example:

`com.symbol.example1`

`com.symbol.example2`

`com.symbol.example3`

`com.symbol.example4`

Groups File

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

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

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

where:

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

`<user1>` through `<userN>` = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 107* for more information.

> **Note:**
>
> If the same user is assigned to multiple groups, then that user's White List will be a logical union of the White Lists for all of the groups that user is assigned.
>
> A line starting with the # character is considered a comment and is ignored.

Examples:

- `AdminGroup:alpha`

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

    - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

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

`<package1name>`

`.`

`.`

`.`

`<packageNname>`

where:

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

Example:

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

`com.companyname.application`

`com.symbol.*` where:

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

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

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

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

> **Note:**
>
> The wildcard ".*" is allowed and indicates that this group is permitted to run any package.
>
> A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

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

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

Determining Applications Installed on the Device

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

Procedure:

1 Connect the device to the host computer.

> **Note:** See *Development Tools on page 134* for information on installing the USB driver for use with adb.

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

`adb devices`. This returns the device id.

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

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

Package List File

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

Example:

```
com.symbol.example1
com.symbol.example2
com.symbol.example3
com.symbol.example4
```

Secure Storage

Secure Storage Administrator application allows:

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

Installing a Key

Procedure:

1 Touch 🄌.

2 Touch 🄌.

3 Touch **Install Key**.

4 Touch **Manual**.

5 Touch **OK**.

Figure 99: Enter Key Dialog Box
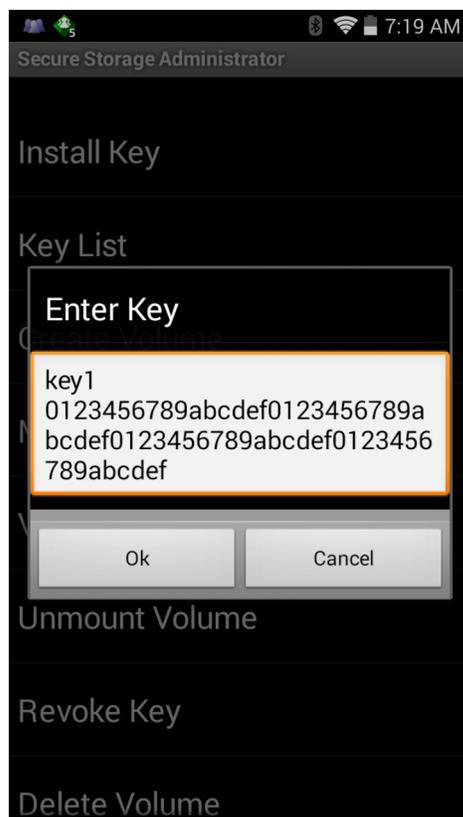
6   In the **Enter key** text box, enter the key name followed by the key value obtained in step 1, using the following format:

            <Key Name> <Key value in Hex String>

            Example: key2 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

            The key value must be a 64 hexadecimal character string.

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

Viewing Key List

Procedure:

1   Touch **Key List**.

Figure 100: List of Keys
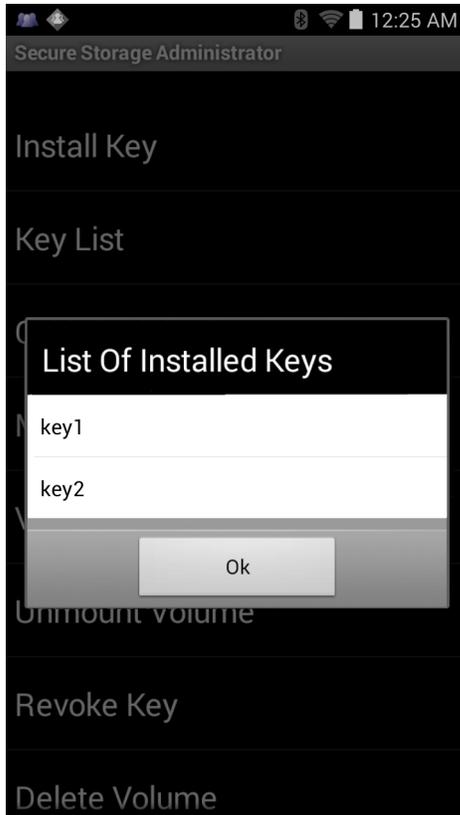
2   Touch **OK**.

Deleting a Key

Procedure:

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

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

Volumes

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

Creating Volume Using EFS File

Procedure:

1   Create an efs file. See *Creating an EFS File on page 119* for instruction on creating the efs file.
2   Copy the `keyfile` and `efsfile` files to root of the microSD card. See *USB Communication on page 65*.
3   Touch **Create Volume**.
4   Touch **Import**.
5   Touch **OK**. The message **Successfully Created the Volume** appears briefly.

Creating a Volume Manually

Procedure:

1 Touch **Create Volume**.

2 Touch **Manual**.

3 Touch **OK**.

4 In the **Enter Parameters To Create Volume** text box, enter the parameters in the follow format:

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

where:

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

Figure 101: Enter Parameter To Create Volume Dialog Box
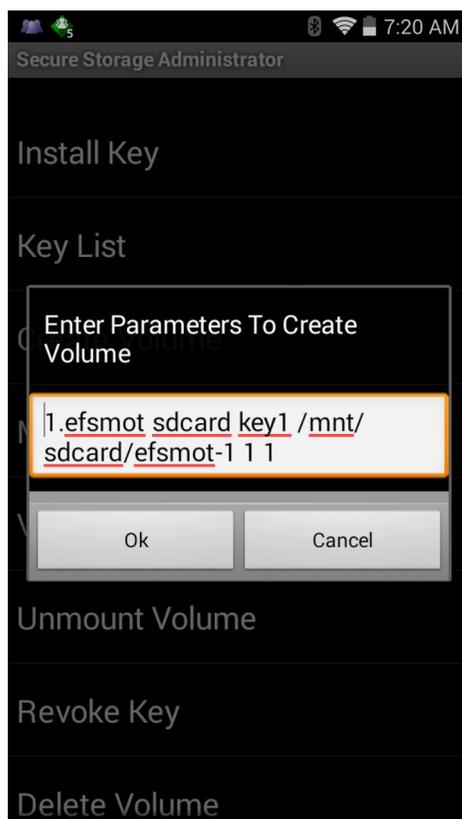
5 Touch **OK**. The message **Successfully Created the Volume** appears briefly. If the size of the volume is very large, a progress bar displays.

Mounting a Volume

Procedure:

1 Touch **Mount Volume**.

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

3 Touch **OK**.

4 Select a volume.

5 Touch **OK**.

Listing Volumes

Procedure:

1 Touch **Volume List**.

2 Touch **sdcard** to list volumes on the microSD card or **internal** to list volumes on internal storage.

3 Touch **OK**. The **List of EFS Volumes** dialog box appears with all the volumes of the selected storage location.

4 Touch **OK**.

Unmounting a Volume

Procedure:

1 Touch **Unmount Volume**.

2 Touch **sdcard** to list the mounted volumes on the microSD card or **internal** to list the mounted volumes on internal storage.

3 Touch **OK**.

4 Select the volume to un-mount.

5 Touch **OK**.

Deleting a Volume

Procedure:

1 If the encrypted volume is mounted, unmount it.

2 Touch **Delete Volume**.

3 Touch **sdcard** to list the unmounted volumes on the microSD card or **internal** to list the unmounted volumes on internal storage.

4 Select the volume to delete.

5 Touch **OK**.

Encrypting an SD Card

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

Procedure:

1 Touch **Encrypt SD card**. A warning message appears.

2 Touch **Yes**. The Key List dialog box appears.

3 Select a key from the list and then touch **Ok**.
The encryption process begins and when completed, displays a successfully completed message.

Creating an EFS File

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

Procedure:

1 On a host computer, create a text file.

2 In the text file enter the following:

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

where:

<Volume Name> = name of the volume

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

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

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

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

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

Example:

MyVolume sdcard key1 /mnt/sdcard/efsfolder 1 1

3 Save the text file as `efsfile`.

Off-line Extraction Tool

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

Connect the device to the host computer.

Usage

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

The following Main Menu appears:

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

Usage

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

The following Main Menu appears:

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

Creating an Image

Procedure:

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

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

Please enter encryption key (64-bytes hex value):

Please enter the EFS image size (in MB): <volume size in MB>

Please enter EFS image filesystem type (e.g. ext4, vfat...): ext4

DONE - OK
```

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

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

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

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

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

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

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

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

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

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

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

Mounting an Image

Procedure:

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

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

DONE - OK
```

2 Enter the name of the volume and then press **Enter**.

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

4 Enter the mount point where to connect the volume into the file system and then press **Enter**. The example of /mnt is provided.

Unmounting an Image

Procedure:

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

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

DONE - OK
```

2 Enter the name of the volume to unmount.

3 Press **Enter**.

Chapter

6

Settings

This chapter describes settings available for configuring the device.

Screen Unlock Settings

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

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

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.
    - **None** - Disable screen unlock security.
    - **Slide** - Slide the lock icon to unlock the screen.
    - **Pattern** - Draw a pattern to unlock screen. See *Set Screen Unlock Using Pattern on page 125* for more information.
    - **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 123* for more information.
    - **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 124* for more information.

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

Single User Mode

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

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

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

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

Set Screen Unlock Using PIN

Procedure:

1 Touch 🎛.

2 Touch ⚙.

3 Touch 🔒 **Security**.

4 Touch **Screen lock**.

5   Touch **PIN**.

6   Touch in the text field.

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

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

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

Figure 102: PIN Screen
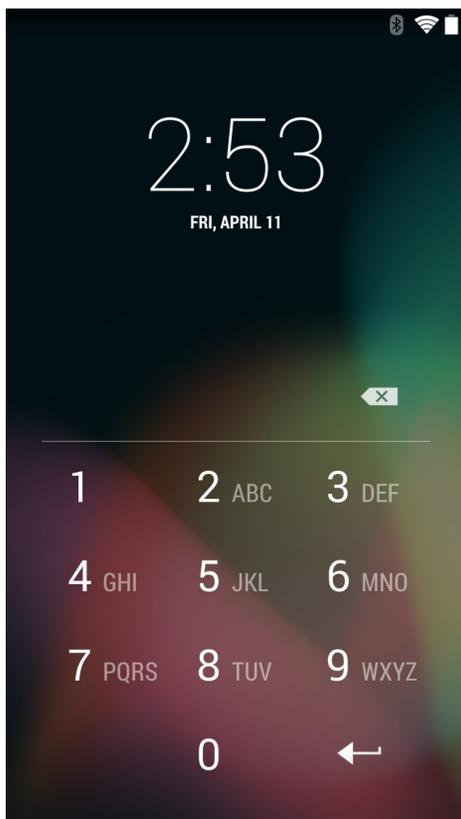
Set Screen Unlock Using Password

Procedure:

1   Touch ⊞.

2   Touch ⚙.

3   Touch 🔒 **Security**.

4   Touch **Screen lock**.

5   Touch **Password**.

6   Touch in the text field.

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

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

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

Figure 103: Password Screen
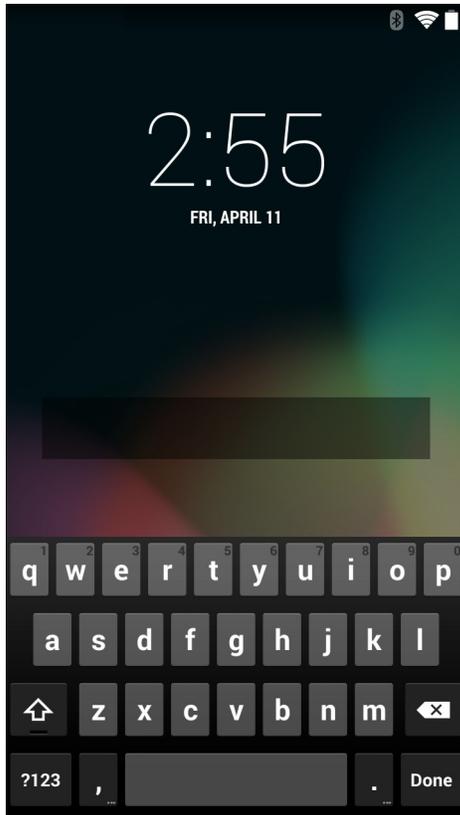
Set Screen Unlock Using Pattern

Procedure:

1 Touch 🔲.

2 Touch ⚙.

3 Touch 🔒 **Security**.

4 Touch **Screen lock**.

5 Touch **Pattern**.

6 Draw a pattern connecting at least four dots.

Figure 104: Choose Your Pattern Screen
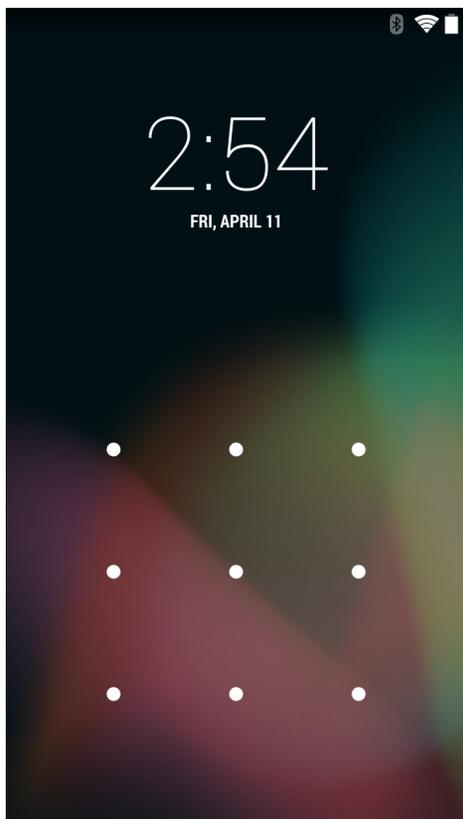
7   Touch **Continue**.

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.

Multiple User Mode

For Multi-user Mode configuration, see .

Passwords

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

Button Remapping

The TC70's buttons can be programmed to perform different functions or shortcuts to installed applications.

•   Trigger 1- PTT button
•   Trigger 2 - Scan button
•   Trigger 3 - Volume up button

- Trigger 4 - Volume down button
- Search Key - ⬭ button below display.

Remapping a Button

Procedure:

1 Touch ⚙️.

2 Touch ▦ **Key Programmer**.

Figure 105: Key Programmer Screen
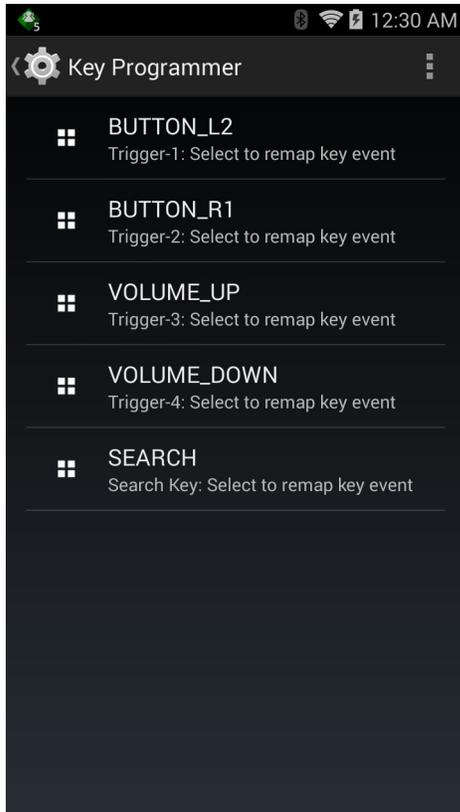
3 Select the button to remap.

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 106: Remapped Button
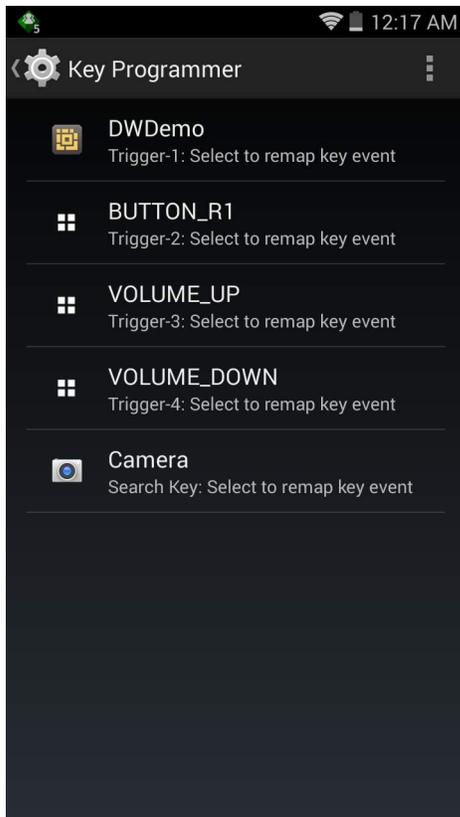
6   Touch ⌂.

Exporting a Configuration File

The Button Remapping configuration can be exported to an xml file and imported into other TC70 devices.

Procedure:

1   Touch ⊕.

2   Touch ⚙.

3   Touch ▦ **Key Programmer**.

4   Touch ≡.

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

6   Copy the xml file from the folder to a host computer. See *USB Communication on page 65* for more information.

Importing a Configuration File

Procedure:

1   Copy the configuration file (`key-config.xml`) from a host computer to the root of the microSD card. See *USB Communication on page 65* for more information.

2   On the TC70, use **File Browser** to move the file from the root of the microSD card to the /enterprise/usr folder.

3 Touch ⚙️ .

4 Touch ▦ **Key Programmer**.

5 Touch ☰ .

6 Touch **Import**.

Creating a Remap File

The administrator can create an xml configuration file and import it into any TC70 device. Use any text editor to create the xml file with the filename: `key-config.xml`.

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

Replace the options for each trigger. See *Keypad Remap Strings on page 169* for a list of available button functions.

Enterprise Reset

To ensure that the configuration persists after an Enterprise Reset:

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

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

Two ways to persist the settings:

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

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

Accounts

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

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

Language Usage

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

Changing the Language Setting

Procedure:

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

The operating system text changes to the selected language.

Adding Words to the Dictionary

Procedure:

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

Keyboard Settings

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

- Android Keyboard
- Japanese IME
- Chinese keyboard

PTT Express Configuration

Refer to the *PTT Express User Guide* for information on configuring the PTT Express Client application.

About Phone

Use **About phone** settings to view information about the TC70. 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 TC70 has been running since being turned on.
- **SW components** - Lists filenames and versions for various software on the TC70.
- **Legal information** - Opens a screen to view legal information about the software included on the TC70.
- **Battery Management** - Displays information about the battery.
- **Battery information** - Displays information about the battery.
- **Hardware config** - Lists part number for various hardware on the TC70.
- **Legal information** - Opens a screen to view legal information about the software included on the TC70.
- **Model number** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

Chapter

7

Application Deployment

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

Security

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

> **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

Procedure:

1 Copy the certificate from the host computer to the root of the microSD card. See for information about connecting the device to a host computer and copying files.

2 Touch 🎛.

3 Touch ⚙.

4 Touch 🔒 **Security**.

5 Touch **Install from SD card**.

6 Navigate to the location of the certificate file.

7 Touch the filename of the certificate to install. Only the names of certificates not already installed display.

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

9 Enter a name for the certificate and touch **OK**. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

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

Configuring Credential Storage Settings

Procedure:

1 Touch ⌨.

2 Touch ⚙.

3 Touch 🔒 **Security**.

- **Trusted credentials** - Touch to display the trusted system and user credentials.
- **Install from SD card** - Touch to install a secure certificate from the microSD card.
- **Clear credentials** - Deletes all secure certificates and related credentials.

Development Tools

Android development 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.

On the Home screen, touch ⌨ > ⚙ > { } **Developer options**. Slide the switch to the **ON** position to enable developer options.

ADB USB Setup

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

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

Application Installation

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

- USB connection, see *Installing Applications Using the USB Connection on page 135*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 136*.
- microSD Card, see *Installing Applications Using a microSD Card on page 137*
- 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.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 65*.

2 On the host computer, copy the application `.apk` file from the host computer to the device.

3 Disconnect the device from the host computer. See *USB Communication on page 65*.

4 On the device, touch 🎛.

5 **Note:**

In **File Browser**, the microSD card path is `/sdcard` or `/storage/sdcard1` and Internal storage path is `/storage/sdcard0`.

Touch 📁 to view files on a microSD card or Internal Storage.

6 Locate the application `.apk` file.

7 Touch the application file to begin the installation process.

8 To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.

Figure 107: Accept Installation Screen
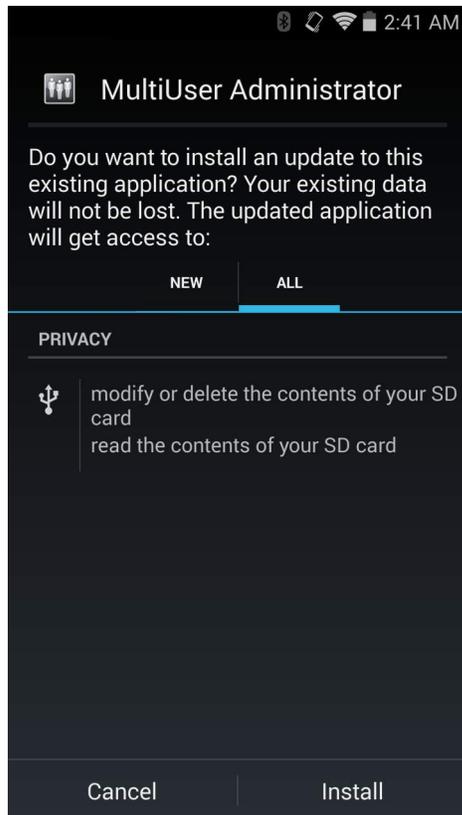
9   Touch **Open** to open the application or **Close** to exit the installation process. The application appears in the App list.

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

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

Prerequisites: Ensure that the ADB drivers are installed on the host computer. See *ADB USB Setup on page 135*.

Procedure:

1   Connect the device to a host computer using USB. See *USB Communication on page 65*.

2   Touch ⚙.

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

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

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

6   Touch **OK**.

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

```
adb install <application>
```

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

8   Disconnect the device from the host computer. See *USB Communication on page 65*.

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.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 65*.

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 If hand strap is attached, slide the hand strap clip up toward the top of the TC70 and then lift.

7 Press the two battery latches in.

8 Lift the battery from the TC70.

9 Lift the access door.

10 Insert the microSD card.

11 Replace the access door.

12 Insert the battery, bottom first, into the battery compartment in the back of the TC70.

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 TC70.

16 Touch ⊞.

17 **Note:**

In **File Browser**, the microSD card path is `/sdcard` or `/storage/sdcard1`.

Touch 📁 to view files on the microSD card.

18 Locate the application `.apk` file.

19 Touch the application file to begin the installation process.

20 To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.

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

Uninstalling an Application

Procedure:

1 Touch ⊞.

2 Touch ⚙.

3 Touch 🖼 **Apps**.

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

Figure 108: Downloaded Screen
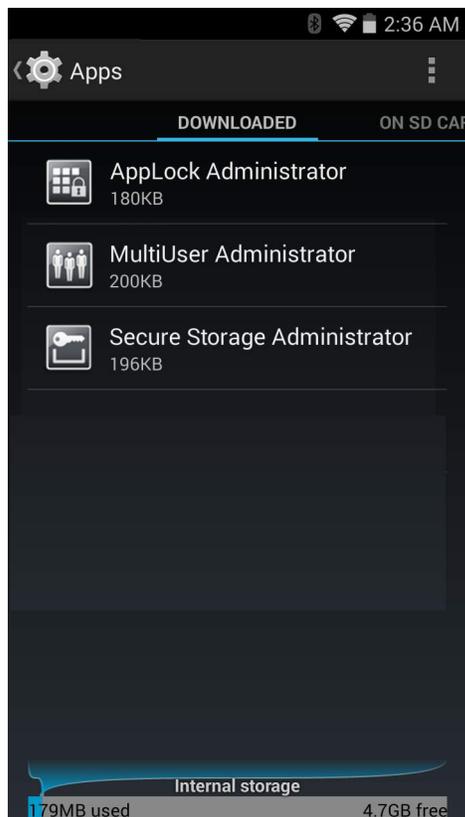
5   Touch the application to uninstall.

6   Touch **Uninstall**.

7   Touch **OK** to confirm.

TC70 System Update

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

Procedure:

1   Download the system update package:

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

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

2   Copy the T700HKXXXPUENxyyzz.zip file to the root directory of the microSD card or to Internal Storage. See *USB Communication on page 65* for more information.

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

4   Touch **Reset**.

5   Press and hold the Scan button.

6   When the System Recovery screen appears, release the button.

Figure 109: System Recovery Screen
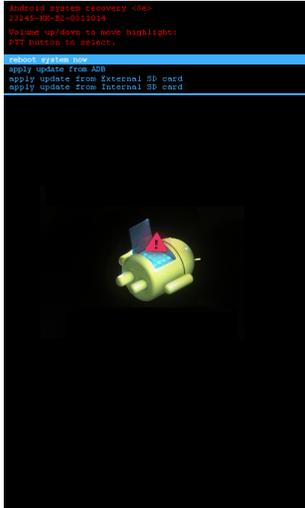
7 Press the Volume Up and Volume Down buttons to navigate to **apply from External SD card** or **apply from Internal SD card**.

8 Press the PTT button.

9 Use the Volume Up and Volume Down buttons to navigate to the `T700HKXXXPUENxyyzz.zip` file .

10 Press the PTT button. The System Update installs and then the TC70 resets.

Storage

The device contains four types of file storage:

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

Random Access Memory

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

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

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

Figure 110: Running Screen
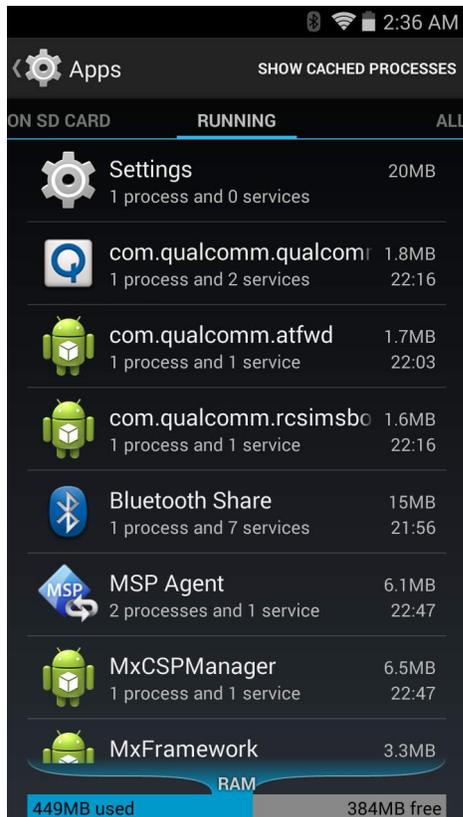
The bar at the bottom of the screen displays the amount of used and free RAM.

External Storage

The TC70 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the TC70 is connected to a host computer. Some applications are designed to be stored on the microSD card rather than in internal memory.

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

Figure 111: Storage Settings
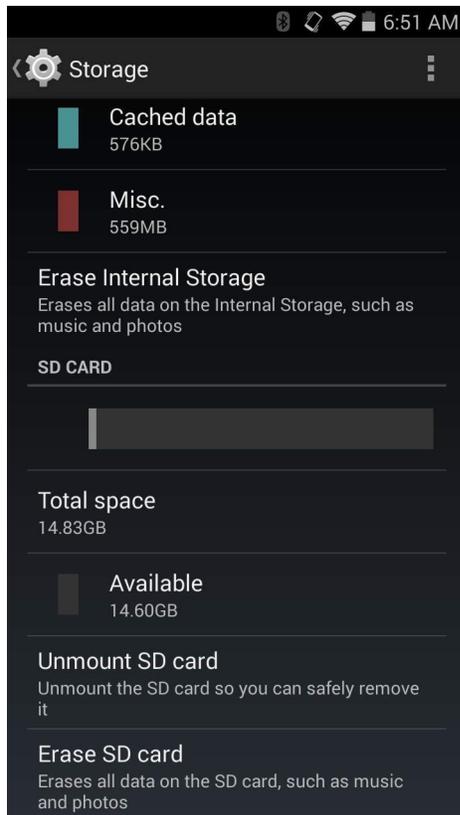
- **Total space** - Displays the total amount of space on the installed microSD card.
- **Apps** - Displays the available space used for applications and media content on the installed microSD card.
- **Pictures, videos** - Displays the available space used for pictures and videos on the installed microSD card.
- **Available** - Displays the available space on the installed microSD card.
- **Unmount SD card** - Unmounts the installed microSD card from the TC70 so that it can be safely removed. This setting is dimmed if there is no microSD card installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase external SD card** - Permanently erases everything on the installed microSD card.

Internal Storage

The TC70 has internal storage. The internal storage content can be viewed and files copied to and from when the TC70 is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

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

Figure 112: Internal Storage Screen
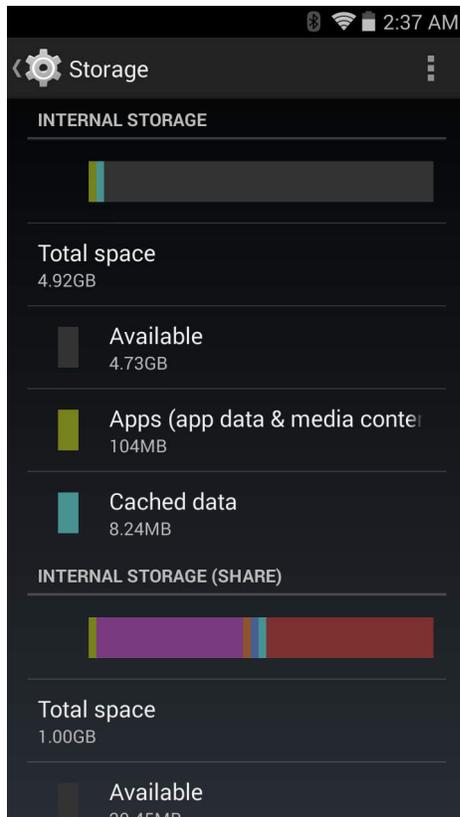
- **Internal Storage**

    - **Total space** - Displays the total amount of space on internal storage (approximately 1.0 GB).

        + **Apps** - Displays the available space used for applications and media content on internal storage.
        + **Available** - Displays the available space on internal storage.

Enterprise Folder

The Enterprise folder (within internal 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.

Figure 113: Manage Applications Screen

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

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

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

When on the **Downloaded**, **All**, or **On SD card** tab, touch ≡ > **Sort by size** to switch the order of the list.

Viewing Application Details

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

* Touch **Force stop** to stop an application.
* Touch **Uninstall** to remove the application and all of its data and settings from the device. See *Uninstalling an Application on page 137* for information about uninstalling applications.
* Touch **Clear data** to delete an application's settings and associated data.
* Touch **Move to USB storage** or **Move to SD card** to change where some applications are stored.
* Cache If the application stores data in a temporary area, lists how much information is stored, and includes a button for clearing it.
* **Launch by default** clears If you have configured an application to launch certain file types by default, you can clear that setting here.

- **Permissions** lists the areas on the device that the application has access to.

Procedure:

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

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

Stopping an Application

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

Procedure:

1 Touch ☰ > **Manage apps**.
2 Swipe the screen to display the **Running** tab.
3 Touch **Show cached processes** or **Show running services** to switch back and forth. The **Running** tab lists the applications, processes, and services that are currently running or that have cached processes and how much RAM they are using.

Figure 114: Running Applications

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

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

Touch **Stop**.

Changing Application Location

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

Procedure:

1 Touch ☰ > **Manage apps**.

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

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

   Applications that are stored on the microSD card are checked.

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

3 Touch an application in the list.

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

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

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

Managing Downloads

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

Procedure:

1 Touch 🔘.

2 Touch 🟢.

3 Touch an item to open it.

4 Touch headings for earlier downloads to view them.

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

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

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

RxLogger

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

Figure 115: RxLogger
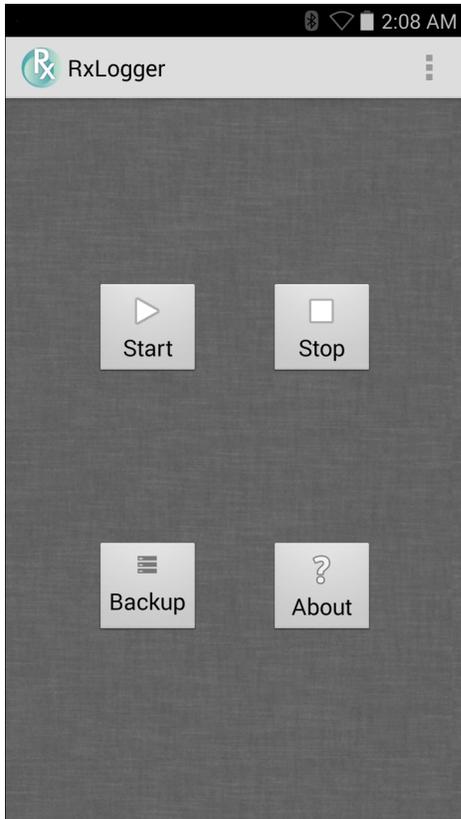
RxLogger Configuration

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

Figure 116: RxLogger Configuration Screen
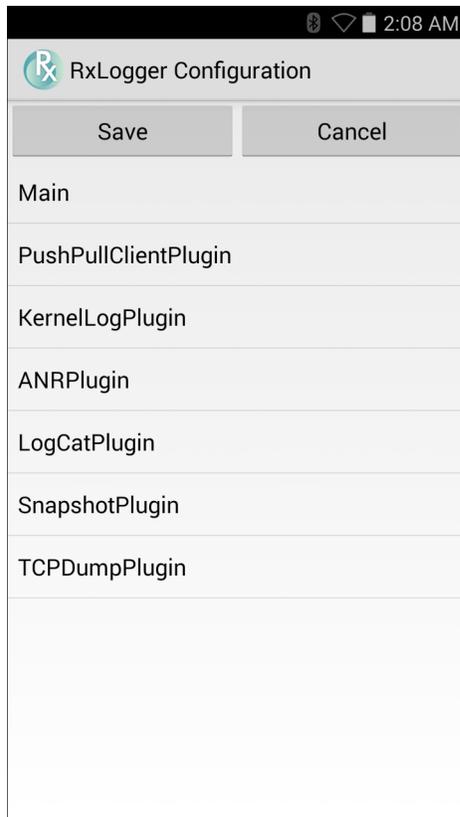
Main Log Plug-in

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

*   **Log Interval** - Specifies the interval, in milliseconds, to poll the collected parameters and write the data to the CSV log file.
*   **Log path** - Specifies the base log path to store the CSV log file. The default to use the default external storage directory which is queried from the Android system.
*   **Log base filename** - The base filename to use for the CSV file before appending the index number of that particular log file. For example, if the base filename is `Resource` and we are rotating through two log files, the actual filename will be: `Resource0.csv` and `Resource1.csv`.
*   **Log file count** - Specifies the number of files to rotate through. Each file is constrained by the Log max size option.
*   **Log max size** - Specifies the maximum size, in kilobytes, of each log file for the main CSV log.
*   **Power**- Enables logging of power related parameters and events. These include battery stats (capacity, current, voltage, etc) and AC/DC power notification events.
*   **System resources** - Enables logging of CPU and memory related items (Avg/current CPU load, program memory, storage memory, process count, etc).
*   **Wifi** - Enables logging of wireless LAN items (WLAN power, signal strength, essid, connected AP, etc).
*   **Cellular** - Enables logging of wireless WAN items (WAN power, network type, signal strength, connected cell tower, etc).
*   **Network** - Enables logging of network items (IP address, default gateway, etc).

- **Bluetooth** - Enables logging of Bluetooth items (Bluetooth power, discoverable, connected, etc).
- **GPS** - Enables logging of GPS data (position, speed, etc).
- **GPS update frequency** - Specifies the frequency of GPS updates requested from the system. This setting can greatly affect battery life when using the tool. Frequent GPS updates will use a lot of power and the effects are greater if the device is indoors where a position cannot be obtained.
- **Output** - The output is a set of comma separated files containing the requested data. The number of files and the file size is determined by the configuration. These files can be viewed using Microsoft Excel.

Snapshot Plug-in

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

Logcat Plug-in

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

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

PushPullClient Plug-in

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

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

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

TCPDump Plug-in

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

- **Log path** - Specifies the location to store the TCPDump output log files.
- **Base filename** - Specifies the base filename to use when storing the TCPDump files. The index number of the current log file will be appended to this filename.
- **Log file count** - Specifies the number of log files to cycle through when storing the network traces.
- **Max file size** - Specifies the maximum file size, in megabytes, for each log file created.
- **Output** - The TCPDump plug-in outputs a set of .cap files according to the configurable options. These are binary files and can be opened with Wireshark tool.

ANR Plugin

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

- **Log path** - Specifies the default log path to store the ANR log files.
- **Max file size** - Specifies the maximum file size, in killobytes, of the ANR trace to be copied. If the file is too large, the copy will be skipped. On older devices that append each ANR event to the same trace file the size can get very large. In this case we will avoid expending resources to copy the large file every time.
- **Output** - The ANR plug-in creates text files in the specified log directory that contain the call stacks of application's that have been shut down by the system due to an ANR event.

Kernal Plug-in

- **Enable Plugin** - Enables logging for this kernal buffer.
- **Log path** - Specifies the high level log path for storage of all kernal logs. This setting applies globally to all kernal buffers.
- **Kernal Log filename** - Specifies the base log filename for this kernal buffer. The current file count is appended to this name.
- **Max Kernal log size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Kernal Log interval** - Sets the interval, in milliseconds, on which to flush the log buffer to the file.

- **Kernal Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Output** - The kernal plug-in outputs a series of text files in accordance with the configuration. The files contain the output of the kernal buffer flushed at the specified interval.

Configuration File

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

Enabling Logging

Procedure:

1 Touch ⊞.

2 Touch ℞.

3 Touch **Start**.

4 Touch ⌂.

Disabling Logging

Procedure:

1 Touch ⊞.

2 Touch ℞.

3 Touch **Stop**.

4 Touch ⌂.

Extracting Log Files

Procedure:

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

Chapter

8

Maintenance and Troubleshooting

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

Maintaining the TC70

For trouble-free service, observe the following tips when using the TC70:

- Do not scratch the screen of the TC70. When working with the TC70, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the TC70 screen.
- The touch-sensitive screen of the TC70 is glass. Do not to drop the TC70 or subject it to strong impact.
- Protect the TC70 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 TC70 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the TC70. If the surface of the TC70 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.

Battery Safety Guidelines

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

Important:

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

[1] When using sodium hypochlorite (bleach) based products always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.
Due to the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidization (corrosion) when exposed to this chemical in the liquid form (including wipes). Avoid allowing any bleach based product to come in contact with the metal electrical contacts on the device, the battery, or the cradle. In the event that these types of disinfectants come in contact with metal on the device, prompt removal with alcohol-dampened cloth or cotton swab after the cleaning step is critical.

Harmful Ingredients

The following chemicals are known to damage the plastics on the device and should not come in contact with the device: ammonia solutions, compounds of amines or ammonia; acetone; ketones; ethers; aromatic and chlorinated hydrocarbons; 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 TC70

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.

Housing

Using the alcohol wipes, wipe the housing including keys and in-between keys.

Display

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

Camera Window

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

Connector Cleaning

To clean the connectors:

Procedure:

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

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

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

Cleaning Cradle Connectors

To clean the connectors on a cradle:

Procedure:

1 Remove the DC power cable from the cradle.

2 Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.

3 Rub the cotton portion of the cotton-tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not leave any cotton residue on the connector.

4 All sides of the connector should also be rubbed with the cotton-tipped applicator.

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

5 Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.

6 Remove any lint left by the cotton-tipped applicator.

7 If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.

8 Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

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

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.

Troubleshooting

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

TC70

Table 10: Troubleshooting the TC70

Problem	Cause	Solution
When pressing the power button the TC70 does not turn on.	Battery not charged.	Charge or replace the battery in the TC70.
	Battery not installed properly.	Install the battery properly.
	System crash.	Perform a reset.
When pressing the power button the TC70 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 TC70.
Battery did not charge.	Battery failed.	Replace battery. If the TC70 still does not operate, perform a reset.

Table continued…

Problem	Cause	Solution
	TC70 removed from cradle while battery was charging.	Insert TC70 in cradle. The 4,620 mAh battery fully charges in less than six 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.	TC70 not powered on.	Press the **Power** button.
Cannot connect to WLAN.	Access point does not broadcast country code.	Disable 802.11d feature. Touch ⊞ > **Settings** > **Wi-Fi** > ▭ > **Advanced**. Deselect the **Enable 802.11d** checkbox.
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	TC70 removed from cradle or disconnected from host computer during communication.	Replace the TC70 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.
APN is not set up correctly.	See system administrator for APN setup information.	
SIM card not installed properly.	Remove and re-install the SIM card.	
Data plan not activated.	Contact your service provider and ensure that your data plan is enable.	
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.
No sound.	Volume setting is low or turned off.	Adjust the volume.
TC70 shuts off.	TC70 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	The device is not responding.	Reset the device.

Table continued…

Problem	Cause	Solution
not activate the corresponding feature.		
A message appears stating that the TC70 memory is full.	Too many files stored on the TC70.	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 TC70.	Remove user-installed applications on the TC70 to recover memory. Select ⚙ > 🖼 Apps > **Downloaded**. Select the unused program and tap **Remove**.
The TC70 does not decode with reading bar code.	Scanning application is not loaded.	Load a scanning application on the TC70 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 TC70 within proper scanning range.
	TC70 is not programmed for the bar code.	Program the TC70 to accept the type of bar code being scanned. Refer to the EMDK or DataWedge application.
	TC70 is not programmed to generate a beep.	If the TC70 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 TC70 low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or the Global Customer Support Center.
TC70 cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (32.8 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
Cannot unlock TC70.	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.

2-Slot Charge Only Cradle

Table 11: Troubleshooting the 2-Slot Charge only Cradle

Symptom	Possible Cause	Action
LEDs do not light when TC70 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.
	TC70 is not seated firmly in the cradle.	Remove and re-insert the TC70 into the cradle, ensuring it is firmly seated.

Table continued…

Symptom	Possible Cause	Action
	Spare battery is not seated firmly in the cradle.	Remove and re-insert the spare battery into the charging slot, ensuring it is firmly seated.
TC70 battery is not charging.	TC70 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure TC70 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 TC70 is not fully seated in the cradle.	Remove and re-insert the TC70 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.

2-Slot USB/Ethernet Cradle

Table 12: Troubleshooting the 2-Slot USB/Ethernet Cradle

Symptom	Possible Cause	Action
During communication, no data transmits, or transmitted data was incomplete.	TC70 removed from cradle during communications.	Replace TC70 in cradle and retransmit.
	Incorrect cable configuration.	Ensure that the correct cable configuration.
	TC70 has no active connection.	An icon is visible in the status bar if a connection is currently active.
	USB/Ethernet module switch in not in the correct position.	For Ethernet communication, slide the switch to the ⊞ position. For USB communication, slide the switch to the ⏚ position.
LEDs do not light when TC70 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.
	TC70 is not seated firmly in the cradle.	Remove and re-insert the TC70 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 continued…

Symptom	Possible Cause	Action
TC70 battery is not charging.	TC70 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure TC70 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 TC70 is not fully seated in the cradle.	Remove and re-insert the TC70 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.

5-Slot Charge Only Cradle Troubleshooting

Table 13: Troubleshooting the 5-Slot Charge Only Cradle

Problem	Cause	Solution
Battery is not charging.	TC70 removed from the cradle too soon.	Replace the TC70 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.
	TC70 is not inserted correctly in the cradle.	Remove the TC70 and reinsert it correctly. Verify charging is active. Touch ⊞ > ⚙ > 🖼 **About device** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

5-Slot Ethernet Cradle Troubleshooting

Table 14: Troubleshooting the 5-Slot Ethernet Cradle

Problem	Cause	Solution
During communication, no data transmits, or transmitted data was incomplete.	TC70 removed from cradle during communications.	Replace TC70 in cradle and retransmit.

Table continued…

Problem	Cause	Solution
	Incorrect cable configuration.	Ensure that the correct cable configuration.
	TC70 has no active connection.	An icon is visible in the status bar if a connection is currently active.
Battery is not charging.	TC70 removed from the cradle too soon.	Replace the TC70 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.
	TC70 is not inserted correctly in the cradle.	Remove the TC70 and reinsert it correctly. Verify charging is active. Touch ⊞ > ⚙ > 🖼 **About device** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

4-Slot Battery Charger Troubleshooting

Table 15: 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.
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.

Magnetic Stripe Reader MSR-TC7X-SNP1-01

Table 16: Troubleshooting the Magnetic Stripe Reader

Symptom	Possible Cause	Action
MSR cannot read card.	MSR removed from TC70 during card swipe.	Reattach MSR to TC70 and reswipe the card.
	Faulty magnetic stripe on card.	See the system administrator.
	Magnetic stripe on card facing wrong way.	Ensure that the magnetic stripe is oriented correctly with stripe facing away from user.
	MSR application is not installed or configured properly.	Ensure the MSR application is installed on the TC70. Ensure the MSR application is configured correctly.

Chapter

9

Technical Specifications

The following sections provide technical specification for the device.

TC70

Table 17: TC70 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions	Height: 161 mm (6.3 in.) Width: 84 mm (3.3 in.) Depth: 28 mm (1.1 in.)
Weight	376 g (13.3 oz)
Display	4.7 in. High Definition (1280 x 720); exceptionally bright image; optically bonded to touch panel
Touch Panel	Glass analog capacitive touch
Backlight	Light Emitting Diode (LED) backlight
Battery Pack	Rechargeable Lithium Ion 3.7V, 4,620 mAh battery
Expansion Slot	User accessible 32 GB microSD slot with SDHC and SDXC support (FAT32 format only)
Connection Interface	Universal Serial Bus (USB) 2.0 High Speed (host and client)
Notification	Audible tone plus multi-color LEDs, vibration
Voice and Audio	Three microphone support with noise cancellation; vibrate alert; speaker; Bluetooth wireless headset support
Performance Characteristics	
CPU	1.7 GHz multi-core.
Operating System	Android-based AOSP V4.4.2
Memory	1 GB RAM/8 GB Flash
Output Power	USB - 5 VDC @ 500 mA max
User Environment	
Operating Temperature	-20 °C to 50 °C (-4 °F to 122 °F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)

Table continued…

Item	Description
Charging Temperature	0° C to 40° C (32°F to 104°F)
Humidity	5 to 85% non-condensing
Drop Specification	6 ft./1.8 m drop to concrete across full operating temperature range
Tumble	2,000 3.2 ft./1.0 m tumbles; meets and exceeds IEC tumble specifications
Electrostatic Discharge (ESD)	+/-20kVdc air discharge, +/-10kVdc direct discharge, +/-10kVdc indirect discharge
Sealing	IP67 per applicable IEC sealing specifications
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 provides motion-sensing for dynamic screen orientation and power management
Light Sensor	Ambient light sensor to auto adjust display backlight brightness
Wireless LAN Data and Voice Communications	
Radio	IEEE® 802.11a/b/g/n/d/h/I
Data Rates Supported	5GHz: 802.11a/n - up to 150 Mbps 2.4GHz: 802.11b/g/n - up to 72.2 Mbps
Operating Channels	5 GHz: Chan 36 - 165 (5180 - 5825 MHz) 2.4 GHz: Chan 1 - 11 (2412 – 2462 MHz) – North America (FCC and IC) Chan 1 - 13 (2412 - 2472 MHz) – Rest of the World Actual operating channels/frequencies depend on regulatory rules and certification agency
Security	**Security Modes:** Legacy, WPA and WPA2 **Encryption:** WEP (40 and 104 bit), TKIP and AES **Authentication:** TLS, TTLS (MS-CHAP), TTLS (MS-CHAP v2), TTLS (PAP), PEAP (MS-CHAP v2), PEAP (GTC), FAST (MS-CHAP v2), FAST (GTC), LEAP. **Fast Roam:** PMKID, OKC, CCKM
Voice Communications	Voice-over-IP ready, Wi-Fi™-certified, IEEE 802.11a/b/g/n direct sequence wireless LAN, Wi-Fi Multimedia™ (WMM)
Wireless PAN Data and Voice Communications	
Bluetooth	Bluetooth v4.0 Low Energy
Data Capture Specifications	
2D Imager	SE4750-SR – 1D and 2D bar codes.
Near Field Communications (NFC)	Supports ISO 14443 Type A & B, FeliCa, and ISO 15963 tags.

Table continued…

Item	Description
Communication and Messaging	
Workforce Connect Push-to-Talk Express Client (included) for instant push-to-talk communications right out of the box WorkForce Connect Voice Client* (sold separately).	
2D Imager Engine (SE4750-SR) 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
Camera Specifications	
Resolution	**Rear:** 8 Mega pixel auto focus with flash **Front:** 1.3 Mega pixel fixed focus

Table 18: Data Capture Supported Symbologies

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

SE4750-SR 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 19: SE4750-SR Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	**Far**
3 mil Code 39	4.1 in.	4.9 in.
	10.41 cm	12.45 cm
5.0 mil Code 128	3.5 in.	6.8 in.
	8.89 cm	17.27 cm
5 mil PDF417	4.4 in.	6.3 in.
	11.18 cm	16.00 cm
6.67 mil PDF417	3.2 in.	8.1 in.
	8.13 cm	20.57 cm
10 mil Data Matrix	3.3 in.	8.5 in.
	8.38 cm	21.59 cm
100% UPCA	2.0 in.	18.0 in.
	5.08 cm	45.72 cm
15 mil Code 128	2.6 in.	19.8 in.
	6.06 cm	50.29 cm
20 mil Code 39	1.8 in.	27.0 in.
	4.57 cm	68.58 cm

Note: Photographic quality bar code at 18° tilt pitch angle under 30 fcd ambient illumination.

TC70 I/O Connector Pin-Outs

Figure 117: I/O Connector

Pin 1
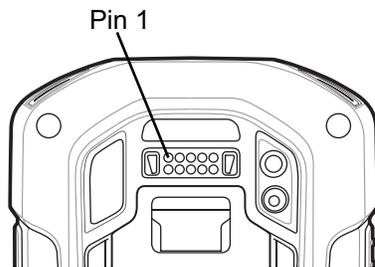
Table 20: I/O Connector Pin-Outs

Pin	Signal	Description
1	GND	Power/signal ground.
2	RXD_MIC	UART RXD + Headset microphone.
3	PWR_IN_CON	External 5.4 VDC power input.
4	TRIG_PTT	Trigger or PTT input.
5	GND	Power/signal ground.
6	USB-OTG_ID	USB OTG ID pin.
7	TXD_EAR	UART TXD, Headset ear.
8	USB_OTG_VBUS	USB VBUS
9	USB_OTG_DP	USB DP
10	USB_OTG_DM	USB DM

2-Slot Charge Only Cradle Technical Specifications

Table 21: 2-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 10.6 cm (4.17 in.)
	Width: 19.56 cm (7.70 in.)
	Depth: 13.25 cm (5.22 in.)
Weight	748 g (26.4 oz.)
Input Voltage	12 VDC
Power Consumption	30 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)

Table continued…

Item	Description
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10 kV contact +/- 10 kV indirect discharge

2-Slot USB/Ethernet Cradle Technical Specifications

Table 22: 2-Slot USB/Ethernet Cradle Technical Specifications

Item	Description
Dimensions	Height: 20 cm (7.87 in.) Width: 19.56 cm (7.70 in.) Depth: 13.25 cm (5.22 in.)
Weight	870 g (30.7 oz.)
Input Voltage	12 VDC
Power Consumption	30 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

5-Slot Charge Only Cradle Technical Specifications

Table 23: 5-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 90.1 mm (3.5 in.) Width: 449.6 mm (17.7 in.)

Item	Description
	Depth: 120.3 mm (4.7 in.)
Weight	1.31 kg (2.89 lbs.)
Input Voltage	12 VDC
Power Consumption	65 watts 90 watts with 4–Slot Battery Charger installed.
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 24: 5-Slot Ethernet Cradle Technical Specifications

Item	Description
Dimensions	Height: 21.7 cm (8.54 in.) Width: 48.9 cm (19.25 in.) Depth: 13.2 cm (5.20 in.)
Weight	2.25 kg (4.96 lbs)
Input Voltage	12 VDC
Power Consumption	65 watts 90 watts with 4-Slot Battery Charger installed.
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

4-Slot Battery Charger Technical Specifications

Table 25: 4–Slot Battery Charger Technical Specifications

Item	Description
Dimensions	Height: 6.06 cm (2.4 in.) Width: 8.65 cm (3.4 in.) Depth: 11.64 cm (4.6 in.)
Weight	225 g (8.0 oz.)
Input Voltage	12 VDC
Power Consumption	40 watts
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	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

Chapter
10

Keypad Remap Strings

Keypad Remap Strings

Table 26: Remap Key Event/Scancodes

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

Table continued…

Key Event	Scancode
VOLUME_UP	115
VOLUME_DOWN	114
CAMERA	212
A	30
B	48
C	46
D	32
E	18
F	33
G	34
H	35
I	23
J	36
K	37
L	38
M	50
N	49
O	24
P	25
Q	16
R	19
S	31
T	20
U	22
V	47
W	17
X	45
Y	21
Z	44
COMMA	51
PERIOD	52
ALT_LEFT	56
ALT_RIGHT	100
SHIFT_LEFT	42
SHIFT_RIGHT	54

Table continued…

Key Event	Scancode
TAB	15
SPACE	57
EXPLORER	150
ENVELOPE	155
ENTER	28
DEL	111
GRAVE	399
MINUS	12
EQUALS	13
LEFT_BRACKET	26
RIGHT_BRACKET	27
BACKSLASH	43
SEMICOLON	39
APOSTROPHE	40
SLASH	53
AT	215
PLUS	78
MENU	139
SEARCH	217
PAGE_UP	59
PAGE_DOWN	60
PICTSYMBOLS	61
SWITCH_CHARSET	62
BUTTON_A	63
BUTTON_B	64
BUTTON_C	65
BUTTON_X	66
BUTTON_Y	67
BUTTON_Z	68
BUTTON_L1	183
BUTTON_R1	184
BUTTON_L2	185
BUTTON_R2	186
BUTTON_THUMBL	187
BUTTON_THUMBR	188

Table continued…

Key Event	Scancode
BUTTON_START	189
BUTTON_SELECT	190
BUTTON_MODE	191

Index

A

approved cleanser *152*

C

cleaning *152*
cleaning instructions *152*
cradle
    connector cleaning *154*

D

data capture options *13*
display
    cleaning *153*

F

Flash *13*

H

harmful ingredients *152*

I

imager *13*

M

memory *13*

O

operating system *13*

R

radios *13*
RAM *13*

S

sensors *162*
soft reset *24*
software version *13*
symbologies *163*

T

troubleshooting
    TC70 *154*

ZEBRA