



TC8000



Touch Computer

Integrator Guide for Android™ Version 4.4.3



TC8000

INTEGRATOR GUIDE FOR ANDROID™
VERSION 4.4.3

MN002411A05

Rev. A

June 2017

Revision History

Changes to the original guide are listed below:

Change	Date	Description
01 Rev A	12/2015	Initial release.
02 Rev A	5/2016	Add Condensation Resistant configuration.
03 Rev A	9/2016	Changes due to software updates.
04 Rev A	3/2017	Correct filenames for Enterprise Reset and factory Reset files.
05 Rev. A	6/2017	In Specifications, add SD card format.

TABLE OF CONTENTS

Revision History	iii
------------------------	-----

Table of Contents

About This Guide

Introduction	xiii
Documentation Set	xiii
Configurations	xiv
Software Versions	xiv
Chapter Descriptions	xv
Notational Conventions	xv
Related Documents and Software	xvi
Service Information	xvi

Chapter 1: Getting Started

Introduction	1-1
Unpacking	1-1
Removing the Screen Protection Film	1-1
Features	1-2
Setup	1-4
Installing the microSD Card	1-4
Installing the Battery	1-7
Charging the Battery	1-8
Starting the TC8000	1-9
Resetting the TC8000	1-10
Performing a Soft Reset	1-10
Performing a Hard Reset	1-10
Performing an Enterprise Reset	1-11
Performing a Factory Reset	1-11

Chapter 2: Accessories

Introduction	2-1
2-Slot USB Charge Cradle	2-4
Setup	2-5
Charging the Device	2-5
Charging the Spare Battery	2-6
Battery Charging	2-6
Main Battery Charging	2-6
Spare Battery Charging	2-6
Charging Temperature	2-6
5-Slot Charge Only Cradle	2-7
Setup	2-8
Charging the TC8000	2-8
Battery Charging	2-9
Main Battery Charging	2-9
Charging Temperature	2-9
5-Slot Charge Only Cradle with Battery Charger	2-10
Setup	2-11
Charging the TC8000	2-11
Battery Charging	2-12
Main Battery Charging	2-12
Spare Battery Charging	2-12
Charging Temperature	2-12
5-Slot Ethernet Cradle	2-13
Charging the TC8000	2-14
Battery Charging	2-15
Main Battery Charging	2-15
Charging Temperature	2-15
Daisy-chaining Ethernet Cradles	2-15
Ethernet Settings	2-16
Configuring Ethernet Proxy Settings	2-16
Configuring Ethernet Static IP Address	2-17
LED Indicators	2-18
Establishing Ethernet Connection	2-18
5-Slot Ethernet Cradle with Battery Charger	2-20
Charging the TC8000	2-21
Battery Charging	2-22
Main Battery Charging	2-22
Spare Battery Charging	2-22
Charging Temperature	2-22
Daisy-chaining Ethernet Cradles	2-23
Ethernet Settings	2-23
Establishing Ethernet Connection	2-23
4-Slot Battery Charger	2-24
Setup	2-24
Charging Spare Batteries	2-25
Charging Temperature	2-25
2-Slot Desk Bracket	2-26
Assembly	2-26
Mounting Cradle	2-26

5-Slot Desktop Bracket	2-28
Assembly	2-28
Mount Cradle	2-29
Cart Mount	2-31
Installation	2-31
5-Slot Cradle Rack Installation	2-34
4-Slot Battery Chargers Rack Installation	2-37
Rack Mount Installation	2-41
5-Slot Cradle Wall Installation	2-44
Bottom Tray Assembly	2-44
Bracket Wall Mounting	2-44
4-Slot Battery Charger Wall Installation	2-47
Bottom Tray Assembly	2-47
Bracket Wall Mounting	2-47
Condensation Resistant Rear Bezel Replacement	2-49

Chapter 3: USB Communication

Connecting to a Host Computer via USB	3-1
Connecting to the TC8000 as a Media Device	3-1
Connecting to the TC8000 as a Camera	3-2
Disconnect from the Host Computer	3-2

Chapter 4: DataWedge Configuration

DataWedge Configuration	4-1
Basic Scanning	4-1
Profiles	4-1
Profile0	4-2
Plug-ins	4-2
Input Plug-ins	4-2
Process Plug-ins	4-3
Output Plug-ins	4-3
Profiles Screen	4-3
Profile Context Menu	4-4
Options Menu	4-4
Disabling DataWedge	4-4
Creating a New Profile	4-5
Profile Configuration	4-5
Associating Applications	4-6
Data Capture Panel	4-7
Bar Code Input	4-10
Enabled	4-10
Scanner Selection	4-10
Decoders	4-10
Decoder Params	4-11
Decode Lengths	4-16
UPC EAN Params	4-16
Reader Params	4-18
Scan Params	4-19

Simulscan Input	4-20
Keystroke Output	4-21
Intent Output	4-21
Intent Overview	4-22
IP Output	4-23
Usage	4-24
Using IP Output with IPWedge	4-24
Using IP Output without IPWedge	4-25
Generating Advanced Data Formatting Rules	4-26
Configuring ADF Plug-in	4-27
Creating a Rule	4-27
Deleting a Rule	4-27
Defining Criteria	4-28
Defining an Action	4-29
Deleting a Rule	4-29
Order Rules List	4-30
Deleting an Action	4-31
ADF Example	4-31
DataWedge Settings	4-34
Importing a Configuration File	4-35
Exporting a Configuration File	4-35
Importing a Profile File	4-35
Exporting a Profile	4-35
Restoring DataWedge	4-36
Configuration and Profile File Management	4-36
Enterprise Folder	4-36
Auto Import	4-36
Programming Notes	4-37
Overriding Trigger Key in an Application	4-37
Capture Data and Taking a Photo in the Same Application	4-37
Soft Scan Feature	4-37
Sample	4-37

Chapter 5: Administrator Utilities

Introduction	5-1
Required Software	5-1
On-device Application Installation	5-1
Multi-user/AppLock Configuration	5-2
Enterprise Administrator Application	5-2
Creating Users	5-2
Adding Packages	5-3
Creating Groups	5-4
Creating Remote Authentication	5-5
Save Data	5-5
Exporting File	5-5
Importing User List	5-6
Importing Group List	5-6
Importing Package List	5-6
Editing a User	5-6

Deleting a User	5-7
Editing a Group	5-7
Deleting a Group	5-7
Editing a Package	5-7
Deleting a Package	5-7
MultiUser Administrator	5-8
Importing a Password	5-8
Disabling the Multi-user Feature	5-9
Enabling Remote Authentication	5-9
Disabling Remote Authentication	5-9
Enabling Data Separation	5-9
Disabling Data Separation	5-10
Delete User Data	5-10
Capturing a Log File	5-10
AppLock Administrator	5-11
Enabling Application Lock	5-11
Disabling Application Lock	5-11
Manual File Configuration	5-11
Groups File	5-11
White List File	5-12
Package List File	5-12
Groups File	5-13
White List File	5-13
Determining Applications Installed on the Device	5-14
Package List File	5-14
Secure Storage	5-16
Installing a Key	5-16
Viewing Key List	5-16
Deleting a Key	5-17
Volumes	5-17
Creating Volume Using EFS File	5-17
Creating a Volume Manually	5-17
Mounting a Volume	5-18
Listing Volumes	5-18
Unmounting a Volume	5-18
Deleting a Volume	5-18
Creating an EFS File	5-19
Off-line Extraction Tool	5-19
Usage	5-19
Creating an Image	5-19
Mounting an Image	5-20
Unmounting an Image	5-20

Chapter 6: Settings

Screen Unlock Settings	6-1
Single User Mode	6-1
Set Screen Unlock Using PIN	6-2
Set Screen Unlock Using Password	6-2
Set Screen Unlock Using Pattern	6-3

Multiple User Mode	6-4
Passwords	6-4
Button Remapping	6-4
Remapping a Button	6-4
Accounts	6-5
Language Usage	6-5
Changing the Language Setting	6-5
Adding Words to the Dictionary	6-5
Keyboard Settings	6-6
PTT Express Configuration	6-6
About Device	6-6

Chapter 7: Application Deployment

Security	7-1
Secure Certificates	7-1
Installing a Secure Certificate	7-1
Development Tools	7-2
ADB USB Setup	7-2
Application Installation	7-3
Installing Applications Using the USB Connection	7-3
Installing Applications Using the Android Debug Bridge	7-4
Installing Applications Using a microSD Card	7-4
Uninstalling an Application	7-5
System Update	7-6
Storage	7-7
Random Access Memory	7-7
Internal Storage	7-8
External Storage	7-9
Enterprise Folder	7-9
Application Management	7-9
Viewing Application Details	7-10
Stopping an Application	7-10
Managing Downloads	7-11

Chapter 8: Maintenance and Troubleshooting

Introduction	8-1
Maintaining the TC8000	8-1
Battery Safety Guidelines	8-1
Cleaning	8-2
Materials Required	8-2
Cleaning the Device	8-3
Housing	8-3
Display	8-3
Scan Exit Window	8-3
Power Connector	8-3
Cleaning Cradle Connectors	8-3
Cleaning Frequency	8-4
Troubleshooting	8-5

Device 8-5
Cradles 8-6

Appendix A: Specifications

Technical Specifications A-1
TC8000 A-1
SE965 Standard Range Laser Decode Zones A-5
SE4750-SR Decode Distances A-6
I/O Connector Pin-Outs A-8
5-Slot Charge Only Cradle Technical Specifications A-10
5-Slot Charge Only Cradle with Battery Charger Technical Specifications A-11
5-Slot Ethernet Cradle Technical Specifications A-12
5-Slot Ethernet Cradle with Battery Charger Technical Specifications A-12
4-Slot Battery Charger Technical Specifications A-13
USB and Charging Cable Technical Specifications A-13
Quick Disconnect Audio Cable Technical Specifications A-14
3.5 mm Audio Cable Technical Specifications A-14

Index

ABOUT THIS GUIDE

Introduction

This guide provides information about using the TC8000 touch computer and accessories.

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

Documentation Set

The documentation set for the TC8000 is divided into guides that provide information for specific user needs.

TC8000 documentation includes:


- **TC8000 Quick Reference Guide** - describes basic set up and operation of the TC8000.
- **TC8000 User Guide** - describes how to set up, operate and program the TC8000 with Android operating system and it's accessories.
- **TC8000 Integrator Guide** (this guide) - describes how to setup and configure TC8000 and accessories.

Configurations


This guide covers the following configurations:

Configuration	Radios			Data Capture				Display	Memory		OS	Sensors					
	802.11 abgn	Bluetooth 4.0	NFC	SE965 Laser Engine	SE4750-SR Imager	SE4750-MR Imager	8 MP Camera	4" WVGA Color	1G RAM/ 4 GB Flash	1G RAM/ 8 GB Flash	Android AOSP V4.4.3	Accelerometer	Proximity Sensor	Gyroscope	Digital Compass	Ambient Light	Condensation Resistant
Standard																	
TC80N0-A000K110NA	X	X		X				X	X		X	X				X	
TC80N0-1000K210NA	X	X			X			X	X		X	X	X			X	
TC80N0-2000K210NA	X	X				X		X	X		X	X	X			X	
TC80N0-A000K110IN	X	X		X				X	X		X	X				X	
TC80N0-1000K210IN	X	X			X			X	X		X	X	X			X	
TC80N0-2000K210IN	X	X				X		X	X		X	X	X			X	
Premium																	
TC80NH-A101K320NA	X	X	X	X			X	X		X	X	X		X	X	X	
TC80NH-1101K420NA	X	X	X		X		X	X		X	X	X	X	X	X	X	
TC80NH-2101K420NA	X	X	X			X	X	X		X	X	X	X	X	X	X	
TC80NH-A101K320IN	X	X	X	X			X	X		X	X	X		X	X	X	
TC80NH-1101K420IN	X	X	X		X		X	X		X	X	X	X	X	X	X	
TC80NH-2101K420IN	X	X	X			X	X	X		X	X	X	X	X	X	X	
TC80N0-A001K31CNA	X	X		X				X		X	X	X		X	X	X	X
TC80N0-1001K31CNA	X	X			X			X		X	X	X		X	X	X	X
TC80N0-2001K31CNA	X	X				X		X		X	X	X		X	X	X	X

Software Versions

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

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

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

- Serial number - Displays the serial number.

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started*, provides information on getting the mobile computer up and running for the first time.
- *Chapter 2, Accessories*, describes the accessories available for the mobile computer and how to use the accessories with the mobile computer.
- *Chapter 3, USB Communication*, explains how to perform Bluetooth functionality on the mobile computer.
- *Chapter 4, DataWedge Configuration*, describes how to use and configure the DataWedge application.
- *Chapter 5, Administrator Utilities*, provides information for using the suite of administrative tools for configuring the TC8000.
- *Chapter 6, Settings*, provides the settings for configuring the TC8000.
- *Chapter 7, Application Deployment*, provides information for developing and managing applications.
- *Chapter 8, Maintenance and Troubleshooting*, includes instructions on cleaning and storing the mobile computer, and provides troubleshooting solutions for potential problems during TC8000 operation.
- *Appendix A, Specifications*, includes a table listing the technical specifications for the TC8000.

Notational Conventions

The following conventions are used in this document:

- “touch computer” refers to the Zebra TC8000 touch computer.
- *Italics* are used to highlight the following:
 - Chapters and sections in this guide
 - Related documents
- **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
 - Icons on a screen
 - Key names on a keypad
 - Button names on a screen.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents and Software

The following documents provide more information about the TC8000.

- *TC8000 Quick Start Guide*, p/n MN002271Axx
- *TC8000 Regulatory Guide*, p/n MN002270Axx
- *TC8000 User Guide*, p/n MN002410Axx
- *Rack/Wall Mount Bracket Installation Guide*, p/n MN002412Axx
- *Desk Mount Installation Guide*, p/n MN002413Axx
- *Hand Strap Installation Guide*, p/n MN002417Axx

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

Service Information

If you have a problem with your equipment, contact Zebra Global Customer Support for your 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
- Model number or product name
- Software type and version number.

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

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

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

CHAPTER 1 GETTING STARTED

Introduction

This chapter describes the features of the TC8000 and explains how to install and charge the battery and how to reset the TC8000.

Unpacking

Carefully remove all protective material from the TC8000 and save the shipping container for later storage and shipping.

Verify that box contains all the equipment listed below:

- TC8000
- Hand strap
- Battery
- Regulatory Guide.

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact Support immediately. See [Service Information on page xvi](#) for contact information.

Removing the Screen Protection Film

A screen protection film is applied to the TC8000 screen to protect the screen during shipping. To remove the screen protector, carefully lift the thin film off the display.

Features

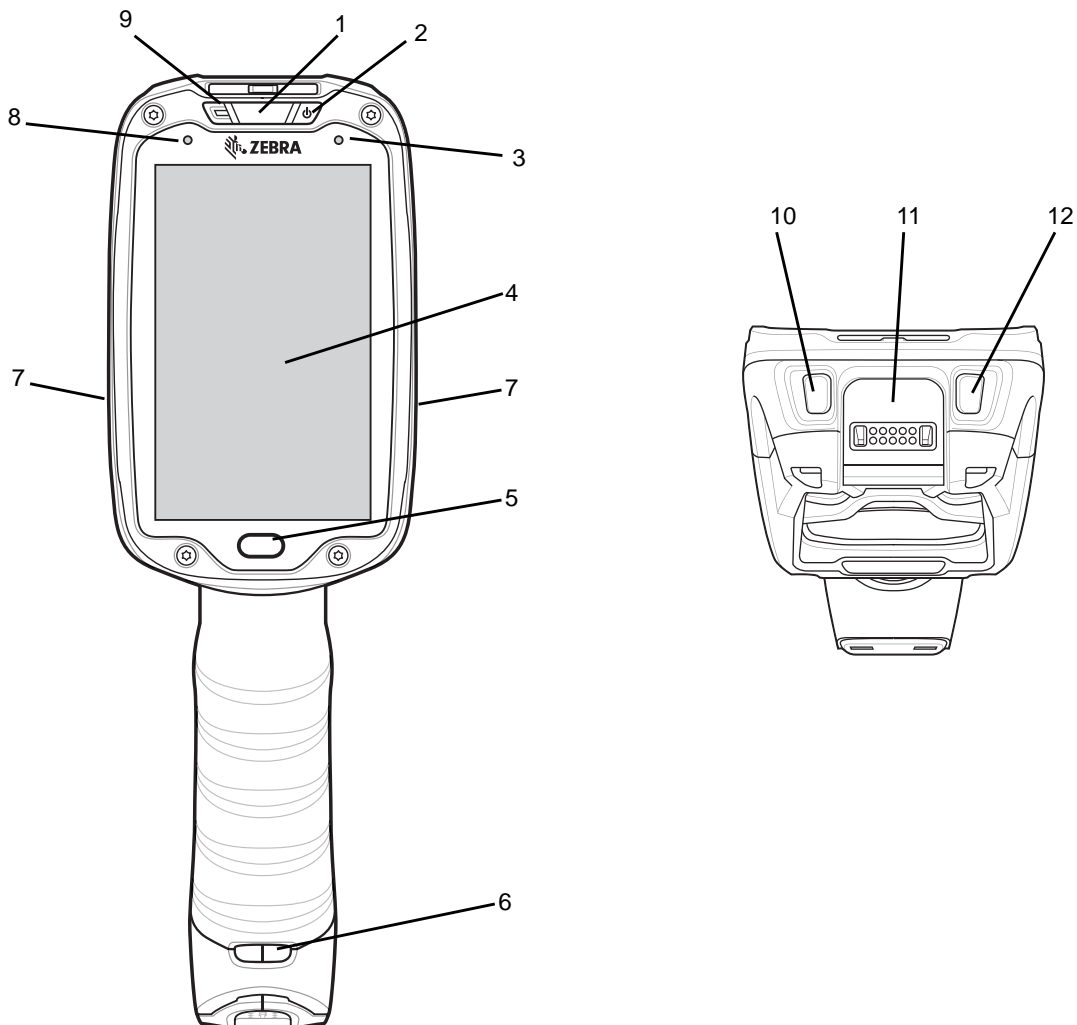


Figure 1-1 Front View

Table 1-1 Front View Descriptions

Number	Item	Function
1	Charging/Scan LED	Indicates battery charging status while charging, good decode indication during data capture and application generated notifications.
2	Power Button	Turns the display on and off. Press and hold to reset the device and power off.
3	Blue Indication LED	User programmable LED.
4	Display	Displays all information needed to operate the TC8000.
5	Touch Button	Press to select items.

Table 1-1 Front View Descriptions (Continued)

Number	Item	Function
6	Hand Strap Mounting Point	Use for installing the optional hand strap.
7	Speakers	Provides audio output for video and music playback.
8	Ambient Light Sensor	Determines ambient light for controlling display backlight intensity (optional).
9	Microphone	Use for communication in Headset mode.
10	Volume Up Button	Increases audio volume (programmable).
11	Interface Connector	Provides USB host and client communication, audio and device charging via cables and accessories.
12	Volume Down Button	Decreases audio volume (programmable).

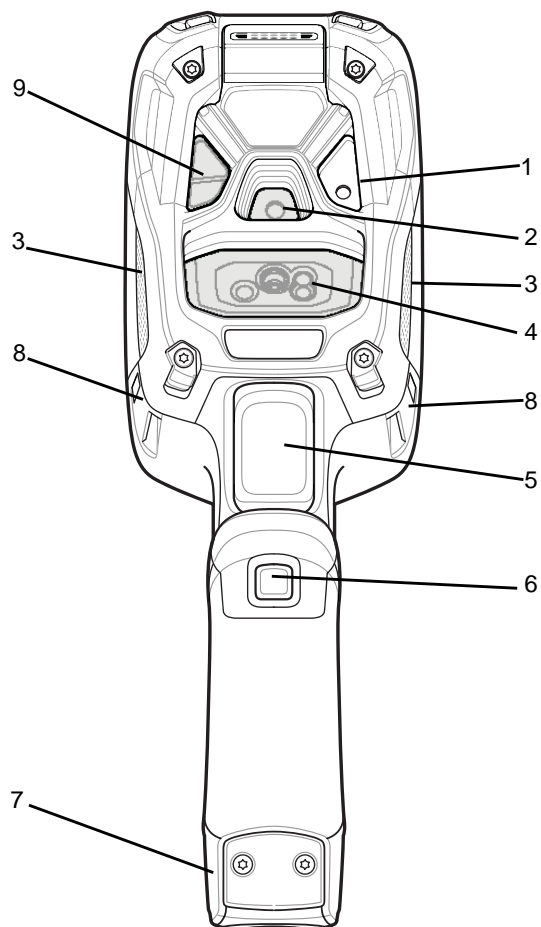
**Figure 1-2** Back View

Table 1-2 Back View Descriptions

Number	Item	Function
1	Camera Flash	Provides illumination for the camera (optional).
2	Camera	Takes photos and videos (optional).
3	Speaker	Provides audio output.
4	Scanner	Provides data capture using the imager or laser scanner.
5	Trigger	Initiates data capture (programmable).
6	Push-To-Talk (PTT) Button	Initiates Push-To-Talk communication (programmable).
7	Battery Pack	Provides power to the device.
8	Hand Strap Mounting Point	Use for installing the optional hand strap.
9	Proximity Sensor	Long range proximity sensor (optional).

Setup

Perform these procedures to start using the TC8000 for the first time.

1. Install a micro secure digital (SD) card (optional).
2. Install the battery.
3. Charge the TC8000.
4. Power on the TC8000.

Installing the microSD Card

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



WARNING! 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.

Remove back bezel only in a dry location.



NOTE The Condensation Resistant configuration has six screws securing the back bezel.

When installing a microSD card on Condensation Resistant configurations, replace the Back Bezel with desiccant pack. See [Condensation Resistant Rear Bezel Replacement on page 2-49](#). Once the Rear Bezel is removed, the desiccant pack absorbs ambient moisture and can lessen the life of the desiccant pack.

1. Remove the Torx T8 screws holding the back bezel in place.

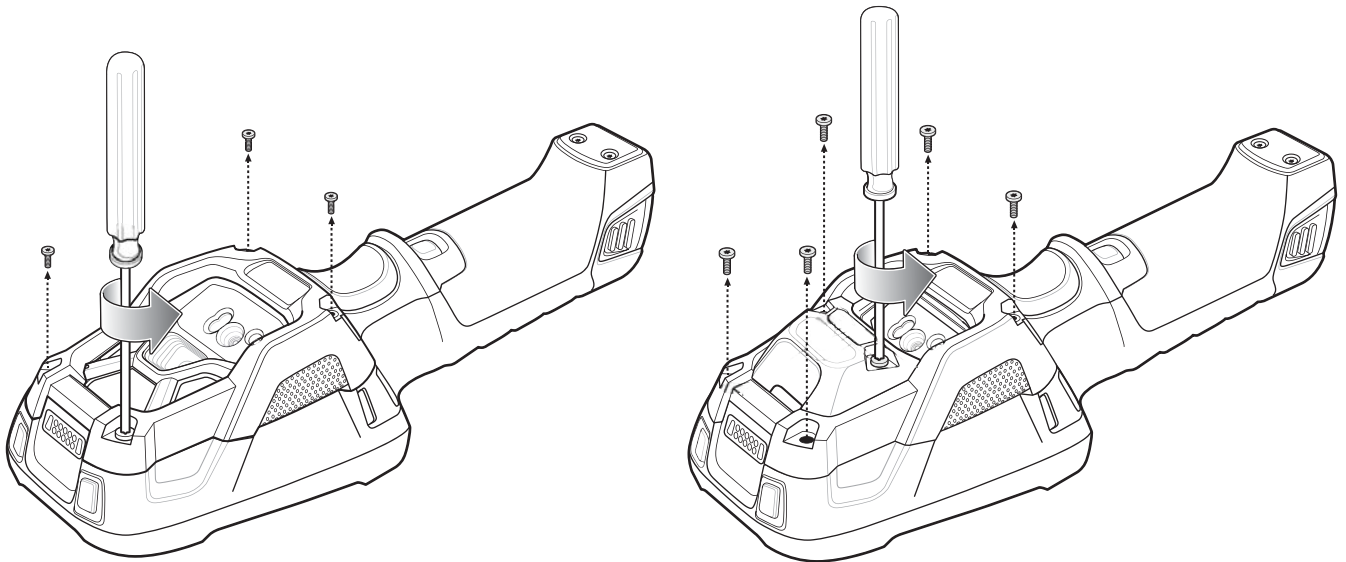


Figure 1-3 *Remove Screws*

2. Lift the bezel to expose the SD slot.

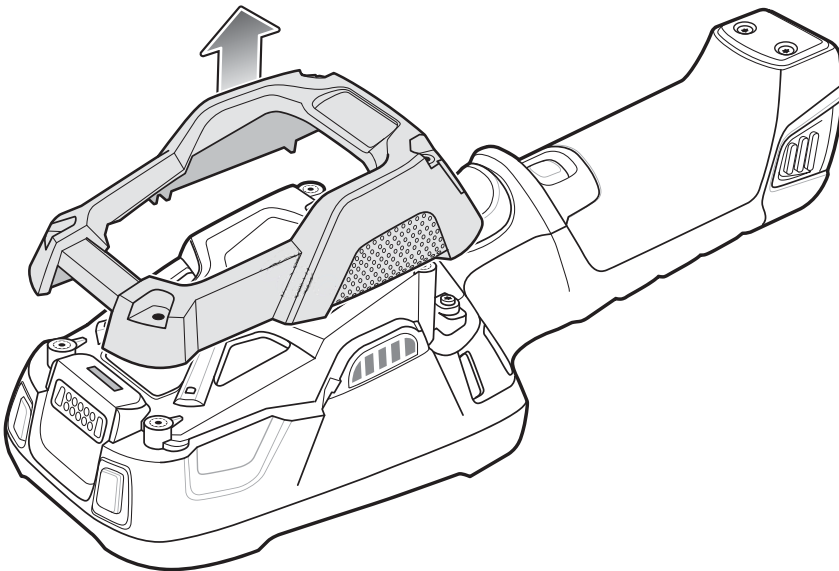


Figure 1-4 *Remove Bezel*

3. Insert the microSD card into the slot with contacts facing the bottom of the device.

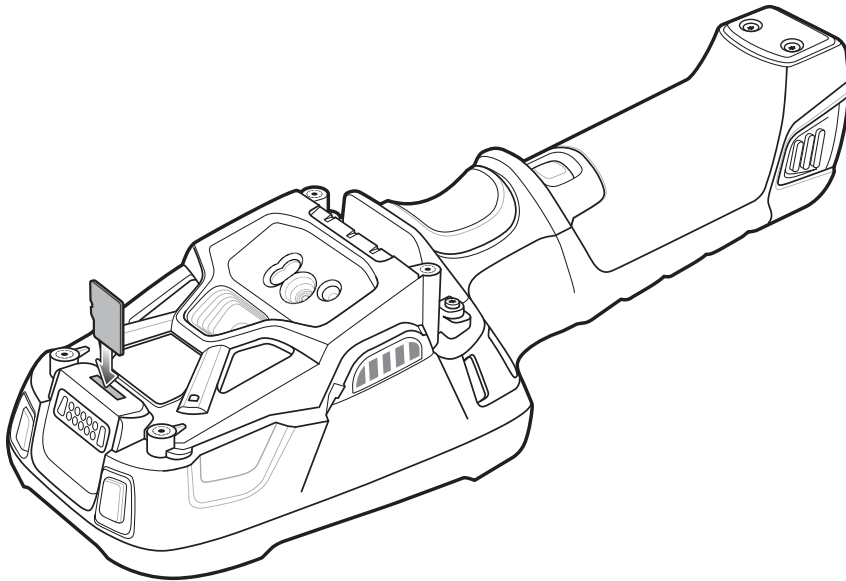


Figure 1-5 *Insert microSD Card*

5. Align the back bezel onto the device.

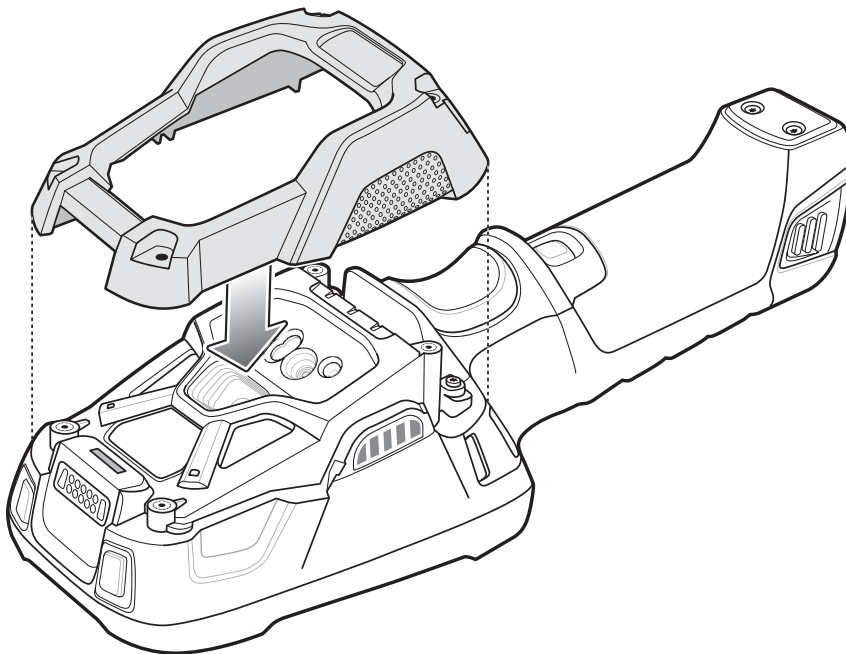


Figure 1-6 *Align Back Bezel*

4. Tighten the four screws using T8 hex screwdriver.
5. Torque to 4.5 kg-cm.

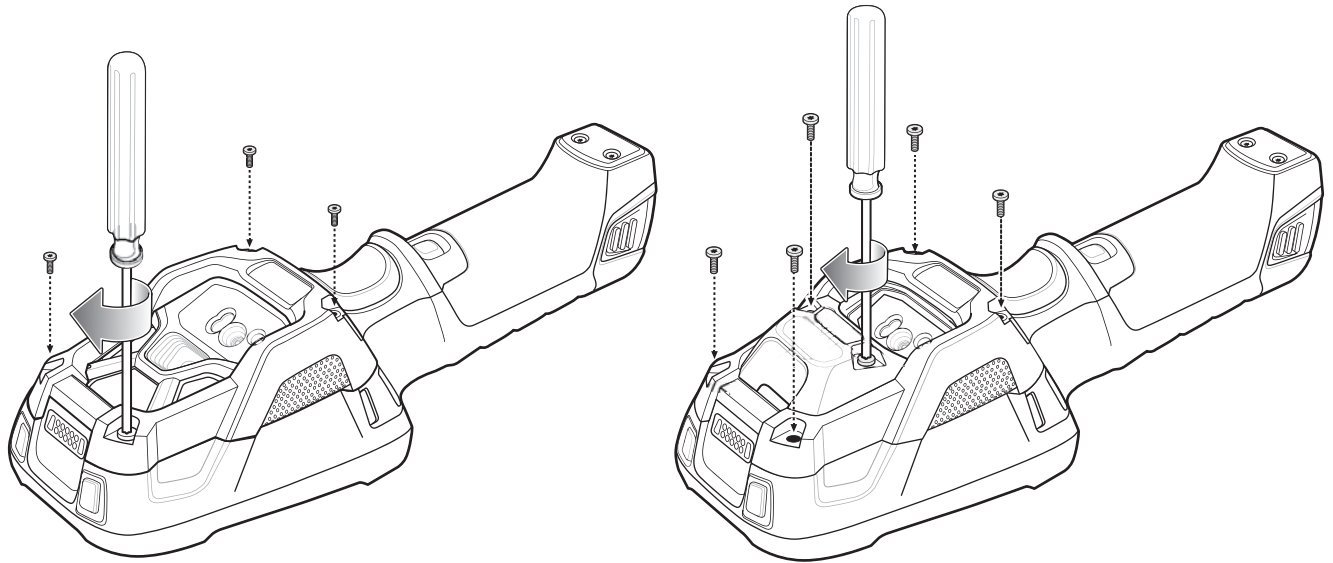


Figure 1-7 *Secure Bezel*

Installing the Battery

To install the battery:

✓ **NOTE** The battery is keyed to ensure that the battery is inserted properly. The notch in the battery must face the back of the device.

1. Align the battery with the notch facing the back of the device.
2. Slide the battery into the handle of the device.

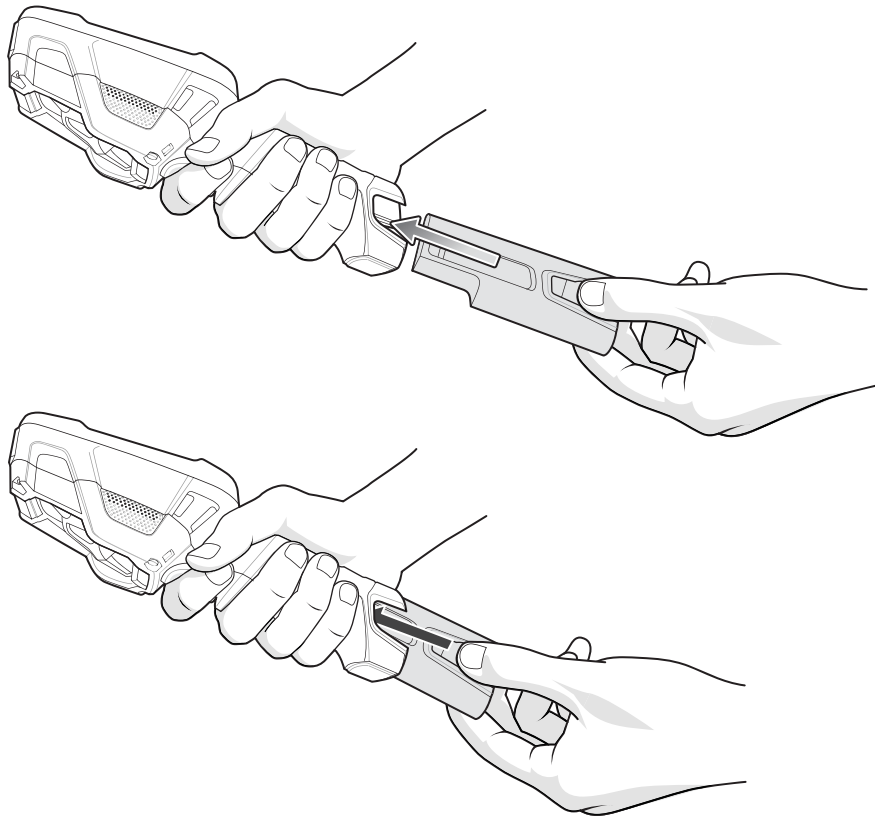


Figure 1-8 *Battery Installation*

3. Snap battery into place.

Charging the Battery

Before using the TC8000 for the first time, charge the battery using a cable or a cradle with the appropriate power supply. For information about the accessories available for the TC8000, see [Chapter 2, Accessories](#).

The TC8000 is equipped with a supercapacitor (supercap) which automatically charges from the fully-charged main battery. The supercap requires approximately 10 minutes to fully charge. The supercap retains random access memory (RAM) data in memory and WLAN connection for at least 30 seconds when the main battery is removed during Hot Swap. After 30 seconds, the WLAN connection is dropped and the RAM data is retained for 20 minutes.

- 4-Slot Battery Charger
- 2-Slot USB Charge Cradle
- 5-Slot Charge Only Cradle
- 5-Slot Ethernet Cradle
- 5-Slot Charge Only Cradle with 4-Slot Battery Charger
- 5-Slot Charge Only Cradle with 4-Slot Battery Charger.

The 6,700 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 TC8000 or accessory always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the

TC8000 or accessory may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC8000 or accessory indicates when charging is disabled due to abnormal temperatures via its LED.

1. To charge the main battery, connect the charging accessory to the appropriate power source.
2. Insert the TC8000 into a cradle or attach to a cable. The TC8000 turns on and begins charging. The Charging/Notification LED blinks amber while charging, then turns solid green when fully charged.

Table 1-3 Charging/Scan LED Charging Indicators

State	Indication
Off	TC8000 is not charging. TC8000 is not inserted correctly in the cradle or connected to a power source. Charger/cradle is not powered.
Solid Amber	Healthy battery is charging.
Solid Green	Healthy battery charging is complete.
Fast Blinking Red (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).
Solid Red	Unhealthy battery is charging or fully charged.



IMPORTANT When trying to power on the device, a quick blink of the charging LED indicates that it does not have enough battery power to turn on. You will need to charge the battery or replace it.

Starting the TC8000

When installed in a cradle, the TC8000 starts automatically as soon as power is applied.

When a charged battery is installed and the TC8000 is turned off, press the Power button to turn on.

When the TC8000 is powered on for the first time, it initializes its system. The splash screen appears for a short period of time.



Figure 1-9 Splash Screen

The splash screen is followed by the boot animation screen and then the **Home Screen**.



Figure 1-10 Home Screen

Resetting the TC8000

There are four reset functions:

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

Performing a Soft Reset

Perform a soft reset if applications stop responding.

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

Performing a Hard Reset



CAUTION Perform a hard reset only if the TC8000 stops responding.

To perform a hard reset, simultaneously press and hold the power button, trigger and PTT button for five seconds. When the device reboots, release the buttons and trigger.

Performing an Enterprise Reset

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

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

1. Download the Enterprise Reset file from the Support Central web site.
2. Copy the TC8K0K3E0REWWxyzz.zip file to the root of the microSD card or the root of the Internal Storage. See [Chapter 3, USB Communication](#).
3. Press and hold the Power button until the menu appears.
4. Touch **Power off**.
5. Touch **OK**. The device turns off.
6. Press and hold the Power button and the trigger.
7. When the Zebra splash screen appears, release the button and trigger.

The System Recovery Screen appears.



Figure 1-11 System Recovery Screen

8. Press the Up and Down Volume buttons to navigate to the **apply update from SD card** or **apply update from internal storage** option.
9. Press the trigger.
10. Press the Up and Down Volume buttons to navigate to the TC8K0K3E0REWWxyzz.zip file.
11. Press the trigger. 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 [System Update on page 7-6](#) for more information.

1. Download the Factory Reset file from the Support Central web site.
2. Copy the `TC8K0K3F0RFWWxyzzyz.zip` file to the root of the microSD card or the root of Internal Storage. See [Chapter 3, USB Communication](#).
3. Press and hold the Power button until the menu appears.
4. Touch **Power off**.
5. Touch **OK**. The device turns off.
6. Press and hold the Power button and the trigger.
7. When the Zebra splash screen appears, release the button and trigger.

The System Recovery Screen appears.



Figure 1-12 System Recovery Screen

8. Press the Up and Down volume buttons to navigate to the **apply update from SD card** or **apply update from internal storage** option.
9. Press the trigger.
10. Press the Up and Down Volume buttons to navigate to the `TC8K0K3F0RFWWxyzzyz.zip` file.
11. Press the trigger. The Factory Reset occurs and then the device resets.

CHAPTER 2 ACCESSORIES

Introduction

The TC8000 accessories provide a variety of product support capabilities. [Table 2-1](#) lists the accessories available.

Table 2-1 *Accessories*

Accessory	Part Number	Description
Cradles		
2-Slot USB Charge Cradle	CRD-TC8X-2SUCHG-01	Provides device and spare battery charging and USB communication with a host computer. Use with power supply, p/n PWRS-14000-148R and country specific grounded AC line cord.
5-Slot Charge Only Cradle	CRD-TC8X-5SCHG-01	Charges up to five TC8000 devices. Use with power supply, p/n PWRS-14000-241R, DC line cord, p/n 50-16002-029R and country specific grounded AC line cord.
5-Slot Ethernet Cradle	CRD-TC8X-5SETH-01	Provides device charging and provides Ethernet communication for up to five devices. Use with power supply, p/n PWRS-14000-241R, DC line cord, p/n 50-16002-029R and country specific grounded AC line cord.
5-Slot Charge Only Cradle with Battery Charger	CRD-TC8X-5SC4BC-01	Charges up to four TC8000 devices and four spare batteries. Use with power supply, p/n PWRS-14000-241R, DC line cord, p/n 50-16002-029R and country specific grounded AC line cord.
5-Slot Ethernet Cradle with Battery Charger	CRD-TC8X-5SE4BC-01	Provides device charging and provides Ethernet communication for up to four devices. Provides charging for four spare batteries. Use with power supply, p/n PWRS-14000-241R, DC line cord, p/n 50-16002-029R and country specific grounded AC line cord.

Table 2-1 *Accessories (Continued)*

Accessory	Part Number	Description
Batteries and Chargers		
Battery	BTRY-TC8X-67MA1-01 BTRY-TC8X-67MA1-10	Replacement battery (single pack). Replacement battery (10-pack).
4-Slot Battery Charger	SAC-TC8X-4SCHG-01	Charges up to four spare batteries. Requires power supply, p/n PWRS-14000-148R and country specific grounded AC line cord.
USB and Charging Cable	CBL-TC8X-USBCHG-01	Provides USB communication and power to the device. Requires power supply PWRS-14000-249R and country specific un-grounded AC line cord.
Audio Accessories		
Quick Disconnect Audio Cable	CBL-TC8X-AUDQD-01	Snaps onto the device and provides audio to a wired headset with Quick Disconnect connector.
3.5 mm Audio Cable	CBL-TC8X-AUDBJ-01	Snaps onto the device and provides audio to a wired headset with 3.5 mm plug.
Mounting Brackets		
2-Slot Cradle Desktop Stand	BRKT-SCRD-SSDK-01	Use for mounting a 2-Slot cradle on a desk.
5-Slot Cradle Desktop Stand	BRKT-SCRD-MSDK-01	Use for mounting a 5-Slot cradle on a desk or rack.
Rack Mount Bracket	BRKT-SCRD-SMRK-01	Use for mounting a 5-Slot cradle or four 4-Slot Battery Chargers on a rack.
Desktop Stand	MNT-TC8X-DKPH-01	Un-powered desktop presentation stand. Allows to use the device on a flat surface (i.e. desktop) for hands-free scanning.
Cart Mount	MNT-TC8X-CMKT-01	Un-powered cart mount. Allows to install the device on carts with up to 2" diameter rail/bar and allows to use the device on hands-free scanning mode. Includes: Includes RAM Mount required for installation.
Forklift Mount	MNT-TC8X-FMKT-01	Un-powered forklift mount. Allows to install the device on a roll bar or square surface of a forklift and allows to use the device on landscape or portrait mode.
Carrying Solutions		
Hand Strap	SG-TC8X-HDSTP-01	Replacement hand strap.
Wrist Lanyard	50-12500-066	Optional lanyard for holding the device.
Quick Draw Soft Holster	SG-TC8X-QDHLST-01	Use to hold the device. Requires the Universal Belt.
Presentation Soft Holster	SG-TC8X-PMHLST-01	Use to hold the device and for hands-free scanning. Requires the Universal Shoulder Strap or Universal Belt.

Table 2-1 Accessories (Continued)

Accessory	Part Number	Description
Universal Belt	11-08062-02R	Use to hold the Quick Draw Soft Holster or the Presentation Soft Holster.
Universal Shoulder Strap	WA6010	Use to hold the Presentation Soft Holster.
Power Supplies		
Power Supply	PWRS-14000-249R	Provides power to the device using the USB and Charging Cable. Requires country specific un-grounded AC line cord.
Power Supply	PWRS-14000-148R	Provides power to the 2-Slot cradles and 4-Slot Spare Battery Charger. Requires country specific grounded AC line cord.
Power Supply	PWRS-14000-241R	Provides power to the 5-Slot Charge Only Cradle, 5-Slot Ethernet Cradle, 5-Slot Charge Only Cradle with Battery Charger and the 5-Slot Ethernet Cradle with Battery Charger. Requires DC Line Cord, p/n 50-16002-029R and country specific grounded AC line cord.
DC Y Cable	25-85993-01R	Provides power from the PWRS-14000-241R power supply to two 4-Slot Battery Chargers.
DC Line Cord	50-16002-029R	Provides power from the power supply to the 5-Slot Charge Only Cradle, 5-Slot Ethernet Cradle, 5-Slot Charge Only Cradle with Battery Charge and 5-Slot Ethernet Cradle with Battery Charger.
Miscellaneous		
Stylus	SG-TC7X-STYLUS-03	Stylus for use with the device (3-pack).
Screen Protectors	MISC-TC8X-SCRN-01	Provides additional protection for display (5-pack).
Replacement Condensation Resistant Back Housing	MISC-TC8X-DSCNT-01	Replacement back housing with dessicate pack.

2-Slot USB Charge Cradle



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

The 2-Slot USB Charge Cradle:

- Provides 5 VDC (nominal) power for operating the TC8000.
- Provide USB communication with a host computer.
- Charges the TC8000's battery.
- Charges a spare battery.

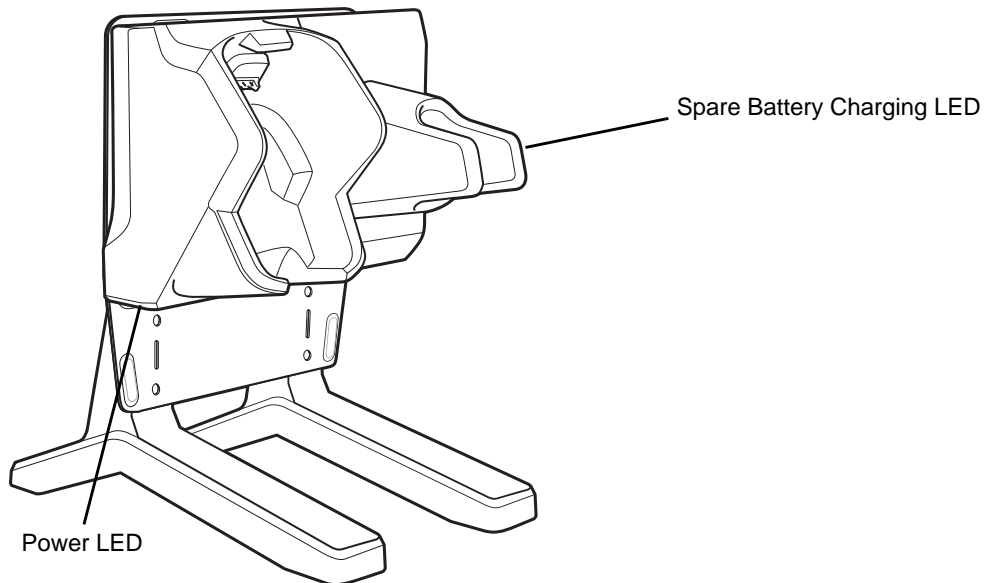


Figure 2-1 2-Slot Charge Only Cradle (Shown on Optional Desk Mount)

Setup

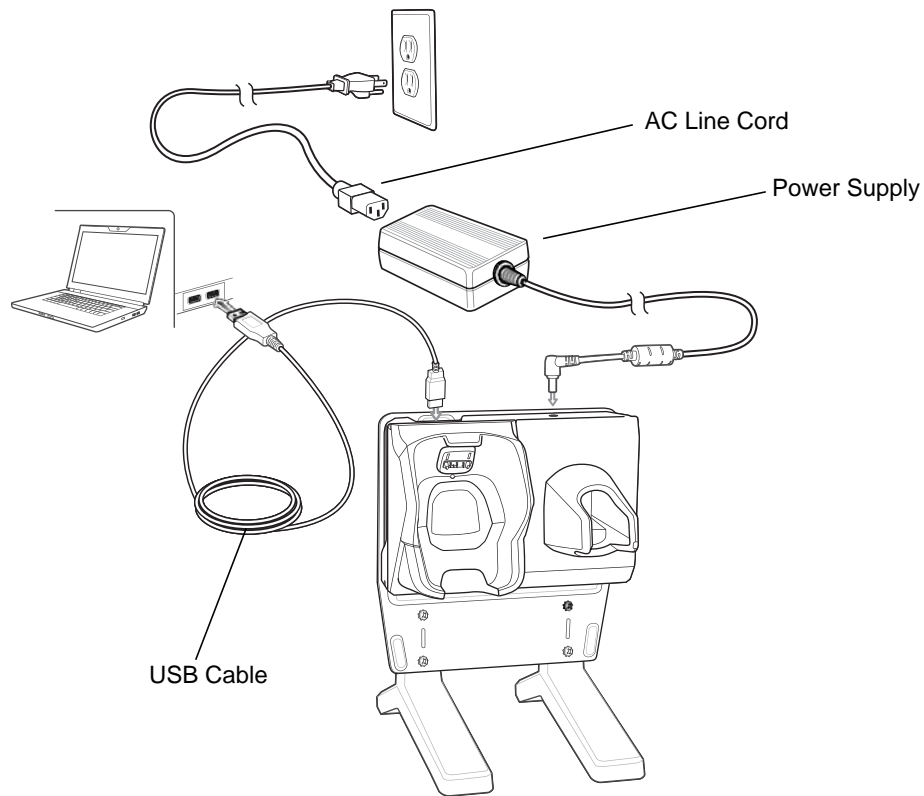


Figure 2-2 Setup (Shown on Optional Desk Mount)

Charging the Device

To charge a device:

1. Insert the TC8000 into the slot to begin charging.

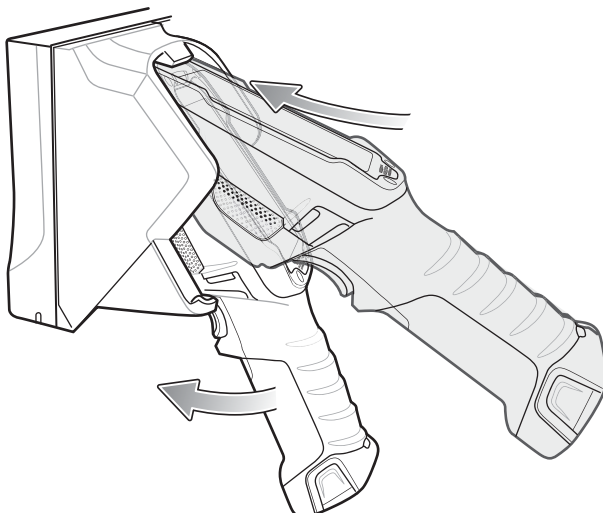


Figure 2-3 Insert TC8000 into Cradle

2. Ensure the TC8000 is seated properly.

Charging the Spare Battery

To charge a spare battery:

1. Insert the battery into the right slot to begin charging.
2. Ensure the battery is seated properly.

Battery Charging

Main Battery Charging

The TC8000's Charging/Notification LED indicates the status of the battery charging in the TC8000. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Spare Battery Charging

The Spare battery Charging LED on the cup indicates the status of the spare battery charging. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Table 2-2 Spare Battery Charging LED Indicators

State	Indication
Off	The battery is not charging. The battery is not inserted correctly in the cradle or connected to a power source. Cradle is not powered.
Solid Amber	Healthy battery is charging.
Solid Green	Healthy battery charging is complete.
Fast Blinking Red (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).
Solid Red	Unhealthy battery is charging or fully charged.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC8000 and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

5-Slot Charge Only Cradle



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

The 5-Slot Charge Only Cradle:

- Provides 5 VDC (nominal) power for operating the TC8000.
- Simultaneously charges up to five TC8000s.

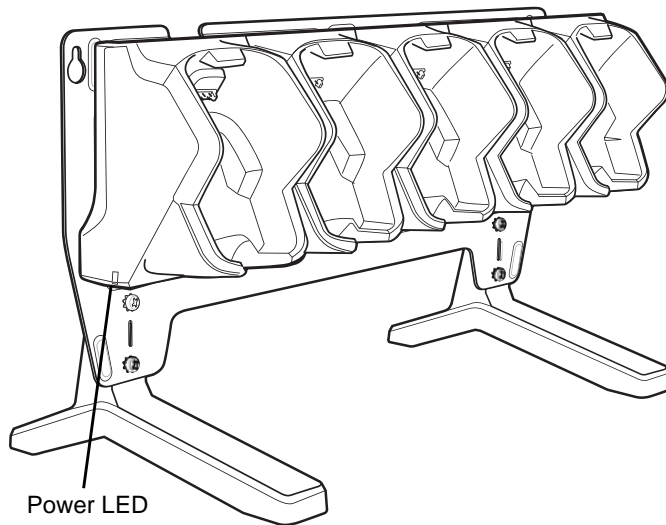


Figure 2-4 5-Slot Charge Only Cradle (Shown on Optional Desk Mount)

Setup

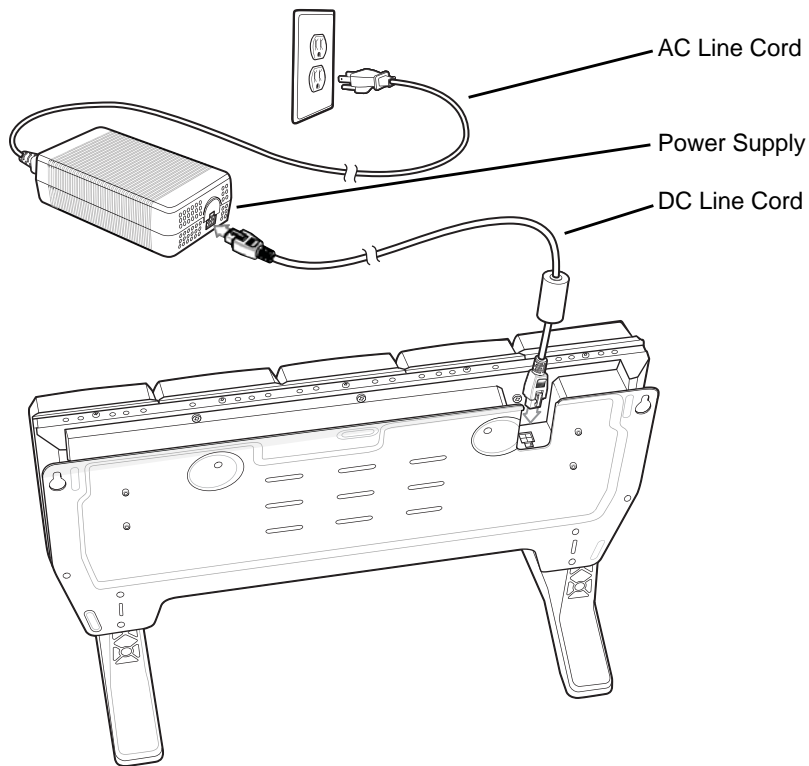


Figure 2-5 5-Slot Charge Only Cradle Setup (Shown on Optional Desk Mount)

Charging the TC8000

1. Insert the TC8000 into a slot to begin charging.

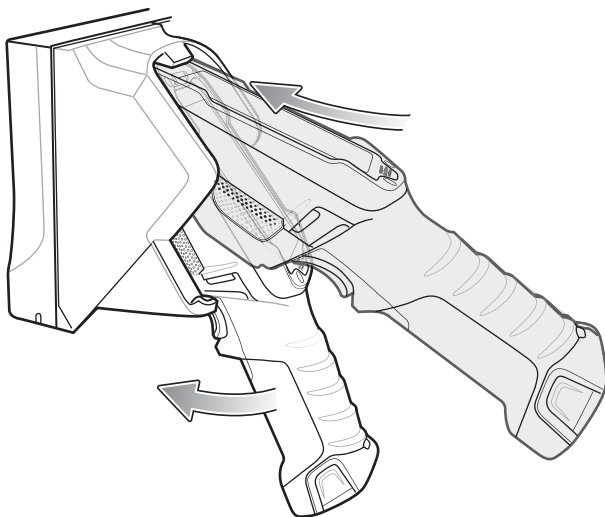


Figure 2-6 Insert TC8000 into Cradle

2. Ensure the TC8000 is seated properly.

Battery Charging

Main Battery Charging

The TC8000's Charging/Notification LED indicates the status of the battery charging in the TC8000. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures.

5-Slot Charge Only Cradle with Battery Charger



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

The 4-Slot Charge Only Cradle with Battery Charger:

- Provides 5 VDC (nominal) power for operating the TC8000.
- Simultaneously charges up to four TC8000s.
- Charges up to four spare batteries.

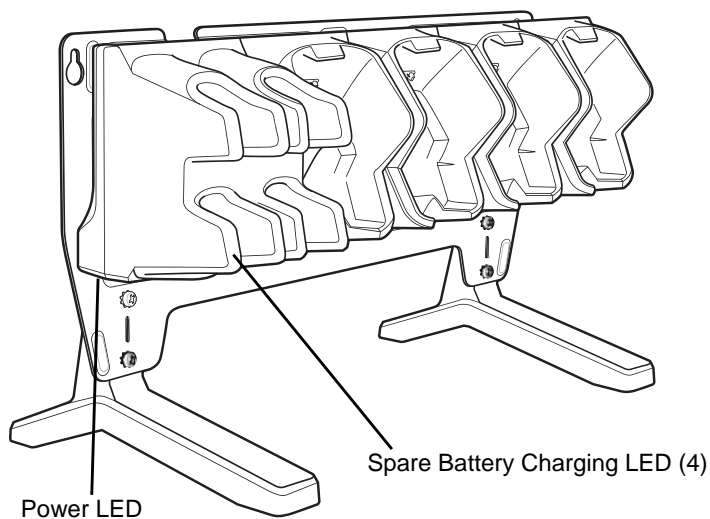


Figure 2-7 5-Slot Charge Only Cradle with Battery Charger (Shown on Optional Desk Mount)

Setup

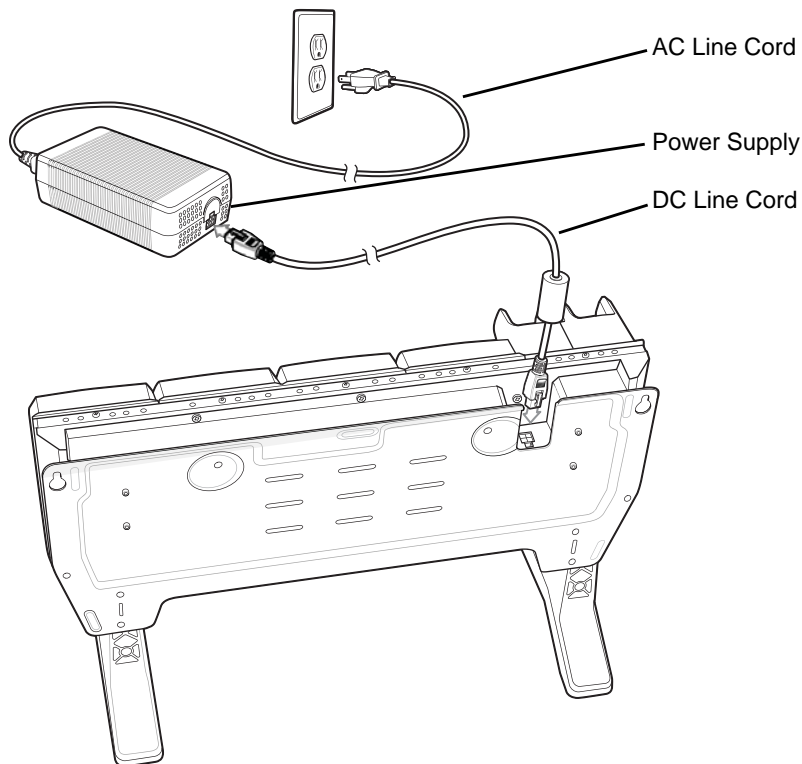


Figure 2-8 5-Slot Charge Only Cradle with Battery Charger Setup (Shown on Optional Desk Mount)

Charging the TC8000

1. Insert the TC8000 into a slot to begin charging.

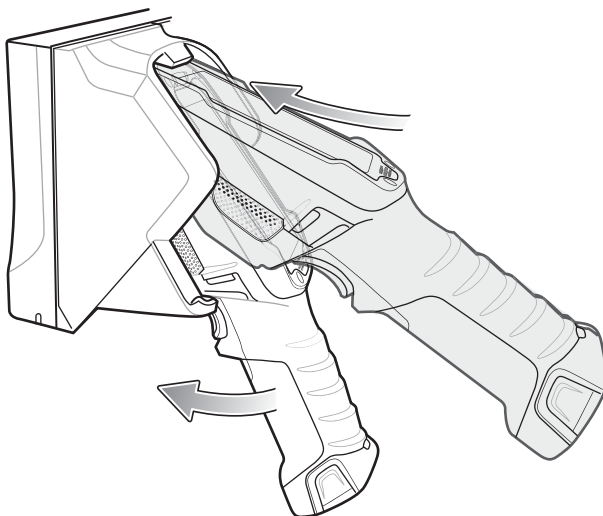


Figure 2-9 Insert TC8000 into Cradle

2. Ensure the TC8000 is seated properly.

Battery Charging

Main Battery Charging

The TC8000's Charging/Notification LED indicates the status of the battery charging in the TC8000. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Spare Battery Charging

The Spare battery Charging LED on the cup indicates the status of the spare battery charging. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Table 2-3 *Spare Battery Charging LED Indicators*

State	Indication
Off	The battery is not charging. The battery is not inserted correctly in the cradle or connected to a power source. Cradle is not powered.
Solid Amber	Healthy battery is charging.
Solid Green	Healthy battery charging is complete.
Fast Blinking Red (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).
Solid Red	Unhealthy battery is charging or fully charged.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures.

5-Slot Ethernet Cradle



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

The 5-Slot Ethernet Cradle:

- Provides 5.0 VDC (nominal) power for operating the TC8000.
- Connects the TC8000 (up to five) to an Ethernet network.
- Simultaneously charges up to five TC8000s.

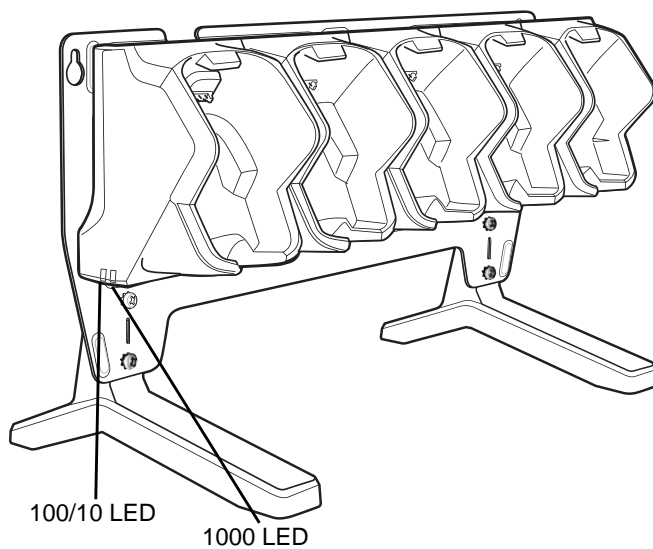


Figure 2-10 5-Slot Ethernet Cradle (Shown on Optional Desk Mount)

To setup the 5-Slot Ethernet cradle:

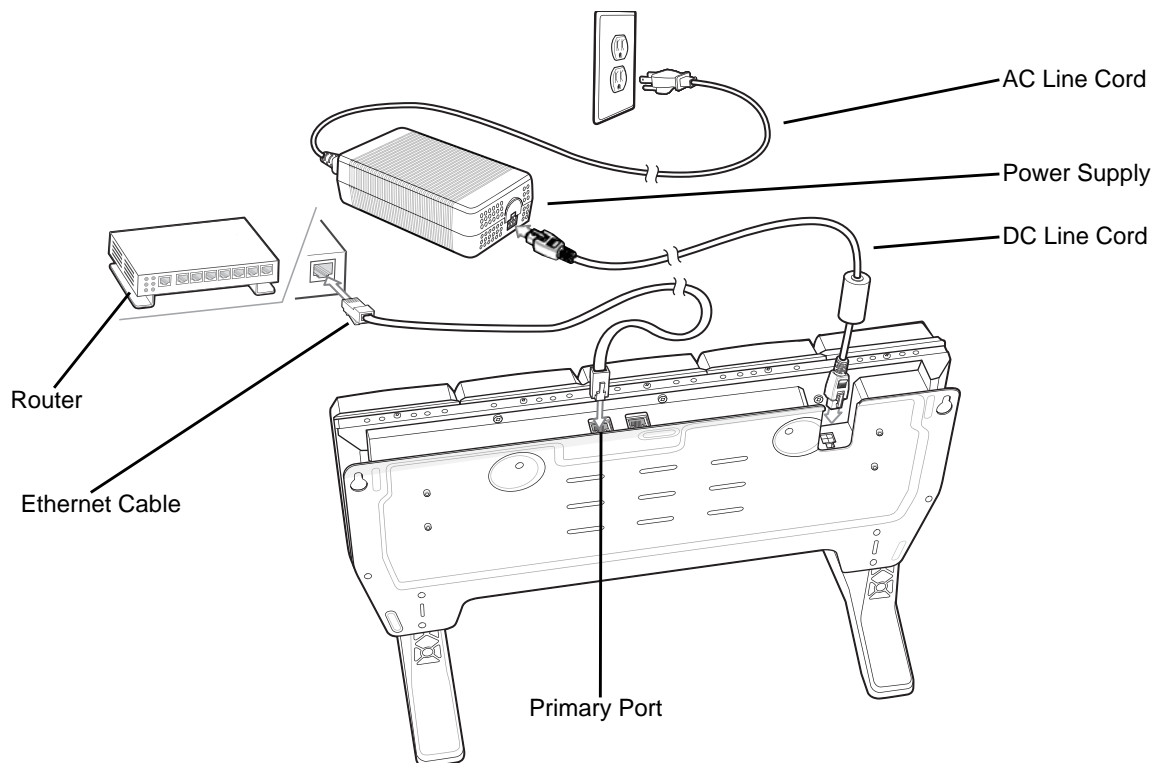


Figure 2-11 5-Slot Ethernet Cradle with Battery Charger Setup (Shown on Optional Desk Mount)

1. Connect the DC line cord to power supply.
2. Connect DC line cord to power input on cradle.
3. Connect Ethernet cable to Ethernet port 1 on cradle.
4. Connect other end of Ethernet cable to router port.
5. Connect the AC line cord to the power supply.
6. Plug the AC line cord into an AC outlet.

Charging the TC8000

To charge the TC8000:

1. Insert the TC8000 into a slot to begin charging.

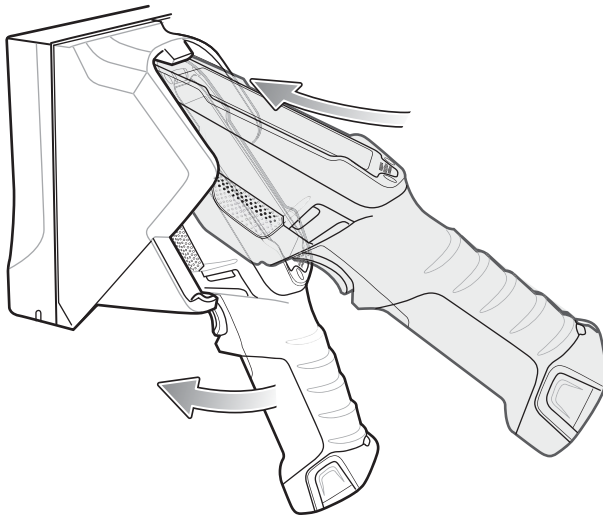


Figure 2-12 *Insert TC8000 into Cradle*

2. Ensure the TC8000 is seated properly.

Battery Charging

Main Battery Charging

The TC8000's Charging/Notification LED indicates the status of the battery charging in the TC8000. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC8000 and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

Daisy-chaining Ethernet Cradles

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

To daisy-chain 5-Slot Ethernet cradles:

1. Connect power to each 5-Slot Ethernet Cradle with Battery Charger.
2. Connect an Ethernet cable to port 1 on the back of the first cradle and to the Ethernet switch.
3. Connect an Ethernet cable to port 2 on the back of the first cradle to port 1 on the back of the second cradle.

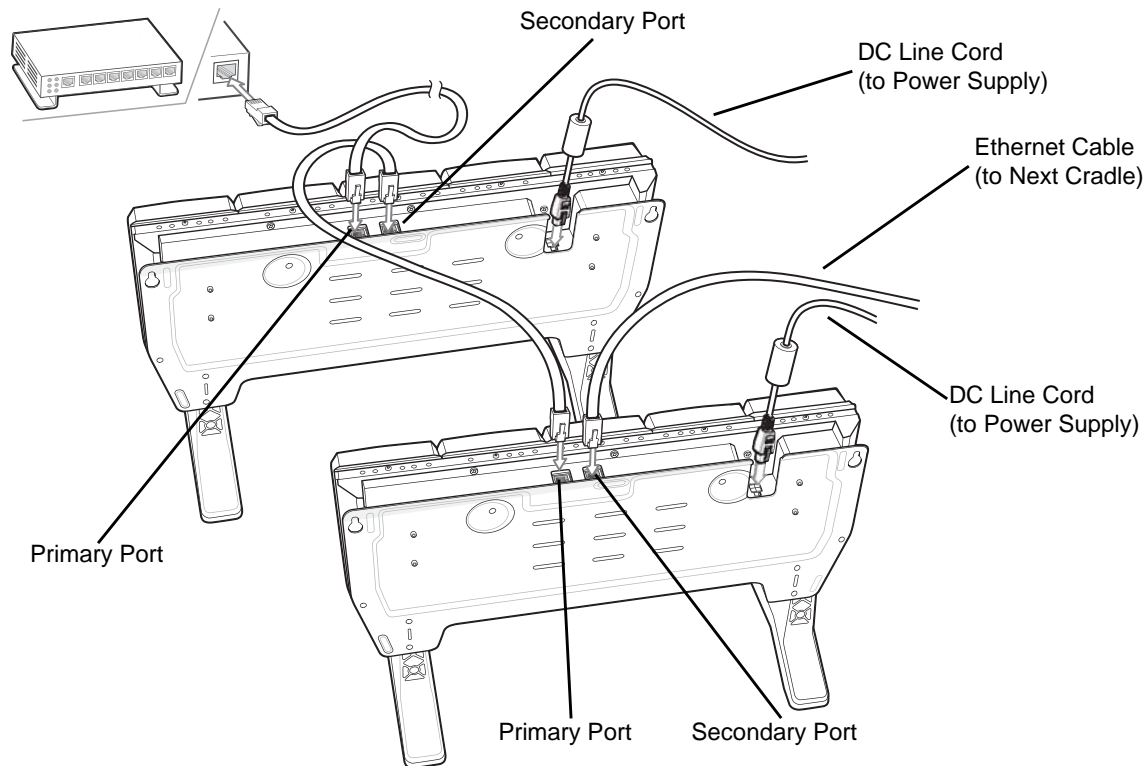


Figure 2-13 *Daisy-Chaining 5-Slot Ethernet Cradles (Shown on Optional Desk Mount)*

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 TC8000 includes Ethernet cradle drivers. After the TC8000, configure the Ethernet connection:

1. Touch  >  >  **Ethernet**.
2. Slide the switch to the **ON** position.
3. Place the TC8000 into the Ethernet cradle slot.
4. Touch and hold **Eth0** until the menu appears.
5. Touch **Modify Proxy**.

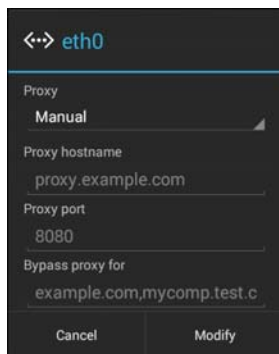



Figure 2-14 Ethernet Proxy Settings




6. Touch the Proxy settings drop-down list and select Manual.
7. In the Proxy hostname field, enter the proxy server address.
8. In the Proxy port field, enter the proxy server port number.

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

9. 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.
10. Touch **Modify**.
11. Touch .

Configuring Ethernet Static IP Address

The TC8000 includes Ethernet cradle drivers. After the TC8000, configure the Ethernet connection:

1. Touch  >  >  **Ethernet**.
2. Slide the switch to the **ON** position.
3. Place the TC8000 into the Ethernet cradle slot.
4. Touch and hold **Eth0** until the menu appears.
5. Touch **Disconnect**.

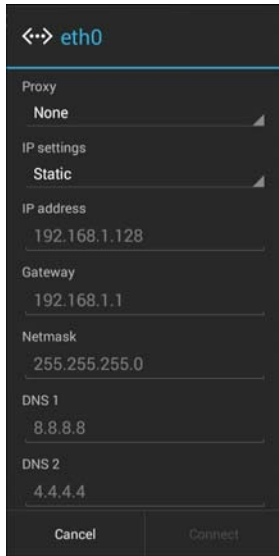



Figure 2-15 Ethernet Static Settings

6. Touch and hold **Eth0** until the menu appears.
7. Touch the IP setting drop-down list and select **Static**.
8. In the **IP address** field, enter the proxy server address.
9. If required, in the **Gateway** text box, enter a gateway address for the TC8000.
10. If required, in the **Network prefix length** text box, enter a the prefix length.
11. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
12. If required, in the **DNS 2** text box, enter a DNS address.
13. Touch **Connect**.
14. Touch .

LED Indicators

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


Table 2-4 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

Establishing Ethernet Connection

1. Touch  >  >  **Ethernet**.

2. Slide the **Ethernet** switch to the **ON** position.
3. Insert the TC8000 into a slot.

The  icon appears in the **Status** bar.

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

5-Slot Ethernet Cradle with Battery Charger



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

The 5-Slot Ethernet Cradle with Battery Charger:

- Provides 5.0 VDC (nominal) power for operating the TC8000.
- Connects the TC8000 (up to five) to an Ethernet network.
- Simultaneously charges up to four TC8000s.
- Simultaneously charges up to four spare batteries.

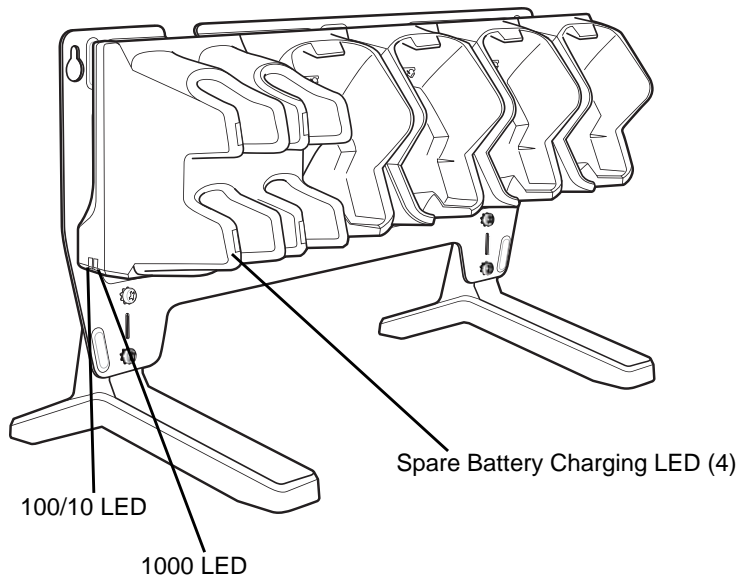


Figure 2-16 5-Slot Ethernet Cradle with Battery Charger (Shown on Optional Desk Mount)

Setup

To setup the 5-Slot Ethernet cradle:

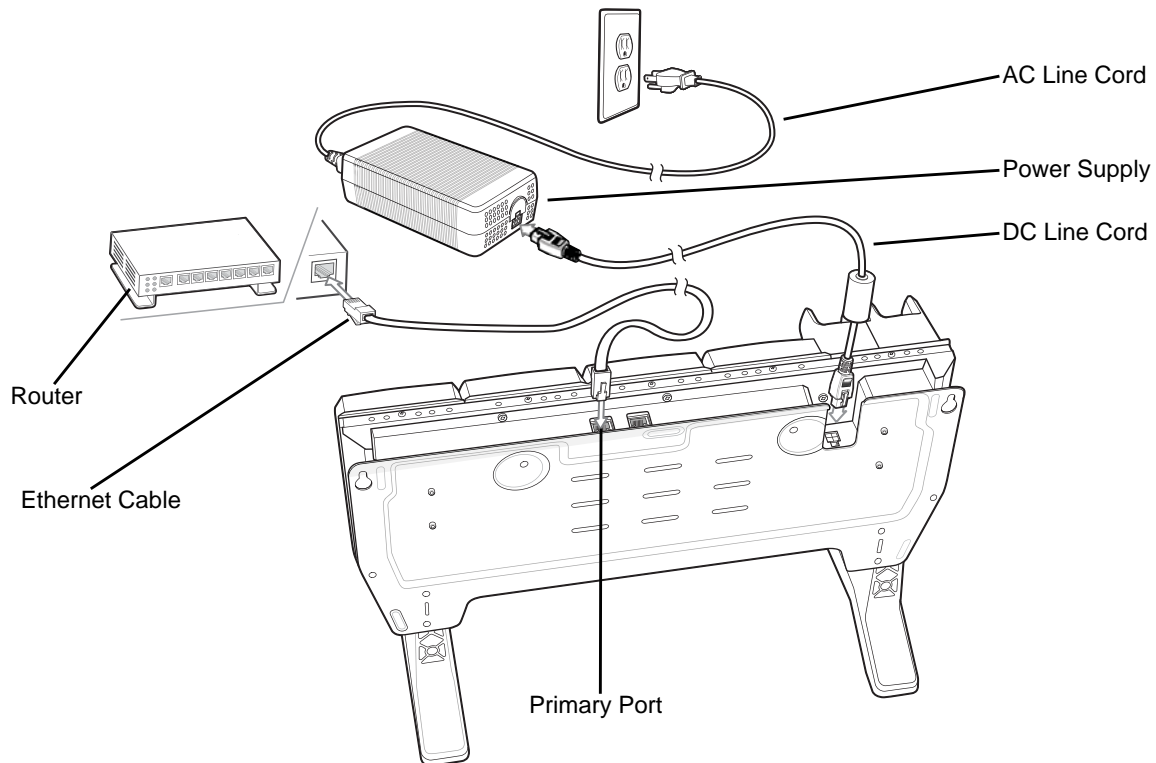


Figure 2-17 5-Slot Ethernet Cradle with Battery Charger Setup (Shown on Optional Desk Mount)

1. Connect the DC line cord to power supply.
2. Connect DC line cord to power input on cradle.
3. Connect Ethernet cable to Ethernet port 1 on cradle.
4. Connect other end of Ethernet cable to router port.
5. Connect the AC line cord to the power supply.
6. Plug the AC line cord into an AC outlet.

Charging the TC8000

To charge the TC8000:

1. Insert the TC8000 into a slot to begin charging.

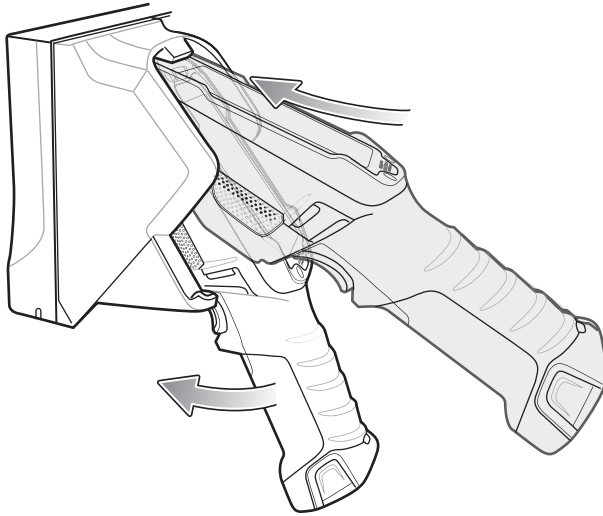


Figure 2-18 *Insert TC8000 into Cradle*

2. Ensure the TC8000 is seated properly.

Battery Charging

Main Battery Charging

The TC8000's Charging/Notification LED indicates the status of the battery charging in the TC8000. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Spare Battery Charging

The Spare battery Charging LED on the cup indicates the status of the spare battery charging. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Table 2-5 *Spare Battery Charging LED Indicators*

State	Indication
Off	The battery is not charging. The battery is not inserted correctly in the cradle or connected to a power source. Cradle is not powered.
Solid Amber	Healthy battery is charging.
Solid Green	Healthy battery charging is complete.
Fast Blinking Red (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).
Solid Red	Unhealthy battery is charging or fully charged.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 or cradle may for small periods of time alternately enable and disable battery charging to keep the battery

at acceptable temperatures. The TC8000 and cradle indicates when charging is disabled due to abnormal temperatures via its LED.



Daisy-chaining Ethernet Cradles

See *Daisy-chaining Ethernet Cradles on page 2-15*.

Ethernet Settings

See *Ethernet Settings on page 2-16*.

Establishing Ethernet Connection

1. Touch  > .
2. Touch **Ethernet**.
3. Slide the **Ethernet** switch to the **ON** position.
4. Insert the TC8000 into a slot.
The icon appears in the **Status** bar.
5. Touch **Eth0** to view Ethernet connection details.

4-Slot Battery Charger

This section describes how to use the 4-Slot Battery Charger to charge up to four TC8000 batteries.

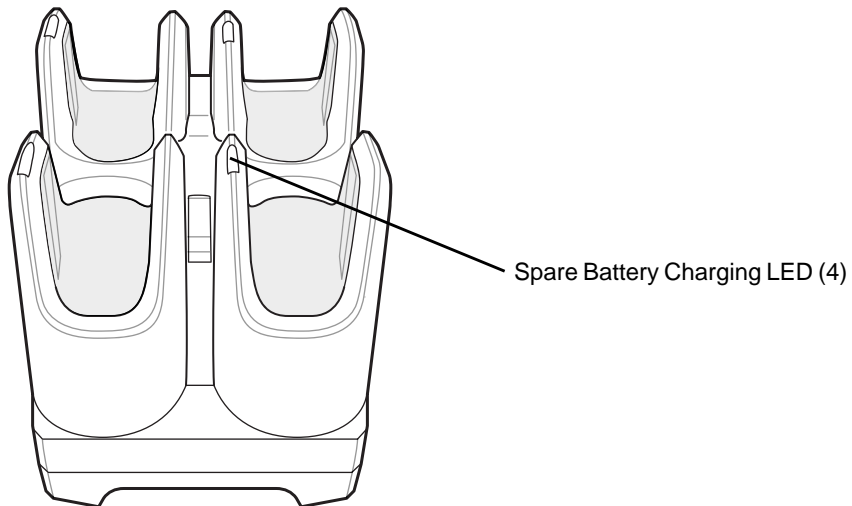


Figure 2-19 4-Slot Battery Charger

Setup

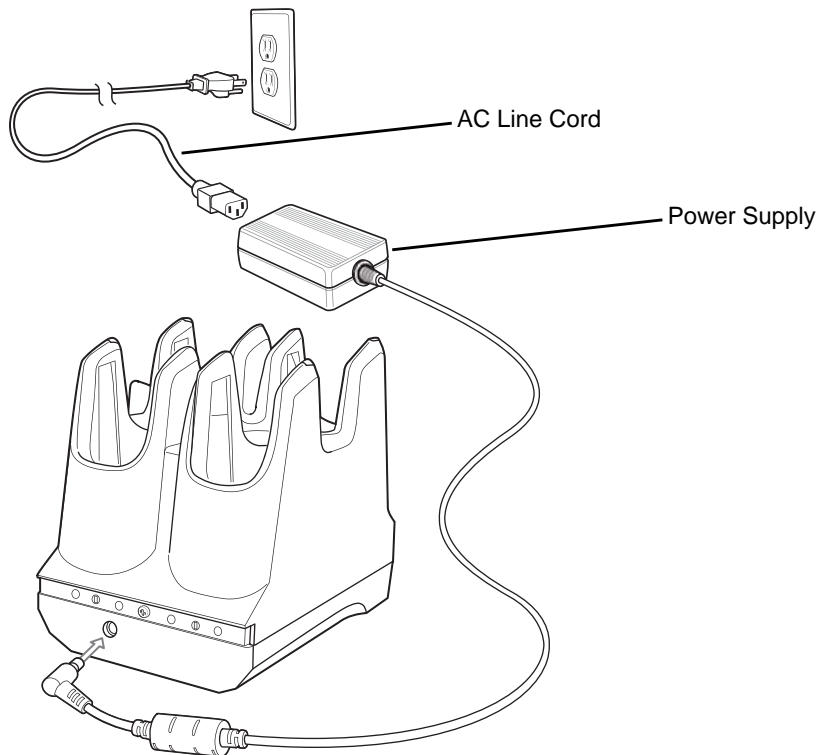


Figure 2-20 Four Slot Battery Charger Power Setup

Charging Spare Batteries

1. Connect the charger to a power source.
2. Insert the battery into a battery charging well and gently press down on the battery to ensure proper contact.

The Spare Battery Charging LED on the cup indicates the status of the spare battery charging. The 6,700 mAh battery fully charges in less than four hours at room temperature.

Table 2-6 *Spare Battery Charging LED Indicators*

State	Indication
Off	The battery is not charging. The battery is not inserted correctly in the cradle or connected to a power source. Cradle is not powered.
Solid Amber	Healthy battery is charging.
Solid Green	Healthy battery charging is complete.
Fast Blinking Red (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).
Solid Red	Unhealthy battery is charging or fully charged.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The TC8000 or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37 °C (+98 °F)) the TC8000 or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC8000 and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

2-Slot Desk Bracket

Use the 2-Slot Desk Mount to mount the 2-Slot USB Charging cradle in a vertical position.

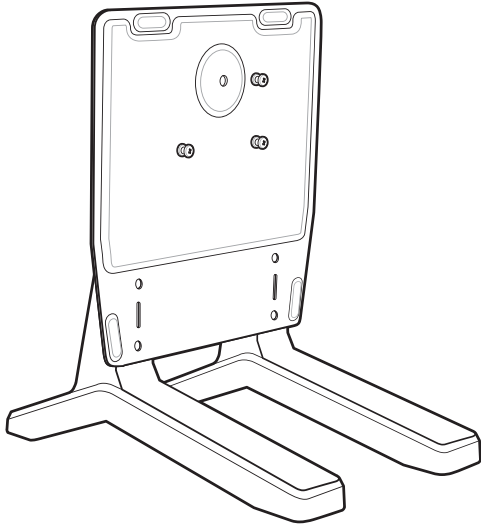


Figure 2-21 2-Slot Desk Mount

Assembly

To assemble the 2-Slot Desk Mount:

1. Align plate mounting holes with holes in feet.

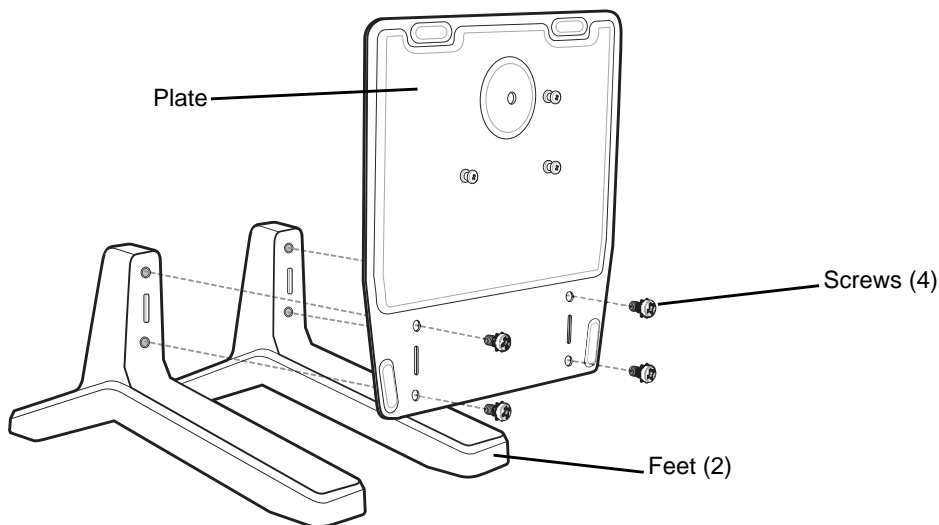


Figure 2-22 Install Feet

2. Secure plate to feet with four screws and four washers.

Mounting Cradle

To mount the cradle:

- 1. Align mounting slots on bottom of cradle with studs on plate.

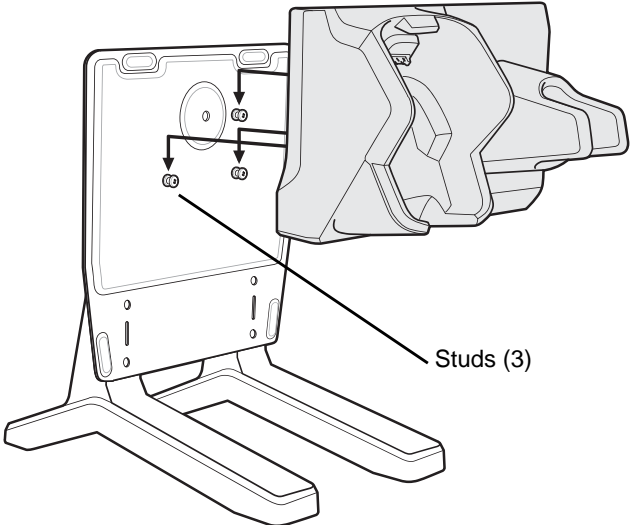


Figure 2-23 *Install Cradle onto Desk Mount*

- 2. Secure cradle to plate using safety screw.

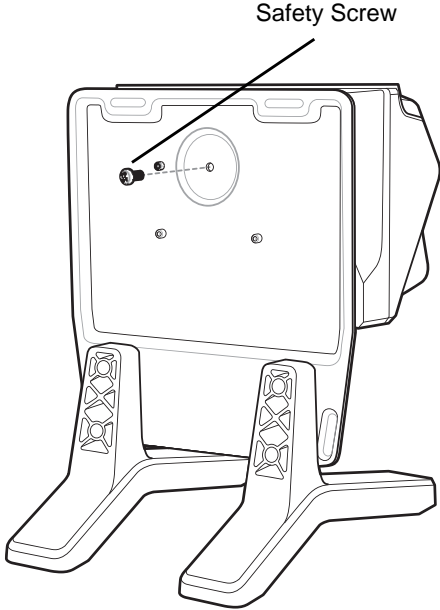


Figure 2-24 *Install Safety Screw*

5-Slot Desktop Bracket

Use the 5-Slot Desk Mount to mount the 5-Slot Charge Only cradles or the 5-Slot Ethernet cradles in a vertical position.

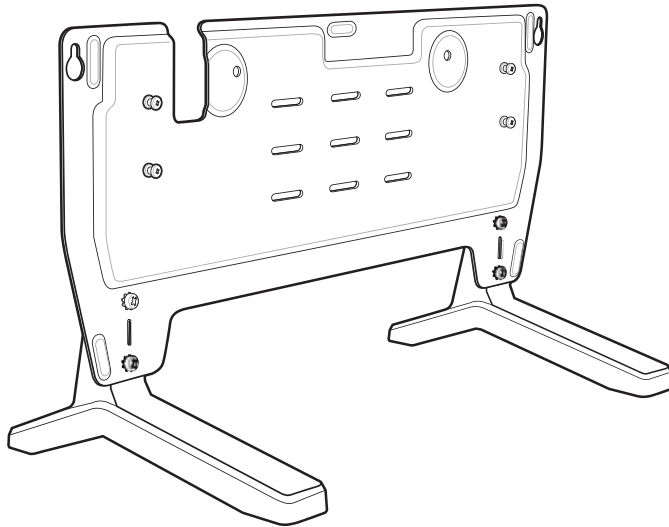


Figure 2-25 5-Slot Desk Mount

Assembly

To assemble the 5-Slot Desk Mount:

1. Align plate mounting holes with holes in feet.

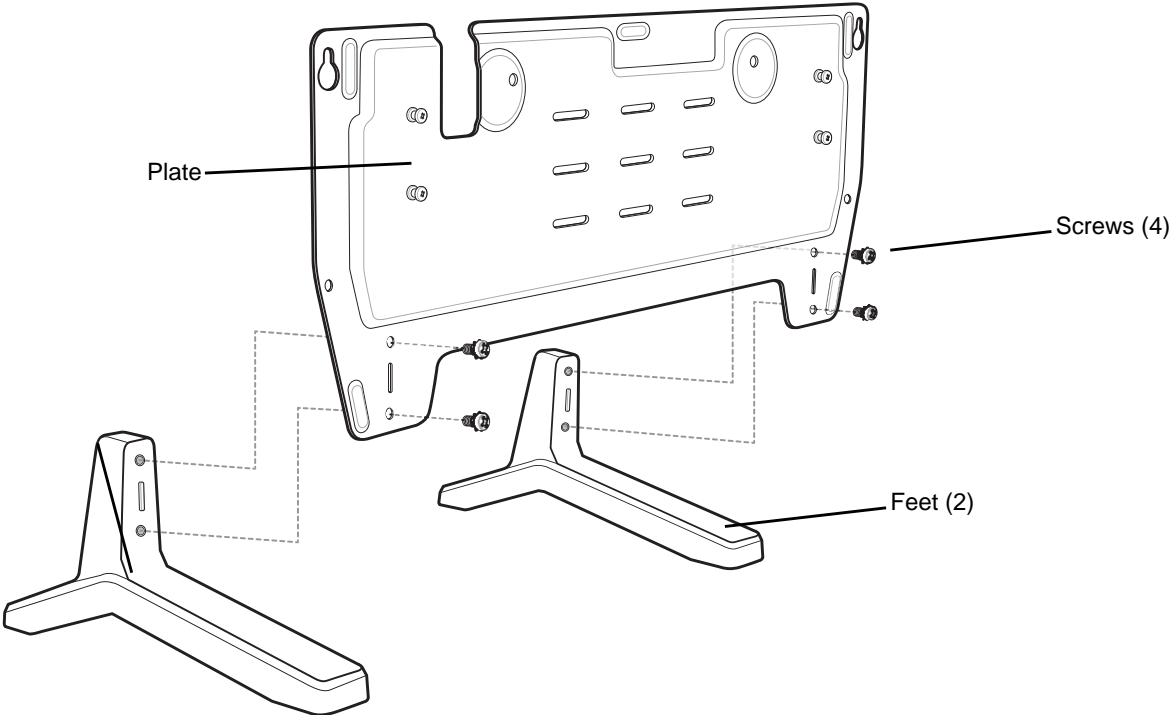


Figure 2-26 Install Feet

- 2. Secure plate to feet with four screws and four washers.

Mount Cradle

To mount the cradle:

- 1. Align mounting slots on bottom of cradle with studs on plate.

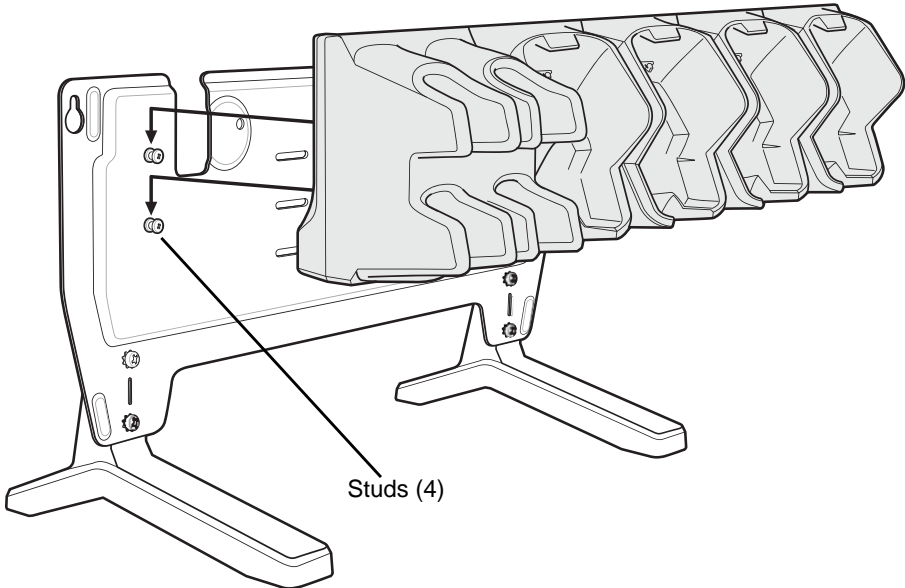


Figure 2-27 Install Cradle onto Desk Mount

2. Secure cradle to plate using two safety screws.

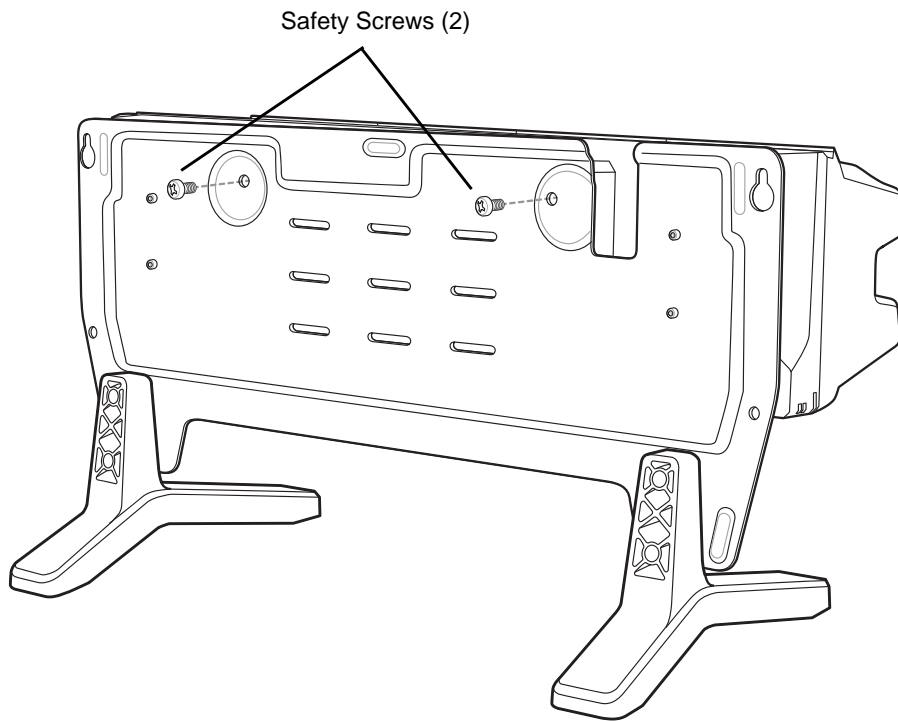


Figure 2-28 *Install Safety Screws*

Cart Mount

Use the Cart Mount to hold the TC8000 and perform hands-free scanning in Presentation Mode.

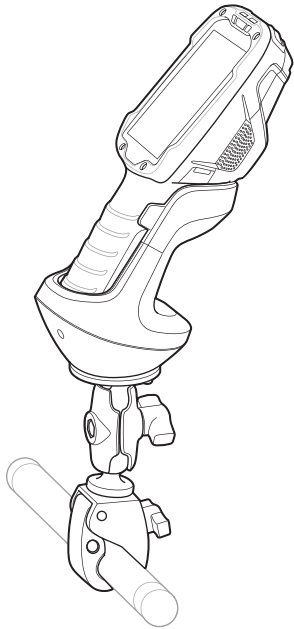


Figure 2-29 *Cart Mount*

Installation

To assemble the Cart Mount and RAM Mount:

1. Secure the RAM Mount ball base to the bottom of the Cart Mount using four screws and four washers (provided).
2. Insert the socket arm to the ball base and claw base.
3. Slightly tighten the knob on the socket arm.

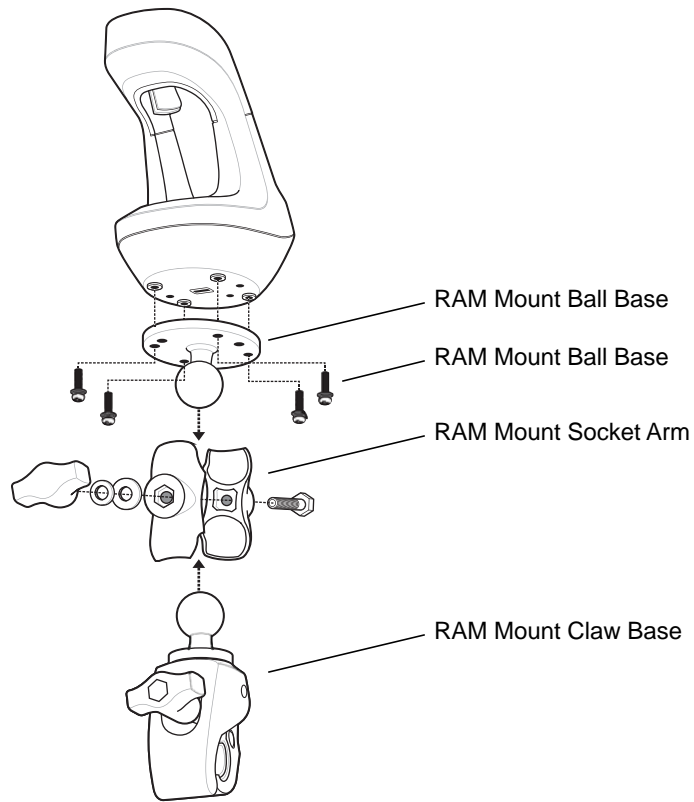


Figure 2-30 *Cart Mount Assembly*

4. Squeeze the claw base and install on a cart rail.

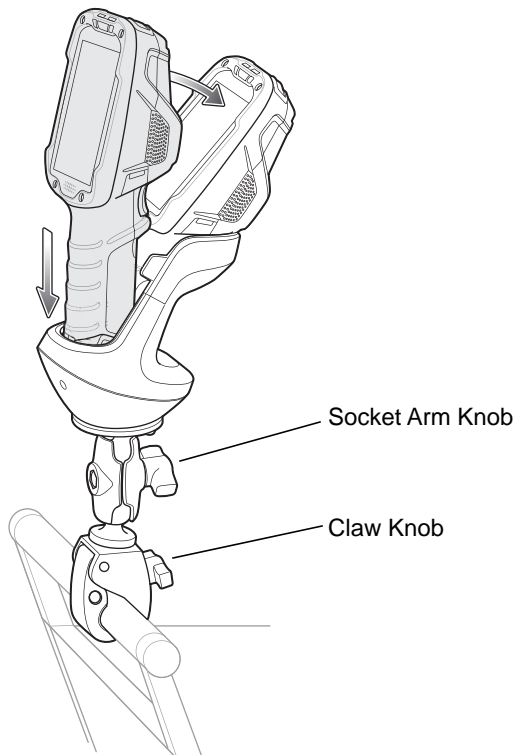


Figure 2-31 *Cart Mount Installation on Cart Rail*

5. Position the Cart Mount and tighten the claw knob and socket arm knob.
6. Insert the TC8000 handle into the Cart Mount cradle and rotate into the cradle.

5-Slot Cradle Rack Installation

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

1. Place the power supply in bottom tray.
2. Connect AC line cord to power supply.
3. Connect DC line cord to power supply.
4. Secure power supply and cables to bottom tray with tie wraps.

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

5. Route cables through cable slots.

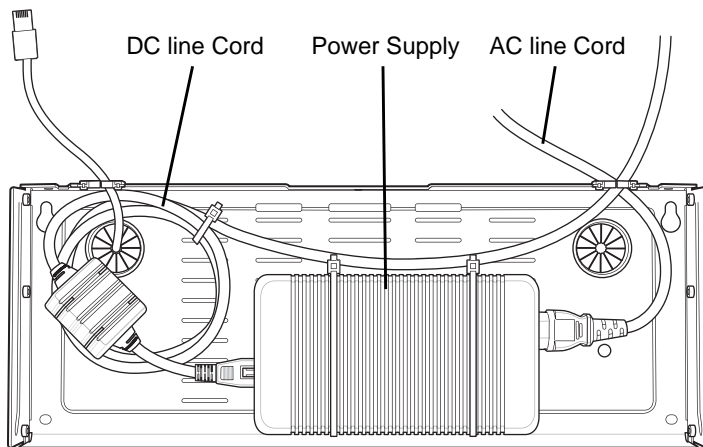


Figure 2-32 Power Supply in Bottom Tray

6. Secure four M2.5 studs to top tray as shown.

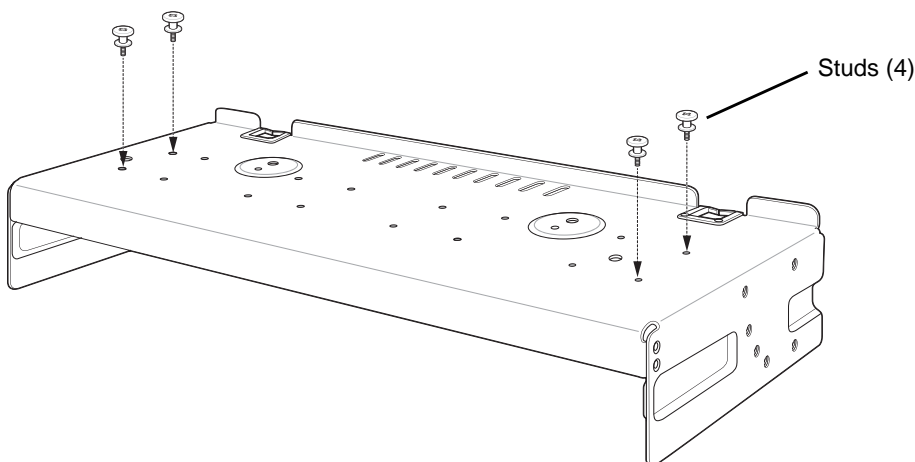


Figure 2-33 Install Studs

7. Align and install 5-Slot cradle onto studs of top tray.

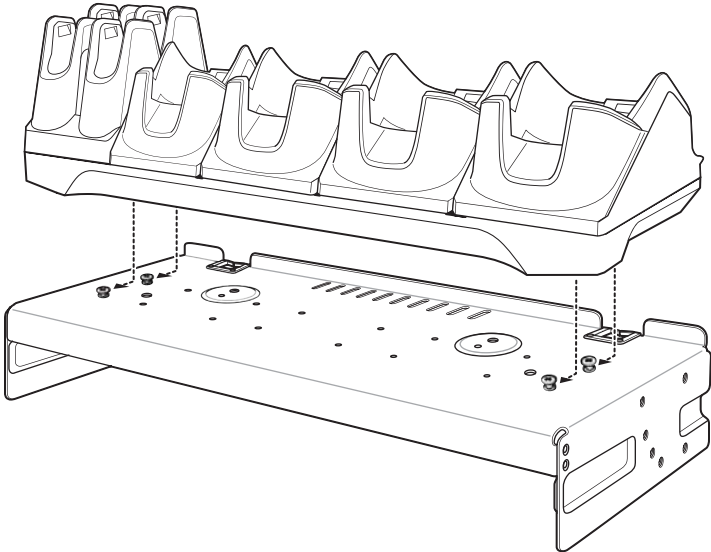


Figure 2-34 *Align Cradle on Studs*

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

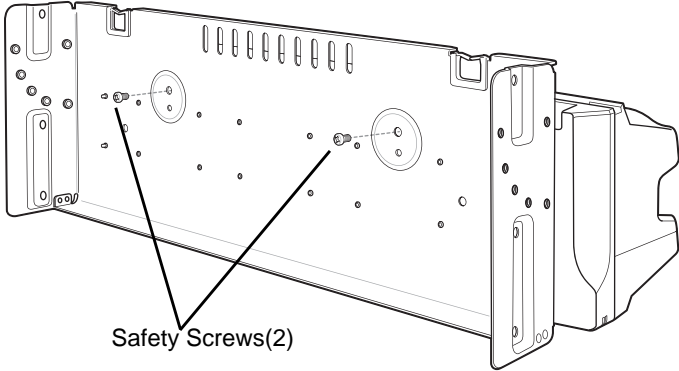


Figure 2-35 *Secure Cradle*

9. Slide top tray onto bottom tray.

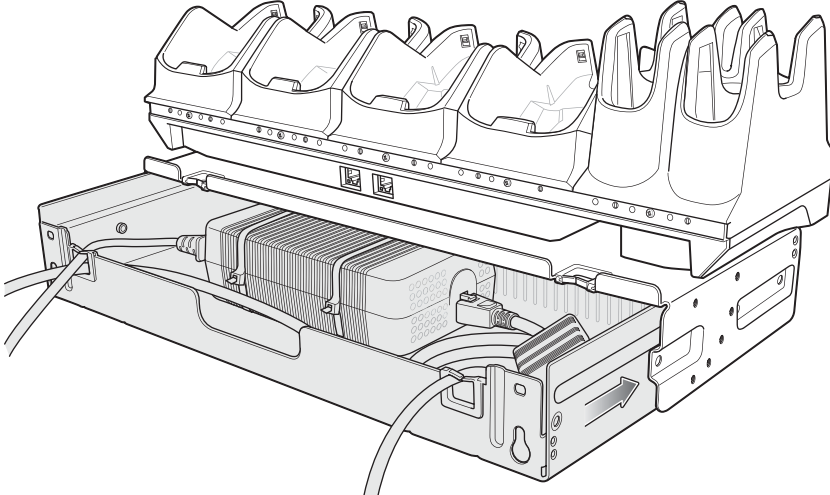


Figure 2-36 *Slide Top Tray onto Bottom Tray*

10. Connect cables to cradle.

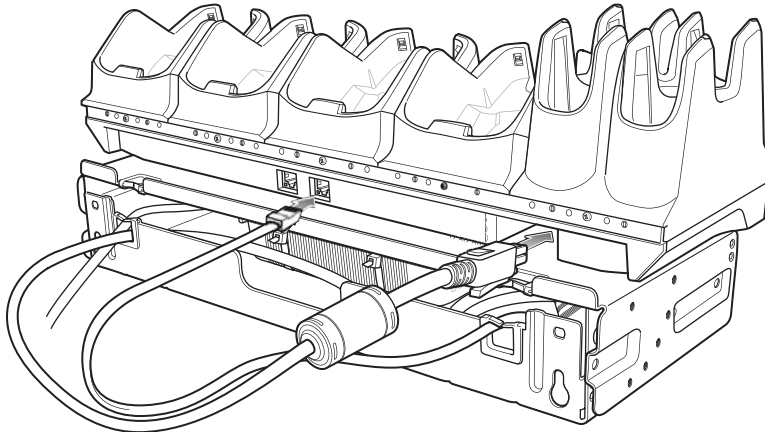


Figure 2-37 *Connect Cables*

11. Secure top tray to bottom tray with 4 M5 screws (two on each side).

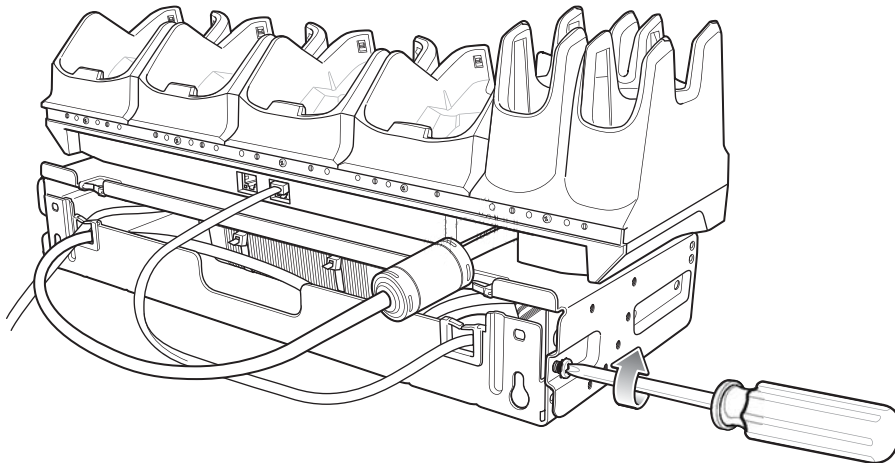


Figure 2-38 *Secure Top and Bottom Tray*

See [Rack Mount Installation on page 2-41](#) for installing the bracket assembly onto a rack.

4-Slot Battery Chargers Rack Installation

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

1. Place one power supply horizontally in bottom tray.
2. Place one power supply vertically in bottom tray.
3. Connect AC line cords to power supplies.
4. Connect DC line cords to power supplies.
5. Secure power supplies and cables to bottom tray with tie wraps.
6. Route cables through cable slots.

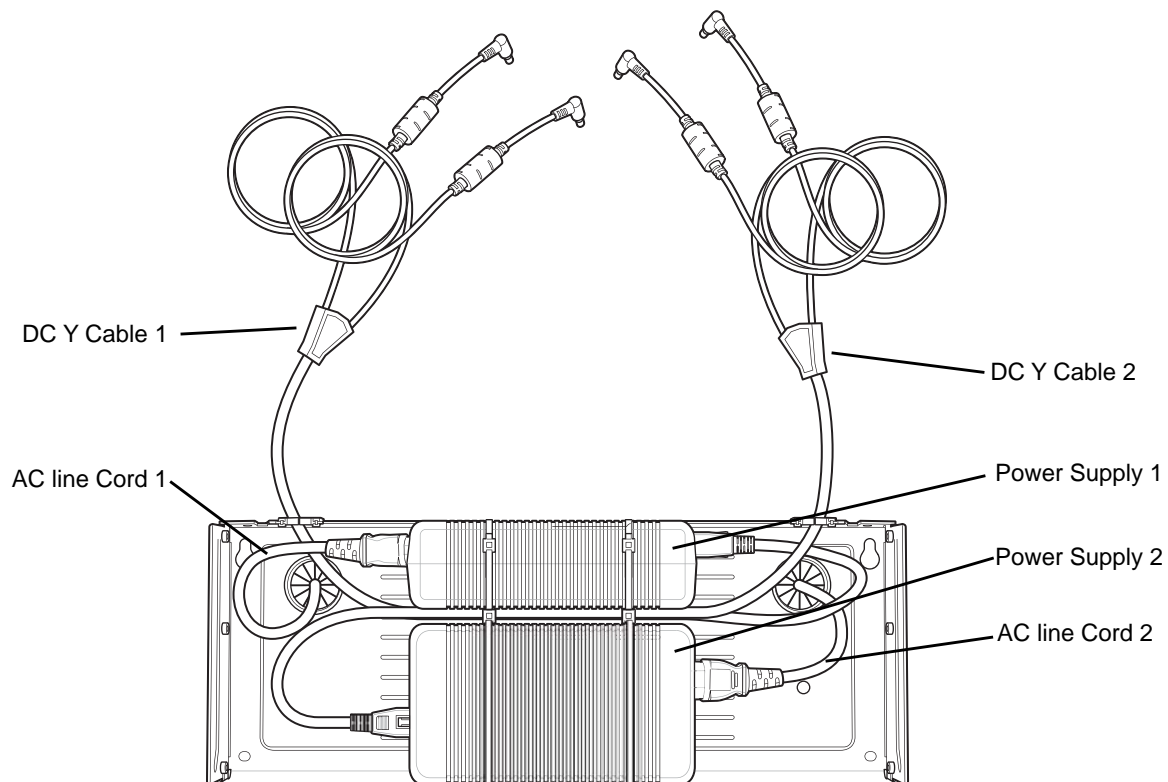


Figure 2-39 Power Supplies in Bottom Tray

7. Slide top tray onto bottom tray until top tray touches vertical power supply.

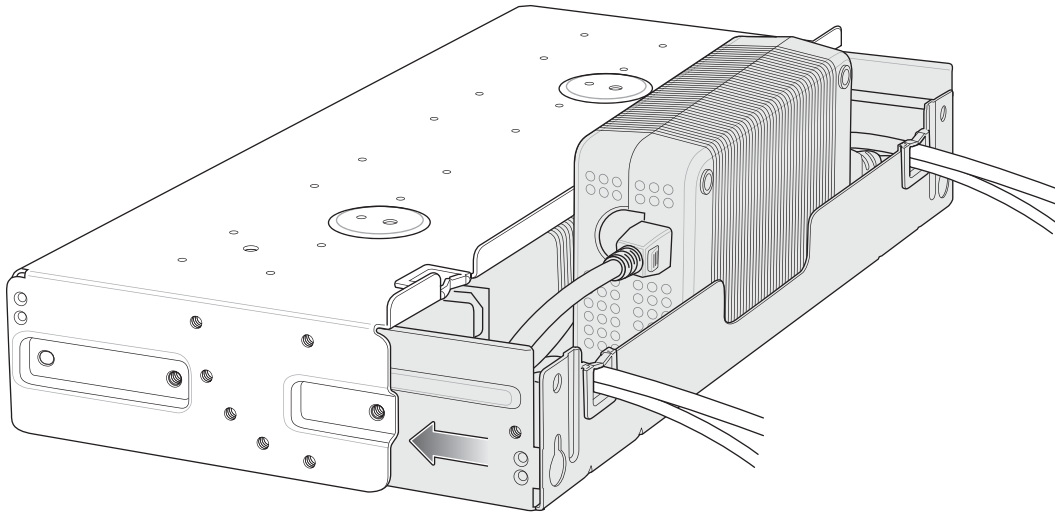


Figure 2-40 Slide top Tray onto Bottom Tray

8. Install 16 M2.5 studs onto top tray as shown below.

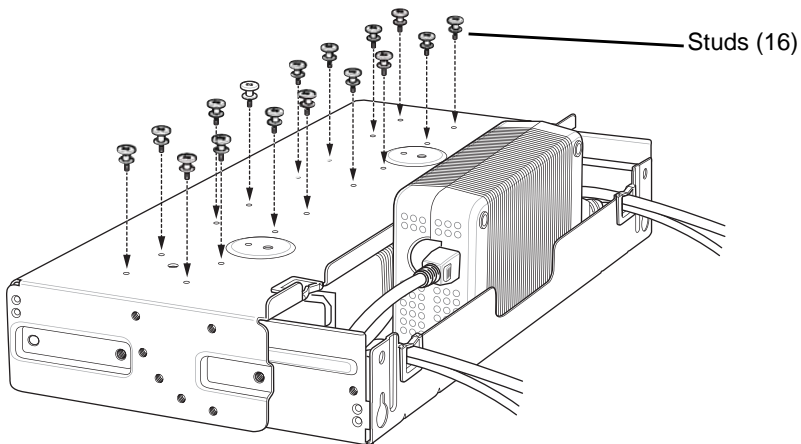


Figure 2-41 Install Studs

9. Align and install 4-Slot Battery Charger onto four studs.

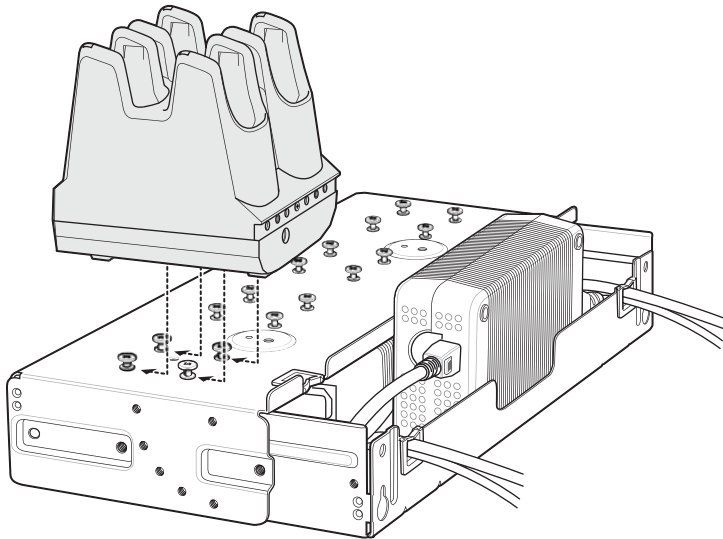


Figure 2-42 *Align Chargers on Studs*

10. Connect DC Y cables to four 4-Slot Battery Chargers.

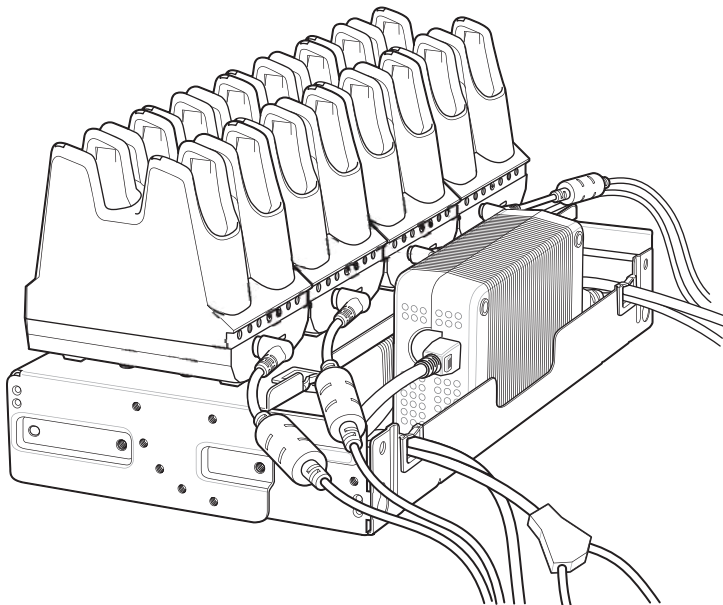


Figure 2-43 *Connect Cables*

11. Secure top tray to bottom tray with four M5 screws (two on each side).

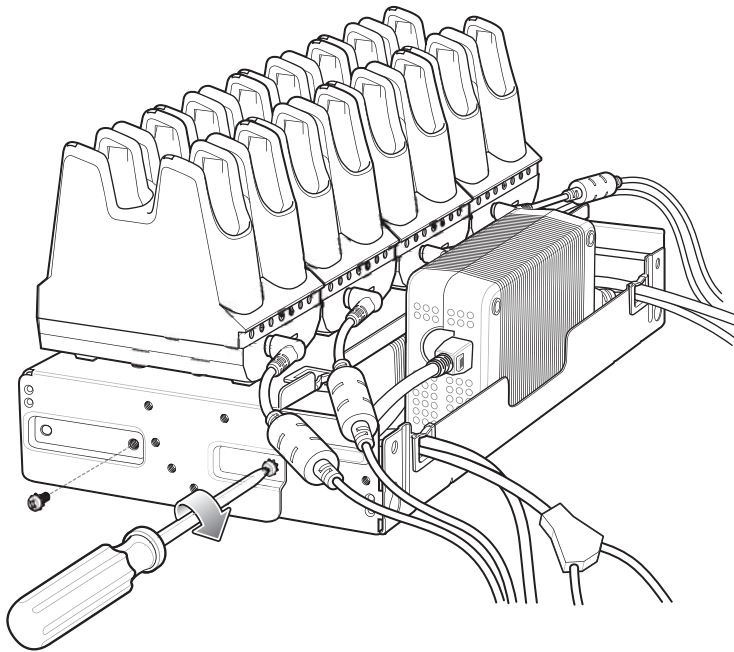


Figure 2-44 *Secure Top Tray to Bottom Tray*

See [Rack Mount Installation on page 2-41](#) for installing the bracket onto a rack.

Rack Mount Installation

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

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

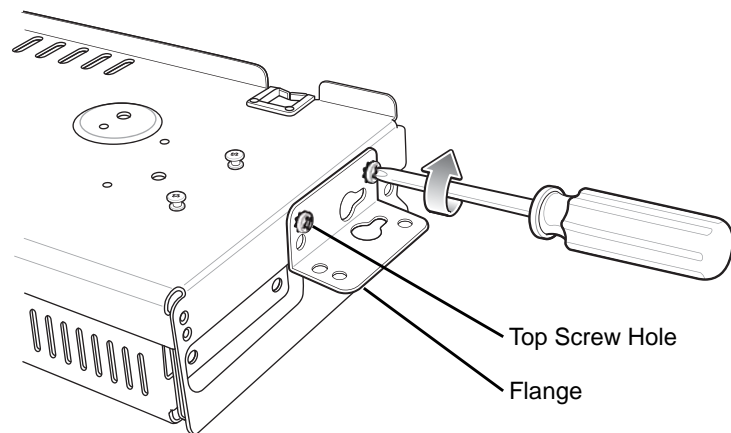


Figure 2-45 Flange Vertical Position (5-Slot Cradles)

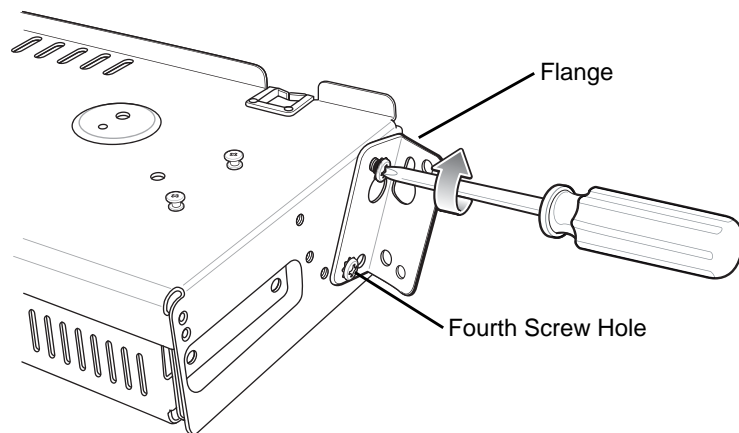


Figure 2-46 Flange 25° Position (4-Slot Battery Chargers)

2. Install two rack system screws for top of mounting brackets. The screw heads should protrude half way from the rail.

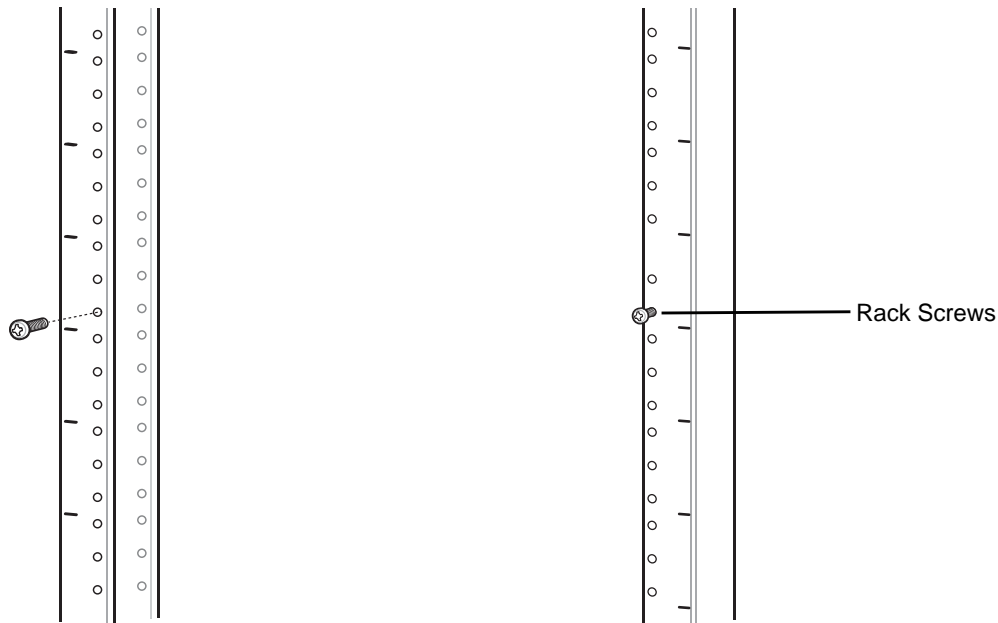


Figure 2-47 *Install Rack System Screws*

3. Align the mounting bracket's top mounting key holes with the screws.
4. Place the brackets on the screws.

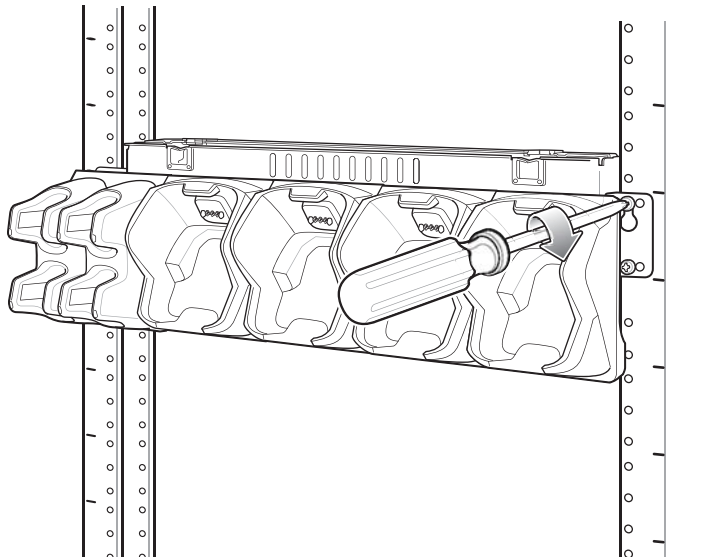


Figure 2-48 *Secure Bracket to Rack (Vertical Position Shown)*

5. Secure the top screws.
6. Install bottom screws and tighten screws.
7. Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

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

5-Slot Cradle Wall Installation

Use the Rack/Wall Mount Bracket to mount a cradle on a wall. When installing on a wall, first assemble the bottom tray, install the bottom tray on the wall and then assemble the top tray.

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

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

Bottom Tray Assembly

See steps 1 through 5 on page 34 for instructions.

Bracket Wall Mounting

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

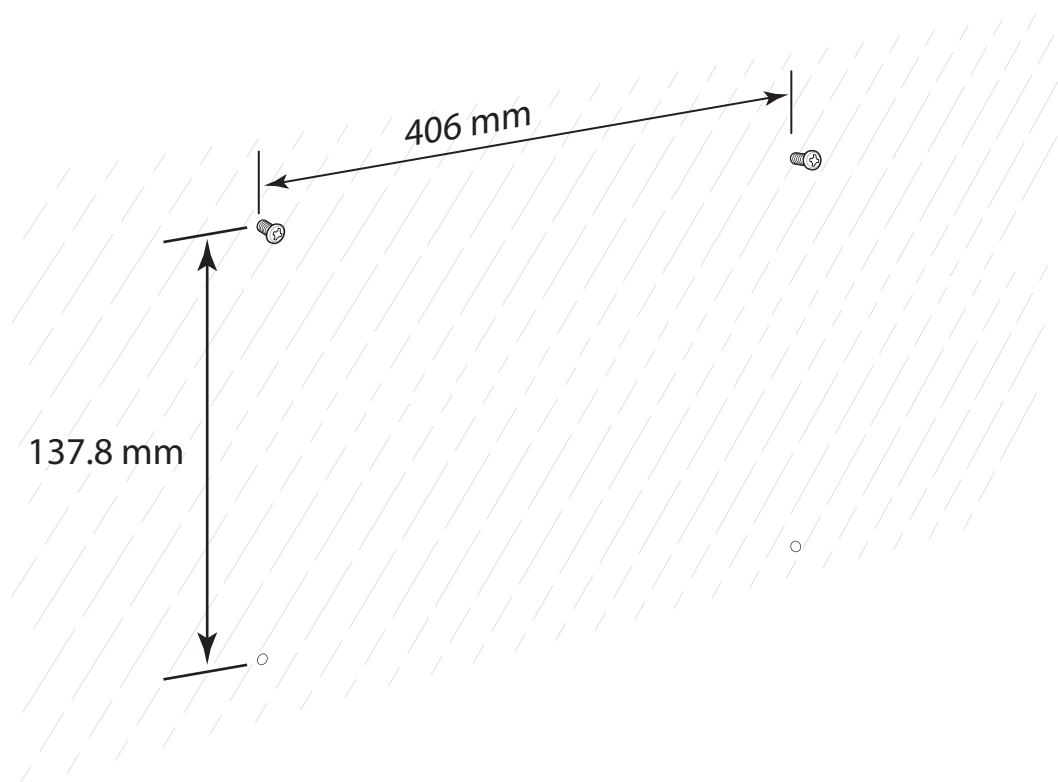


Figure 2-49 Vertical Wall Mounting Dimensions

3. Align the mounting bracket's bottom mounting key holes with the screws.
4. Hang the bracket on the screws.

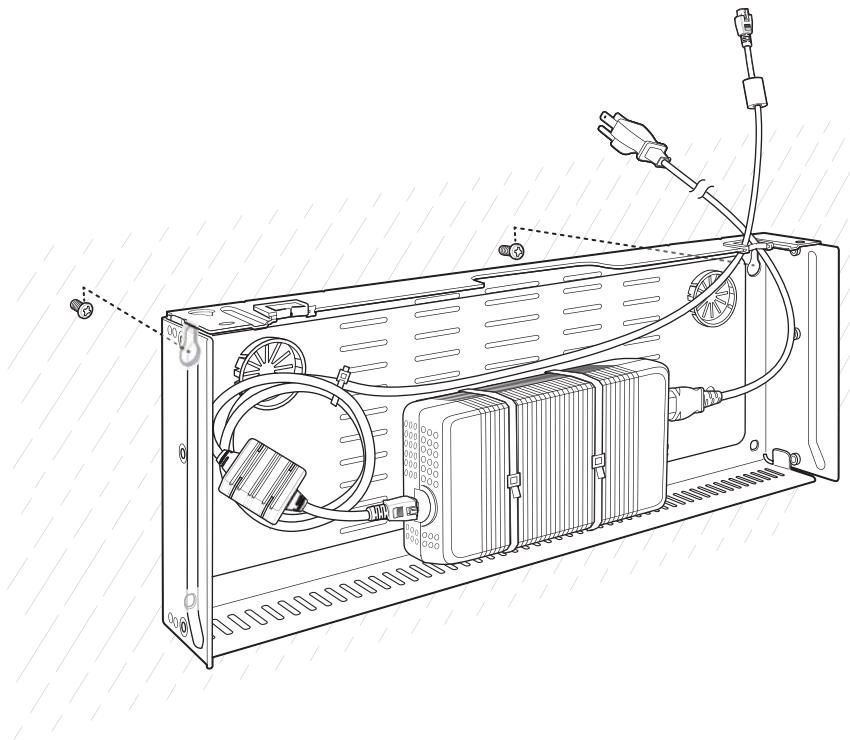


Figure 2-50 *Vertical Installation*

5. Install two top screws.
6. Tighten all screws.

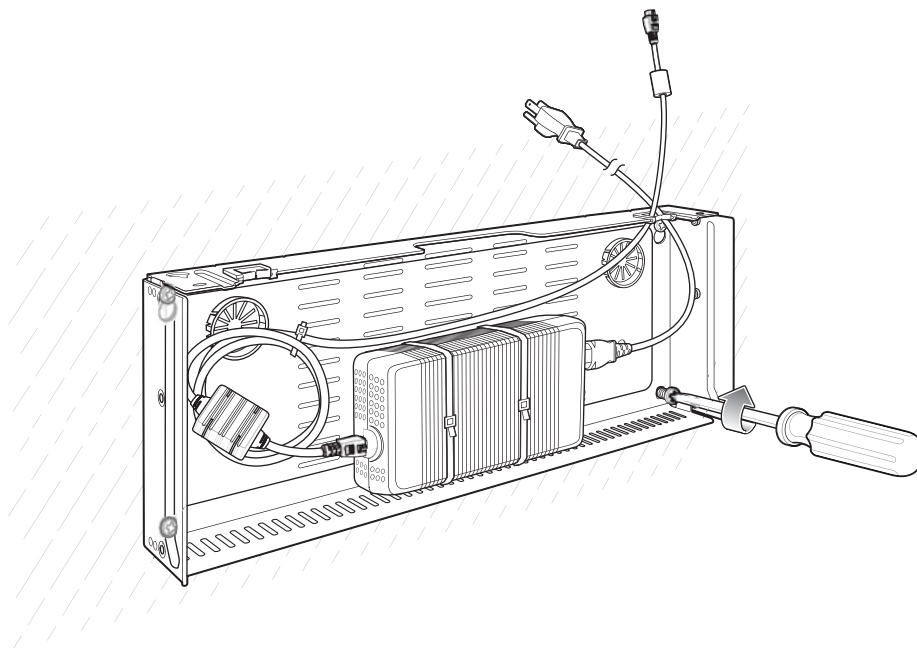


Figure 2-51 *Horizontal Installation - Tighten Screws*

7. Assemble the top tray. See steps 6 through 8 on page 34.
8. Slide the assembled top tray onto bottom tray.

9. Connect cables to cradle.
10. Secure top tray to bottom tray with four M5 screws (two on each side).
11. Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

- Use tie wraps to secure cables to the bracket.
- Coil cables wherever possible.
- Route power cables along wall and secure.

4-Slot Battery Charger Wall Installation

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

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

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

Bottom Tray Assembly

See steps 1 through 5 on page 37 for instructions.

Bracket Wall Mounting

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

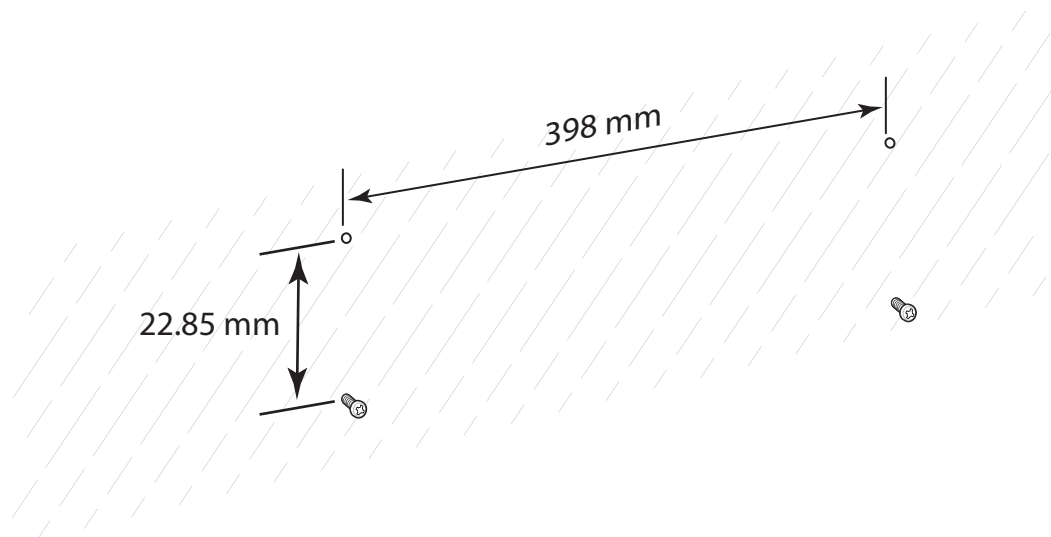


Figure 2-52 *Horizontal Mounting Template*

3. Align the mounting bracket's bottom mounting key holes with the screws.
4. Hang the bracket on the screws.

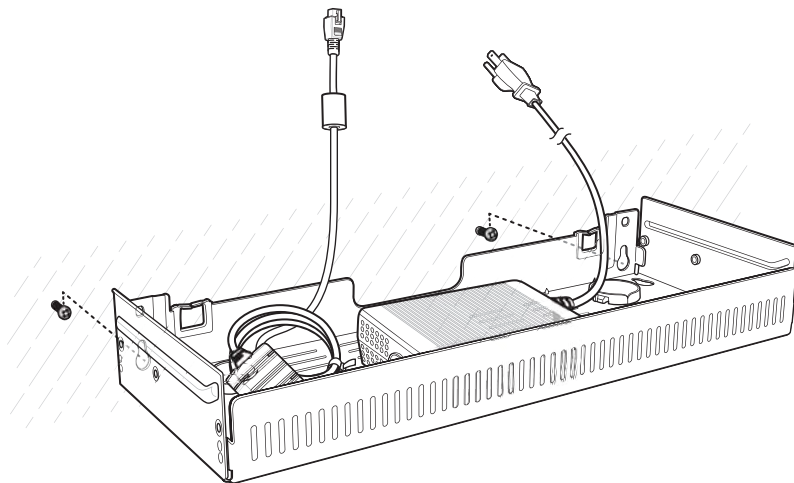


Figure 2-53 *Horizontal Installation*

5. Install two top screws.
6. Tighten all screws.

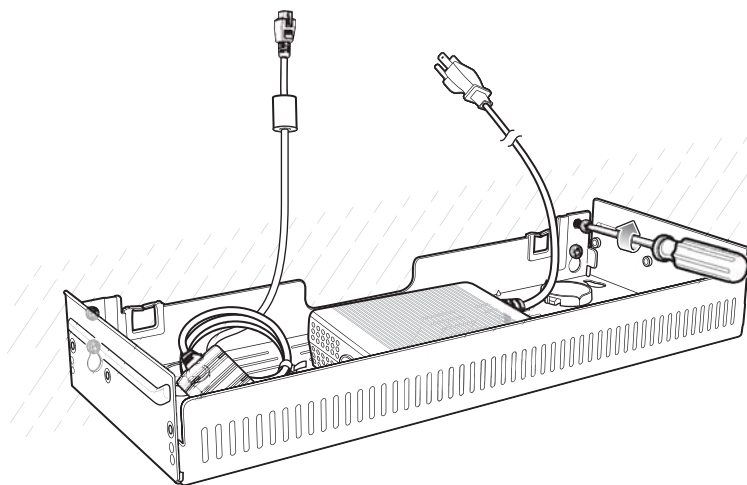


Figure 2-54 *Horizontal Installation - Tighten Screws*

7. Assemble the four 4-Slot Battery Chargers onto the bracket. See steps 7 through 11 on page 37.
8. Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

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

Condensation Resistant Rear Bezel Replacement

The Condensation Resistant configurations contain a desiccant pack that must be replaced every five months. The desiccant pack is part of the Back Bezel. Replacement Back Bezel with desiccant pack comes in a vacuum sealed package. Do not open the package until instructed in the steps below. Install immediately after opening.

To replace the Back Bezel:

1. Remove six screws securing the Back Bezel.

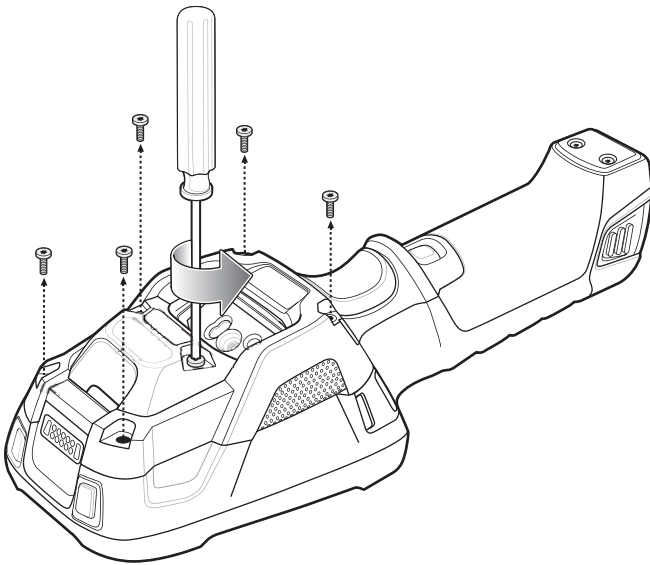


Figure 2-55 *Remove Screws*

2. Lift Rear Bezel.

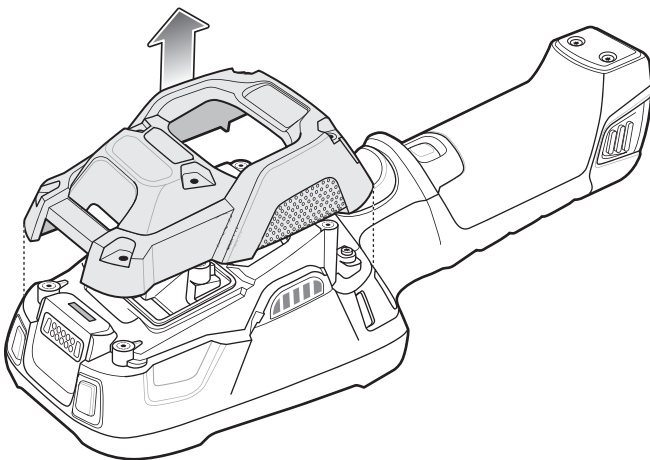


Figure 2-56 *Lift Rear Bezel*

3. Cut the package open with scissors.

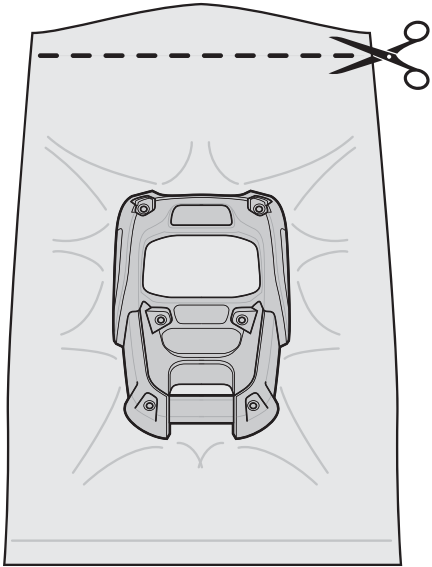


Figure 2-57 *Open Vacuum Bag*

4. Remove Rear Bezel from package.
5. Align Rear Bezel with device.

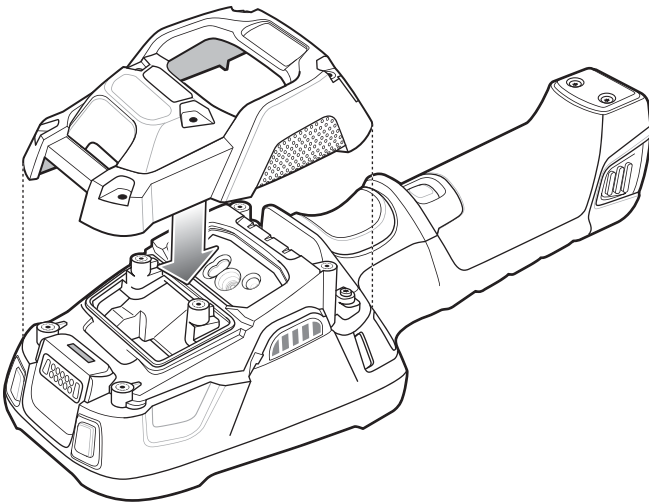


Figure 2-58 *Align Back Bezel*

6. Secure Rear Bezel using six screws.

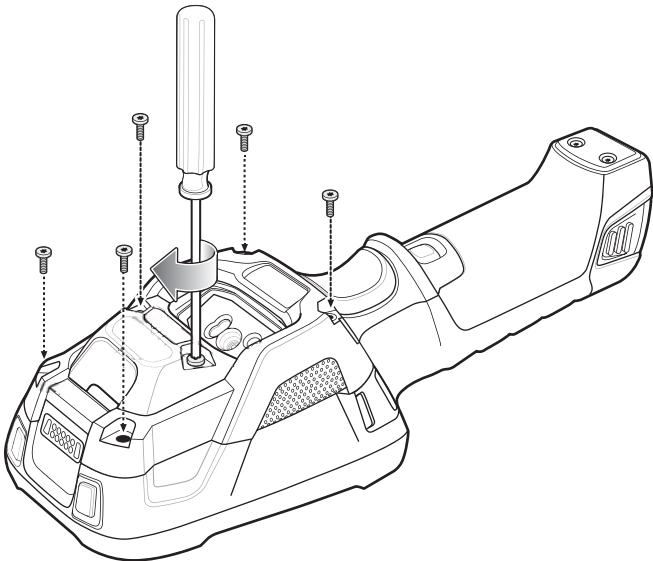


Figure 2-59 *Secure Back Bezel*

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 TC8000 to a host computer using the USB and Charging Cable to transfer files between the TC8000 and the host computer.



CAUTION When connecting the TC8000 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 TC8000 as a Media Device



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

1. Connect the USB Charge cable to the TC8000 and then to the host computer.
Connected as a media device or **Connected as a camera** appears on the Status bar.
2. If **Connected as a camera** appears, pull down the Notification shade and touch **Connected as a camera** and then touch **Media device (MTP)**.
3. On the host computer, open a file explorer application.
4. Locate the **TC8000** as a portable device.
5. Open the **SD card**, **Internal storage** or **Enterprise storage** folder.
6. Copy or delete files as required.

Connecting to the TC8000 as a Camera

✓ **NOTE** Using Camera, you can copy files to internal memory.

1. Connect the USB and Charging cable to the TC8000 and then to the host computer.
Connected as a media device or **Connected as a camera** or appears on the Status bar.
2. If **Connected as a media device** appears, pull down the Notification shade and touch **Connected as a media device** and then touch **Camera (PTP)**.
3. On the host computer, open a file explorer application.
4. Locate the **TC8000** as a portable device.
5. Open 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 device and disconnect USB devices correctly to avoid losing information.

7. On the host computer, unmount the device.
8. Remove the USB and Charging Cable from the device.

CHAPTER 4 DATAWEDGE CONFIGURATION

DataWedge Configuration

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

Basic Scanning

Scanning can be performed using the laser scanner or imager.

To capture bar code data:

1. Ensure that an application is open on the TC8000 and a text field is in focus (text cursor in text field).
2. Aim the exit window at a bar code.
3. Press the trigger button. Ensure the red scan beam covers the entire bar code. The Charging/Scan LED Indicators illuminate green and a beep sounds to indicate a successful decode.

Profiles

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

Profile information consists of:

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

Using profiles, each application can have a specific DataWedge configuration. For example, each user application can have a profile which outputs scanned data in the required format when that application comes to the

foreground. DataWedge can be configured to process the same set of captured data differently based on the requirements of each application.

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

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

Profile0

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

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

Plug-ins

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

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

Input Plug-ins

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

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

Process Plug-ins

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

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

Output Plug-ins

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

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

Profiles Screen

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

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

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

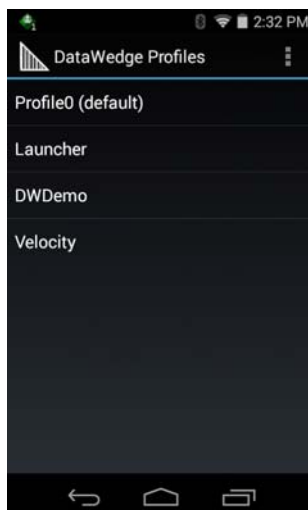


Figure 4-1 DataWedge Profiles Screen

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

To configure a profile touch the profile name.

Profile Context Menu

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

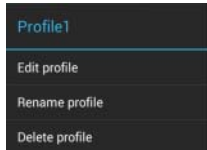



Figure 4-2 *Profile Context Menu*

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

Options Menu

Touch  to open the options menu.

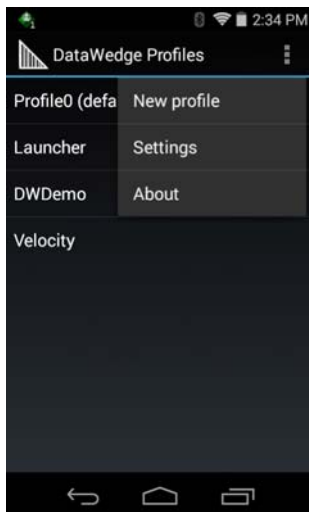





Figure 4-3 *DataWedge Options Menu*




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

Disabling DataWedge

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

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

Creating a New Profile

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

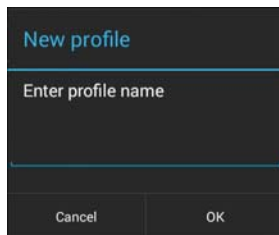


Figure 4-4 *New Profile Name Dialog Box*

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

Profile Configuration

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

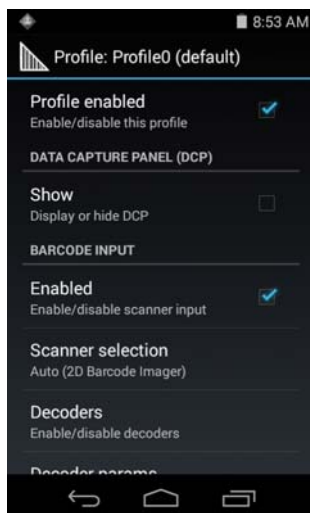


Figure 4-5 *Profile Configuration Screen*

The configuration screen lists the following sections:

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

- Barcode Input
- Keystroke output
- Intent Output
- IP Output.

Associating Applications

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

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

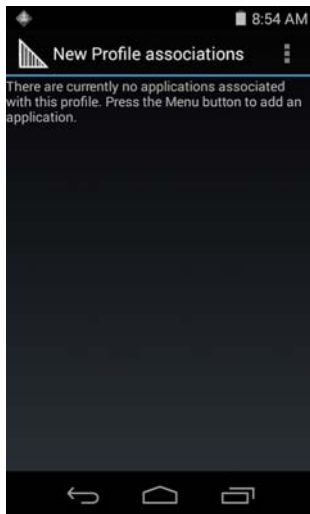


Figure 4-6 Associated Apps Screen

2. Touch **⋮**.
3. Touch **New app/activity**.

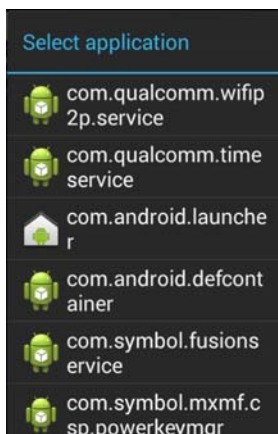


Figure 4-7 Select Application Menu

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

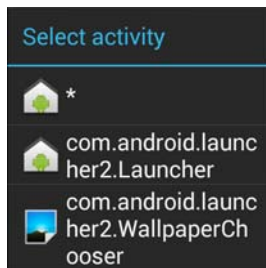


Figure 4-8 *Select Activity Menu*

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

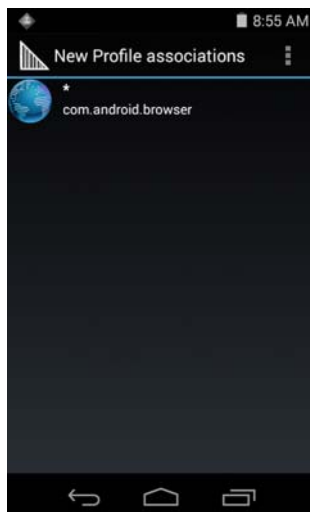


Figure 4-9 *Selected Application/Activity*

Data Capture Panel

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



Figure 4-10 *Minimized Data Capture Panel*

Drag the DCP tab horizontally to maximized overlay. Drag the DCP tab vertically to reposition the tab.

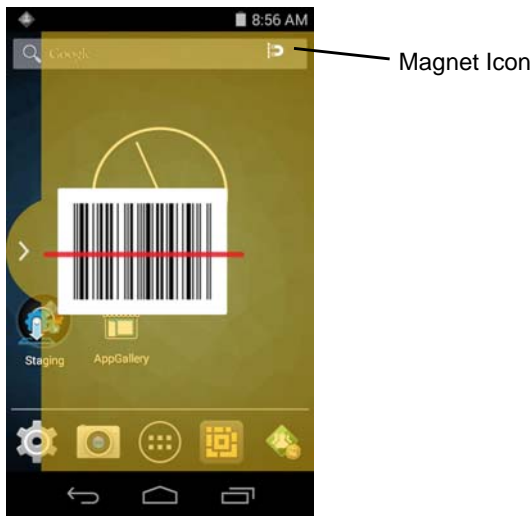


Figure 4-11 *Maximized DCP*

Touch the Magnet icon to change the orientation of the overlay to opposite side of the screen.

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

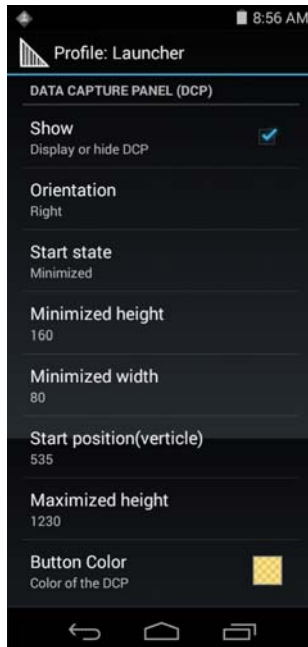


Figure 4-12 Data Capture Panel Settings

- **Orientation** - Indicates whether the DCP displays on the right hand or left hand side of the screen. Options: **Left** (default) or **Right**.
- **Start state** - Indicates whether the DCP should be started in maximized or minimized state. Options: **Minimized** (default) or **Maximized**.
- **Minimized height** - Indicates the height of the DCP when in the minimized state (default - 112).
- **Minimized width** - Indicates the width of the DCP when in the minimized state (default - 56).
- **Start position (vertical)** - Indicates the distance from top of the device screen to the DCP (default - 292).
- **Maximized height** - Indicates the height of DCP when in maximized state (default - 697).
- **Button Color** - Use to change the color and transparency of the DCP overlap. Touch to open the color picker window.



Figure 4-13 Color Picker



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

Bar Code Input

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

Enabled

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

Scanner Selection

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

- **Auto** - The software automatically selects the 2D Imager.
- **Camera Scanner - Scanning is performed using the camera.**
- **1D Barcode Scanner** - - Scanning is performed using the 1D laser scanner.
- **2D Barcode Imager** - Scanning is performed using the 2D Imager.
- **Bluetooth Scanner** - Scanning is performed using the optional RS507 Hands-free Bluetooth scanner.


Decoders

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

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



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

Touch  to return to the previous screen.

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	US Postnet	US Planet
UK Postal	Japanese Postal	Australian Postal
Canadian Postal	Dutch Postal	US4state

US4state FICS	Codabar*	MSI
Code 93	Trioptic 39	Discrete 2 of 5
Chinese 2 of 5	Korean 3 of 5	Code 11
TLC 39	MAIL MARK*	HAN XIN
Matrix 2 of 5	UPC-E1	

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 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-16](#) 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.
 - **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 bar codes.
 - **Ignore Code128 FNC4** - When enabled, and a Code 128 bar code has an embedded FNC4 character, it will be removed from the data and the following characters will not be changed. When the feature is disabled, the FNC4 character will not be transmitted but the following character will have 128 added to it.
- **Code39**
 - **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-16](#) for more information.
 - **Length2** - Use to set decode lengths 4 (default - 55). See [Decode Lengths on page 4-16](#) 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).
 - **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 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 bar codes.
- **Interleaved 2 of 5**
 - **Length1** - Use to set decode lengths (default - 14). See [Decode Lengths on page 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 10). See [Decode Lengths on page 4-16](#) 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).
 - **I2of5 Reduced Quiet Zone** - Enables decoding of margin-less I2of5 bar codes.
- **GS1 DataBar Limited**
 - **GS1 Limited Security Level** -

- **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.
- **Composite AB**
 - **UCC Link Mode**
 - **Link Flag ignored** - 1D component is transmitted regardless of whether a 2D component is detected.
 - **Always Linked** - 1D and the 2D components are transmitted. If 2D is not present, the 1D component is not transmitted.
 - **Auto Discriminate** - the digital scanner determines if there is a 2D portion, then transmits the 1D component, as well as the 2D portion if present. (default).
- **UK Postal**
 - **Report Check Digit** - Transmit UK Postal data with or without the check digit. A check in the checkbox indicates to send UK Postal data with check digit (default - disabled).
- **Codabar**
 - **Length1** - Use to set decode lengths (default - 6). See [Decode Lengths on page 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-16](#) 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 4-16](#) for more information.
 - **Length 2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-16](#) 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 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-16](#) for more information.
 - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Discrete 2 of 5**
 - **Length1** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 14). See [Decode Lengths on page 4-16](#) 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 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 4-16](#) 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).
- **HAN XIN**
 - **HAN XIN Inverse**
 - **Disable** - Disables decoding of HAN XIN inverse bar codes (default).
 - **Enable** - Enables decoding of HAN XIN inverse bar codes.
 - **Auto** - Decodes both HAN XIN regular and inverse bar codes.
- **Matrix 2 of 5**
 - **Length1** - Use to set decode lengths (default - 10). See [Decode Lengths on page 4-16](#) for more information.
 - **Length2** - Use to set decode lengths (default - 0). See [Decode Lengths on page 4-16](#) for more information.
 - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
 - **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
 - **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).

- **UPCE1**

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).
- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.
There are three options for transmitting a UPCE1 preamble:
 - **Preamble Sys Char** - Transmit System Character only.
 - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
 - **Preamble None** - Transmit no preamble (default).
- **Convert UPCE1 To UPCA** - Enable this to convert UPCE1 decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable this to transmit UPCE1 decoded data as UPCE1 data, without conversion (default - disabled).

Decode Lengths

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

UPC EAN Params

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

- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
 - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding "in-spec" UPC/EAN bar codes (default).
 - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
 - **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
 - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.
- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.

- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
 - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
 - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
 - **Supplementals Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the bar code the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
 - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the bar code starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
 - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
 - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
 - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN bar code 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
 - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN bar code not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto, Supplementals Smart, Supplementals 378-379, Supplementals 978-979, Supplementals 977 or Supplementals 414-419-434-439** (2 to 20, default 10).
- **Bookland** - Enable 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 an interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
- **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
- **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
- **Ean Zero Extended** – Enable this parameter to add five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols. Disable this to transmit EAN-8 symbols as is. Default – disabled.
- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC bar codes.

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).
 - **Hardware Picklist** – Enables Picklist mode so that only the bar code under the projected reticle can be decoded.
 - **Software Picklist** - Enables Picklist mode so that only the bar code in the center of the image is decoded.
- **AIM Type**
 - **Trigger** - The device decodes a bar code on each Scan button press. (default).
 - **Continuous Read** - The device continuously decodes bar codes as long as the Scan button is held down and the previous bar code decoding is complete. This mode is useful when the user wants to perform rapid scanning.
- **Same Symbol Timeout** - Use to prevent the device from decoding the same bar code within a specific time interval (applicable only when Aim Type is set to **Continuous Read**). The user can perform rapid scanning and prevents the user from decoding the same bar code twice. Set this value to an appropriate interval (in milliseconds). A value of 0 indicates no interval is required between two successive reads (default - 500).
- **Different Symbol Timeout** - Use to prevent the device from decoding another bar code within a specific interval (applicable only when aim type is set to **Continuous Read**). The user may want to prevent decoding

too quickly and set an interval that the user can aim before scanning the next bar code. A value of 0 indicates no interval is required between two successive reads (default - 500).

- **Illumination mode** - Turns camera illumination on and off. This option is only available when camera is selected in the Barcode input Scanner selection option.
 - **On** - Illumination is on.
 - **Off** - Illumination is off (default).
- **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.
 - **Disable** - Disables the LCD mode (default).
 - **Enable** - Enables LCD mode.
- **Hardware Engine Low Power Timeout** -
- **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.
- **1D Quiet Zone Level** - Sets the effort the decoder performs to decode margin-less bar codes. Applies to any symbology with margin-less bar code decode enabled parameter. Since higher margin-less levels will increase the mis-decode risk and decoding time, we strongly recommend the user only enable the symbologies which needs to choose higher margin-less level, and leave all other symbologies at low default level 1.
- **Poor Quality Decode Effort** - Enable poor quality bar code decoding enhancement feature.

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).

Simulscan Input

Use the **SimulScan Input** to configure the SimulScan Input Plug-in.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.
- **Device Selection** - Configures which scanning device to use for data capture when the profile is active.
 - **Camera** - Scanning is performed with the rear-facing camera.
 - **Imager** - Scanning is performed using the integrated 2D Imager.
 - **Default** - Scanning is performed with the default selected scanning device (default).
- **Template Selection** - Select template to use.
 - **Default - BankCheck.xml** – Use this template to read the MICR E-13B font (length between 19 and 40 characters) on bank checks.
 - **Default - Barcode 1.xml** – Use this template to read a single supported bar code.
 - **Default - Barcode 10.xml** – Use this template to read up to 10 supported bar codes.
 - **Default - Barcode 2.xml** – Use this template to read two supported bar codes.
 - **Default - Barcode 4.xml** – Use this template to read up to supported four bar codes.
 - **Default - Barcode 5.xml** – Use this template to read up to supported five bar codes.
 - **Default - BookNumber.xml** – Use this template to read the OCR-B ISBN 10 or 13 digit book numbers.
 - **Default - DocCap + Optional Barcode** – Use this template to capture a full page image and decode any supported bar codes that are in the form. The captured area is the largest rectangular region in the field of view defined by the solid border or contrast of background. Any OCR or OMR content will not be decoded in this mode. The captured area is further processed to correct, de-skew and sharpen and returned as a picture(default).
 - **Default - DocCap + Required Barcode** – Use this template to capture a full page image and decode of any supported bar codes that are present in the form. The captured area is the largest rectangular region in the field of view defined by the solid border or contrast of background. Any OCR or OMR content will not be decoded in this mode. The captured area is further processed to correct, de-skew and sharpen and returned as a picture.
 - **Default - TravelDoc.xml** – Use this template to read passport and Visa travel documents with OCR-B types A and B fonts.
 - **Default - Unstructured Multi-Line** – Use this template to read up to seven lines of text.
 - **Default - Unstructured Single Line** – Use this template to read a single line of text.
- **Region separator** - Use to configure a separator character for SimulScan region data. When there are multiple text regions the region separator will be inserted between two data strings. By default no separator will be set. Possible values for region separator are None, Tab, Line feed and Carriage return. Region separator can be used with the Keystrokes plug-in Action key character setting to dispatch SimulScan region data to separate text fields.
- **Log directory** - Select a folder for storing log files to help debug a template. The folders are named based on the timestamp of the session and the debug data saved includes logs, templates, frame data, etc.

- **Timestamp** - Enable to capture the time when the data was captured and processed in case of a successful SimulScan session.

Keystroke Output

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

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code data for use in native Android applications. This feature is helpful when populating or executing a form.
 - **None** - Action key character feature is disabled (default).
 - **Tab** - Tab character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
 - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
 - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
 - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
 - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 4-26](#) 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 4-26](#) for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
 - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
 - **Prefix to data** - Add characters to the beginning of the data when sent.
 - **Suffix to data** - Add characters to the end of the data when sent.
 - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
 - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Overview

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

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

```
<intent-filter . . . >
```

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

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

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

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

and the Intent category would be:

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

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

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

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

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

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

IP Output



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

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.

- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
 - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
 - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See [Generating Advanced Data Formatting Rules on page 4-26](#) for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
 - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
 - **Prefix to data** - Add characters to the beginning of the data when sent.
 - **Suffix to data** - Add characters to the end of the data when sent.
 - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
 - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Usage

This section provides information on how to configure IP Output using the DataWedge configuration user interface. To use IP Output in a particular DataWedge profile (for example: **Profile0**), scroll downward on **IP Output**.

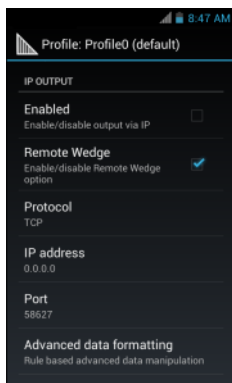


Figure 4-14 IP Output Screen

Using IP Output with IPWedge

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

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

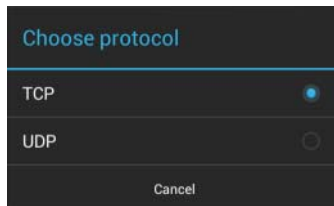


Figure 4-15 *Protocol Selection*

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

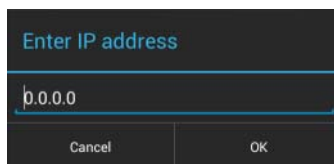


Figure 4-16 *IP Address Entry*

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

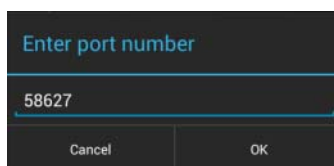


Figure 4-17 *Port Number Entry*

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

Using IP Output without IPWedge

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

1. In **IP Output**, touch **Enabled**.
2. A check appears in the checkbox.
3. Ensure **Remote Wedge** option is disabled.

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

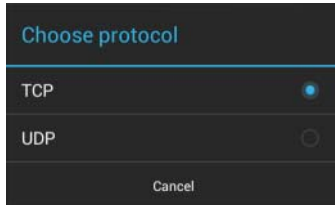


Figure 4-18 *Protocol Selection*

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

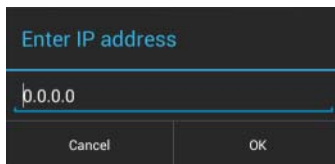


Figure 4-19 *IP Address Entry*

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

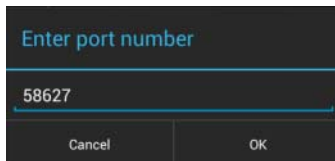


Figure 4-20 *Port Number Entry*

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

Generating Advanced Data Formatting Rules



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

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

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

Configuring ADF Plug-in

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

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

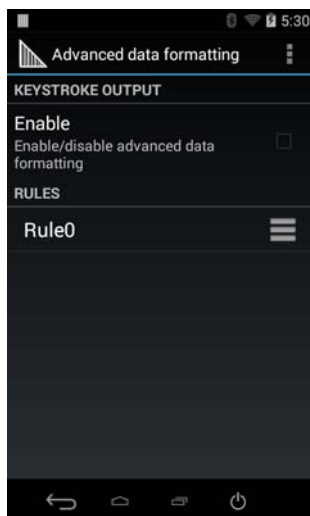



Figure 4-21 *Advanced Data Formatting Screen*

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

Creating a Rule

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

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

Deleting a Rule

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

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



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

Defining Criteria

1. Touch **Criteria**.

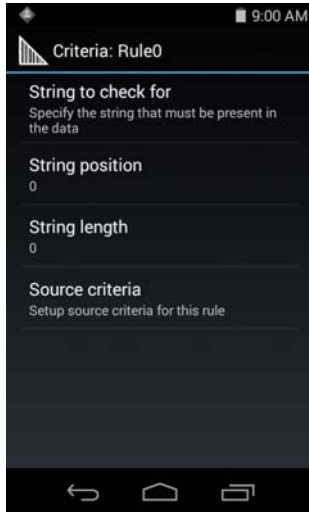


Figure 4-22 *Criteria Screen*

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

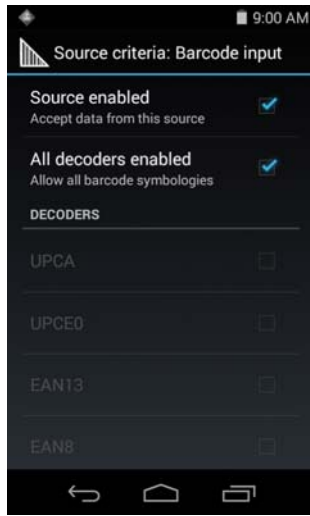







Figure 4-23 Barcode Input Screen

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

Defining an Action

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

1. Touch .
2. Touch **New action**.
3. In the **New action** menu, select an action to add to the **Actions** list. See [Table 4-1 on page 4-30](#) for a list of supported ADF actions.
4. Some Actions require additional information. Touch the Action to display additional information fields.
5. Repeat steps to create more actions.
6. Touch .
7. Touch .

Deleting a Rule

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

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

Order Rules List

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

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

Table 4-1 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.
	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.

Table 4-1 ADF Supported Actions (Continued)

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

Deleting an Action

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:


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







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


Modify the data as follows:

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

To create an ADF rule for the above example:

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

8. Touch **String position**.
9. Change the value to 0.
10. Touch **OK**.
11. Touch **String length**.
12. Change value to 12.
13. Touch **OK**.
14. Touch **Source criteria**.
15. Touch **Barcode input**.
16. Touch **All decoders enabled** to disable all decoders.
17. Touch **Code 39**.
18. Touch  three times.
19. Touch and hold on the **Send remaining rule** until a menu appears.
20. Touch **Delete action**.
21. Touch .
22. Touch **New action**.
23. Select **Pad with zeros**.
24. Touch the **Pad with zeros** rule.
25. Touch **How many**.
26. Change value to 8 and then touch **OK**.
27. Touch  three times.
28. Touch .
29. Touch **New action**.
30. Select **Send up to**.
31. Touch **Send up to** rule.
32. Touch **String**.
33. In the **Enter a string** text box, enter x.
34. Touch **OK**.
35. Touch  three times.
36. Touch .
37. Touch **New action**.
38. Select **Send char**.

39. Touch **Send char** rule.
40. Touch **Character code**.
41. In the **Enter character code** text box, enter 32.
42. Touch **OK**.
43. Touch .

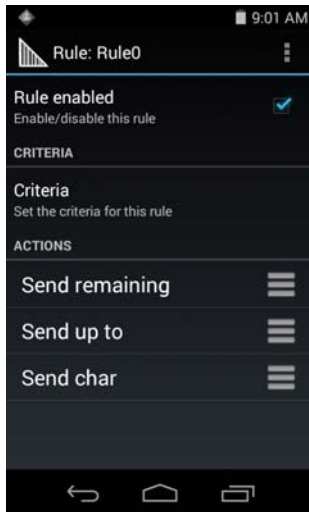


Figure 4-24 ADF Sample Screen

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



Figure 4-25 Sample Bar Code

46. Press and hold the scan key.

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

47. The LED lights green, a beep sounds and the device vibrates, by default, to indicate the bar code was decoded successfully. The LED lights green and a beep sounds, 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.

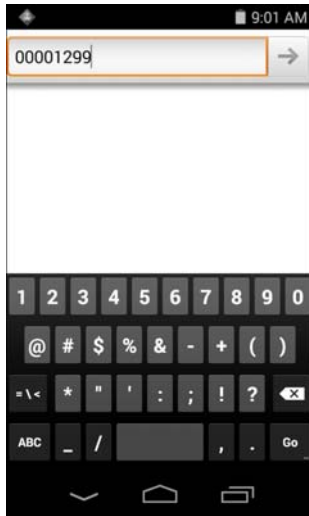


Figure 4-26 *Formatted Data*

DataWedge Settings

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

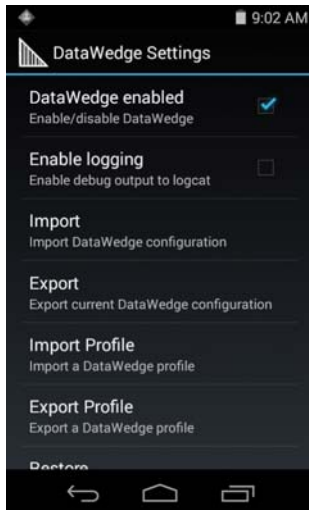








Figure 4-27 *DataWedge Settings Window*

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

Importing a Configuration File




1. Copy the configuration file to the Internal Storage `/Android/data/com.symbol.datawedge/files` folder.
2. Touch  > .
3. Touch .
4. Touch **Settings**.
5. Touch **Import**.
6. Touch **filename to import**.
7. Touch **Import**. The configuration file (*datawedge.db*) is imported and replaces the current configuration.

Exporting a Configuration File




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

Importing a Profile File

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

1. Copy the profile file to the Internal Storage `/Android/data/com.symbol.datawedge/files` folder.
2. Touch  > .
3. Touch .
4. Touch **Settings**.
5. Touch **Import Profile**.
6. Touch the profile file to import.
7. Touch **Import**. The profile file (*dwprofile_x.db*, where x = the name of the profile) is imported and appears in the profile list.

Exporting a Profile


1. Touch  > .
2. Touch .

3. Touch **Settings**.
4. Touch **Export Profile**.
5. Touch the profile to export.
6. Touch **Export**.

The profile file (*dwprofile_x.db*, where x = name of the profile) is saved to the selected location.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

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

Configuration and Profile File Management

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

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

Enterprise Folder

Internal storage contains the Enterprise folder (*/enterprise*). The Enterprise folder is persistent and maintains data after an Enterprise reset. After an Enterprise Reset, DataWedge checks folder */enterprise/device/settings/datawedge/enterprisesetfor* 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 key to be pressed. The active DataWedge profile is required to control all the parameters during a scan operation.

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

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

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

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

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

Sample

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


CHAPTER 5 ADMINISTRATOR UTILITIES

Introduction

Zebra 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 7-3](#) 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 5-11](#) 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.

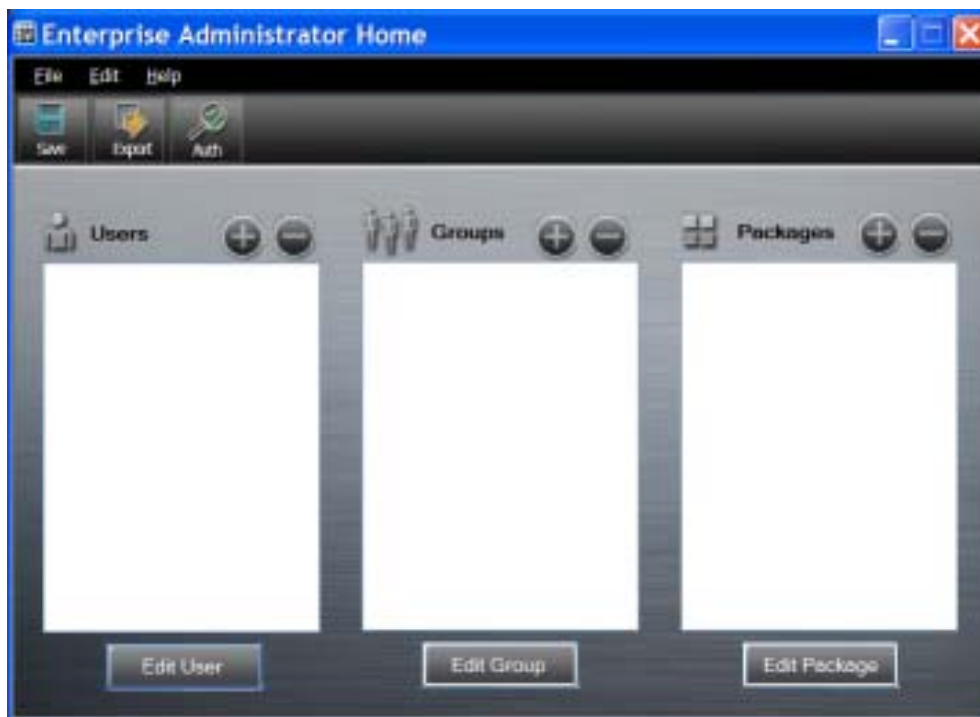


Figure 5-1 Enterprise Administrator Window

Creating Users

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

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



Figure 5-2 *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.

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 5-14](#).

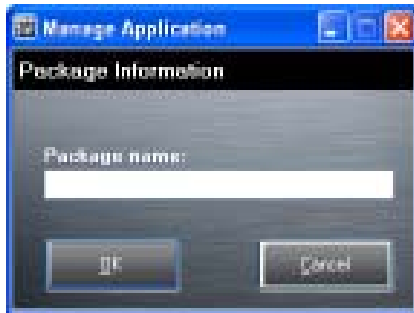


Figure 5-3 Package Information Window

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.

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



Figure 5-4 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.

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



Figure 5-5 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.

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 On-device Storage. See [Chapter 3, USB Communication](#) for information on copying files to the device.

Importing User List

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

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 5-14](#) for instructions for creating a Package List file):

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

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

Deleting a User

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

Editing a Group

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

Deleting a Group

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

Editing a Package

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

Deleting a Package

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.

1. Touch  > .

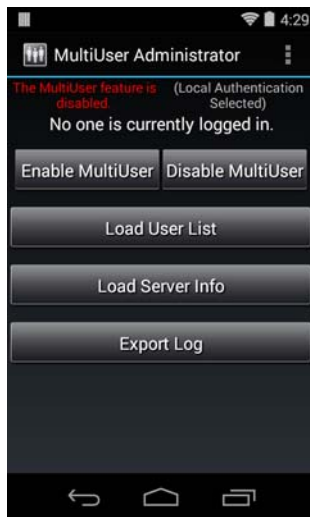


Figure 5-6 *MultiUser Administrator Screen*

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

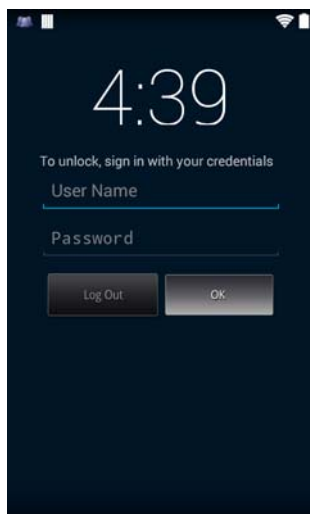




Figure 5-7 *MultiUser Login Screen*

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

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

1. Touch  > .
2. 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.

1. Touch  > .
2. Touch **Load Server Info**. The application reads the data from the *server* file and configures the Multi-user Login feature.
3. Touch .
4. 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.




1. Touch  > .
2. Touch .
3. 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:

1. Touch  > .
2. Touch .
3. 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.

1. Touch  > .
2. Touch .
3. 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.

1. Touch  > .
2. Touch .
3. Touch **Delete Individual User Data**. A dialog box displays with all of the users that currently have data associated with their log in.
4. Select each user to delete or **Select All** to delete all user data.
5. Touch **Delete** to delete the data.

Capturing a Log File

1. 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.

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

1. Touch  > .
2. Touch **Enable Application Lock**.

Disabling Application Lock

1. Touch  > .
2. 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 5-8](#) 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:

```
<packageName>
.
.
.
<packageNname>
```

where:

- `<packageName>` = 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 5-8](#) 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 is named default.

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

At a minimum, the White List for the administrative users group should contain *com.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:

1. Connect the device to the host computer.

✓ **NOTE** See [Development Tools on page 7-2](#) 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 On-device Storage. 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

To install a key:

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

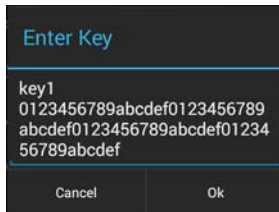


Figure 5-8 *Enter Key Dialog Box*

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

To view a key list:

1. Touch **Key List**.

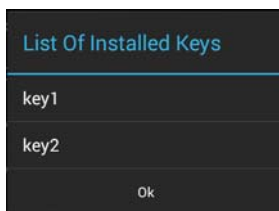


Figure 5-9 *List of Keys*

2. Touch **OK**.

Deleting a Key

To delete a key:

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

1. Create an efs file. See [Creating an EFS File on page 5-19](#) for instruction on creating the efs file.
2. Copy the keyfile and efsfile files to root of Internal Storage. [Chapter 3, USB Communication](#).
3. Touch **Create Volume**.
4. Touch **Import**.
5. Touch **OK**. The message **Successfully Created the Volume** appears briefly.

Creating a Volume Manually

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.

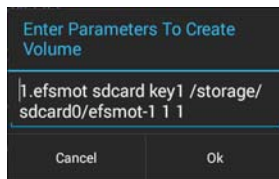


Figure 5-10 Enter Parameter To Create Volume Dialog Box

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

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

Listing Volumes

1. Touch **Volume List**.
2. Touch **sdcard** to list volumes on the On-device Storage 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

1. Touch **Unmount Volume**.
2. Touch **sdcard** to list the mounted volumes on the On-device Storage 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

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

Creating an EFS File

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

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
```

1. Save the text file as `efsfile`.

Off-line Extraction Tool

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

Connect the device to the host computer.

Usage

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

The following Main Menu appears:

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

Creating an Image

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

- The utility first prompts for the name of the volume to create. Any ASCII string that meets standard Linux file naming rules is valid. Enter the image name and then press **Enter**.
- The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
- The utility then prompts for the image size. Enter the size of the volume in MB. A number must be entered without the units. It is understood that MB. A value of 2000, is 2 GB. Note that 4 GB is the largest volume that is supported on the device.
- The utility lastly prompts for the filesystem type. Enter ext4 and then press **Enter**.
The utility then creates the volume in the current working directory.
The utility then finishes the creation process and then prompts to whether the volume should be mounted.
Press [1] if you want to mount or press [2] if you want to exit
- Press **1** will prompt for the mount point. For example, /mnt is prompted. Press **Enter** to mount the encrypted volume at the selected point. After mounting, an option to return to the Main Menu or Exit is provided.
Press **2** to exit the utility without mounting.
- If the volume is mounted on the desktop, then that volume can be provisioned with files for deployment.
- Unmounted volumes can then be copied to the device and subsequently mounted using the Secure Storage Administrator by providing the encryption key used.

Mounting an Image

- From the Main Menu, select item **2**. The following appears:
Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>
Please enter encryption key (64-bytes hex value):
Please enter mount path (e.g. /mnt): <existing mount point>

DONE - OK

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

- From the Main Menu, select item **3**. The following appears:
Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>

DONE - OK




- 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 for more information.
 - **PIN** - Enter a numeric PIN to unlock screen. See Set Screen Unlock Using PIN for more information.
 - **Password** - Enter a password to unlock screen. See Set Screen Unlock Using Password for more information.

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

Single User Mode

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

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

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

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

Set Screen Unlock Using PIN









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



Figure 6-1 PIN Screen

Set Screen Unlock Using Password

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

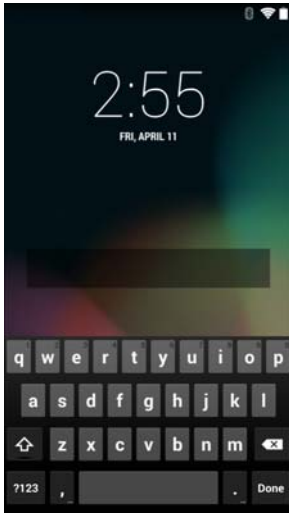




Figure 6-2 Password Screen

Set Screen Unlock Using Pattern

1. Touch  >  >  **Security** > **Screen lock**.
2. Touch **Pattern**.
3. Draw a pattern connecting at least four dots.

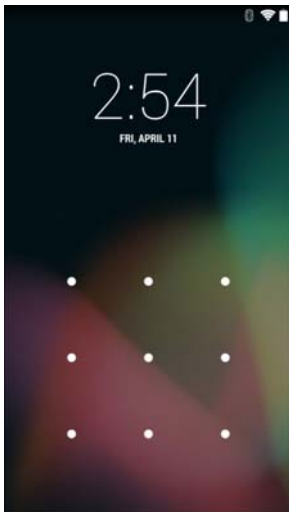





Figure 6-3 Choose Your Pattern Screen

4. Touch **Continue**.
5. Re-draw the pattern.
6. Touch **Confirm**.
7. On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.
8. Touch **Vibrate on touch** to enable vibration when drawing the pattern.

Multiple User Mode

For Multi-user Mode configuration, see Administrator Utilities.

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 TC8000'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.

Remapping a Button

1. Touch  > .
2. Touch  **Key Programmer**.

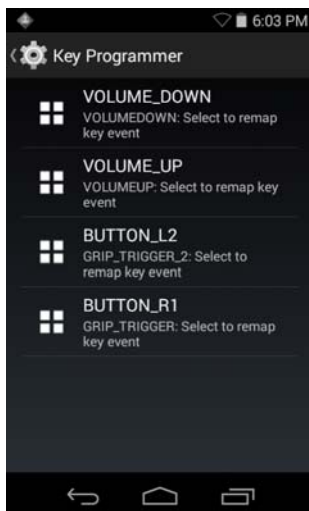


Figure 6-4 *Key Programmer Screen*

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.

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

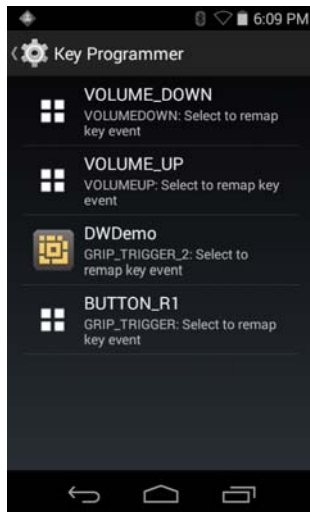


Figure 6-5 Remapped Button

6. Touch .

Accounts

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

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

Language Usage

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

Changing the Language Setting

1. Touch **Language**.
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

1. In the **Language & input** screen, touch **Personal dictionary**.
2. Touch **+** to add a new word or phrase to the dictionary.
3. In the **Phrase** text box, enter the word or phrase.
4. In the **Shortcut** text box, enter a shortcut for the word or phrase.

5. In the **Language** drop-down list, select the language that this word or phrase is stored.
6. Touch **Add to dictionary** in the top left corner of the screen to add the new word.

Keyboard Settings




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

- Android Keyboard
- Japanese IME
- Chinese keyboard

PTT Express Configuration

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

About Device

Use About phone settings to view information about the TC8000. Touch  >  >  **About device**.

- **Status** - Touch to display the following:
 - **Battery status** - Indicates if the battery is charging (on AC power) or discharging (on battery power).
 - **Battery level** - Indicates the battery charge level.
 - **IP address** - Displays the IP address of the device.
 - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
 - **Ethernet MAC address** - Displays the Ethernet 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 TC8000 has been running since being turned on.
- **Hardware configuration** - Lists part number for various hardware on the TC8000.
- **SW components** - Lists filenames and versions for various software on the TC8000.
- **Legal information** - Opens a screen to view legal information about the software included on the TC8000.
- **Battery Management** - Displays information about the battery.
- **Model number** - Displays the devices model number.
- **Processor info** - Displays the type of processor used in the TC8000.
- **Android version** - Displays the operating system version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

CHAPTER 7 APPLICATION DEPLOYMENT

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

1. Copy the certificate from the host computer to the root of the On-device Storage. See [Chapter 3, USB Communication](#) for information about connecting the device to a host computer and copying files.
2. Touch  >  >  **Security**.
3. Touch **Install from On-device Storage**.
4. Navigate to the location of the certificate file.
5. Touch the filename of the certificate to install. Only the names of certificates not already installed display.
6. If prompted, enter the certificate's password and touch **OK**.

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

The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the On-device Storage.

Development Tools

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




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



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

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

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

Open the Developer options screen to set development related settings.

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

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

ADB USB Setup

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 7-3*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 7-4*.
- microSD Card, see *Installing Applications Using a microSD Card on page 7-4*.
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

Installing Applications Using the USB Connection



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

1. Connect the device to a host computer using USB. See *Chapter 3, USB Communication*.
2. On the host computer, copy the application `.apk` file from the host computer to the device.
3. Disconnect the device from the host computer. See *Chapter 3, USB Communication*.
4. On the device, touch



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

5. Touch to view files on the 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**.

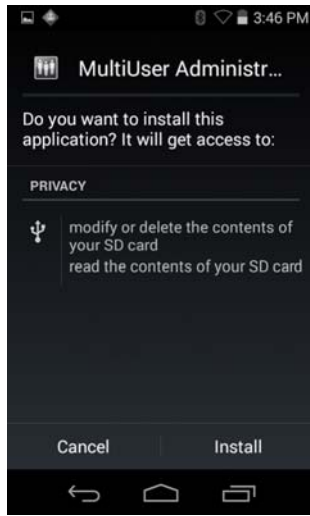


Figure 7-1 Accept Installation Screen

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.

Ensure that the ADB drivers are installed on the host computer. See [ADB USB Setup on page 7-2](#).

1. Connect the device to a host computer using USB. See [Chapter 3, USB Communication](#).
2. Touch  >  > { } **Developer options**.
3. Slide the switch to the **ON** position.
4. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
5. Touch **OK**.
6. On the host computer, open a command prompt window and use the adb command:



```
adb install <application>
```

 where: <application> = the path and filename of the apk file.
7. Disconnect the device from the host computer. See [Chapter 3, USB Communication](#).

Installing Applications Using a microSD Card




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

1. Connect the device to a host computer using USB. See [Chapter 3, USB Communication](#).
2. Copy the application .apk file from the host computer to the microSD card.
3. Remove the microSD card from the host computer.
4. Press and hold the Power button until the menu appears.
5. Touch **Power off**.
6. Touch **OK**.
7. Install the microSD card. See [Installing the microSD Card on page 1-4](#).
8. Press and hold the Power button to turn on the TC8000.
9. On the device, touch .






NOTE In **File Browser**, the microSD card path is /external or /storage/sdcard1.

10. Touch  to view files on the microSD card.
11. Locate the application .apk file.
12. Touch the application file to begin the installation process.
13. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
14. Touch **Open** to open the application or Close to exit the installation process. The application appears in the App list.

Uninstalling an Application

To uninstall an application:

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

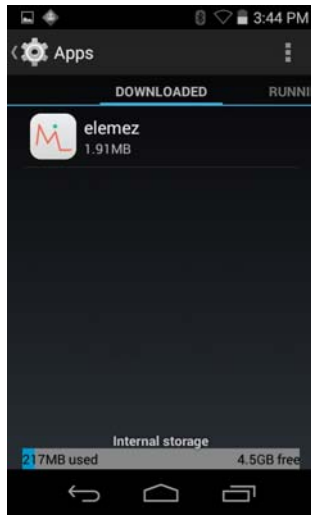


Figure 7-2 Downloaded Screen

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

System Update

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

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 TC8K0K300PUWWxyzz.zip file to the root directory of microSD card or internal storage. See [Chapter 3, USB Communication](#) for more information.
3. Press and hold the Power button until the menu appears.
4. Touch **Power off**.
5. Touch **OK**. The device turns off.
6. Press and hold the Power button and the trigger.
7. When the Zebra splash screen appears, release the button and trigger.
The System Recovery screen appears.



Figure 7-3 System Recovery Screen

8. Press the Up and Down volume buttons to navigate to the **apply update from SD card** or **apply update from internal storage** option.
9. Press the trigger.
10. Press the Up and Down volume buttons to navigate to `TC8K0K300PUWWxyz.zip` file.
11. Press the trigger. The System Update installs and then the TC8000 resets.

Storage


The device contains four types of file storage:

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

Random Access Memory

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

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

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

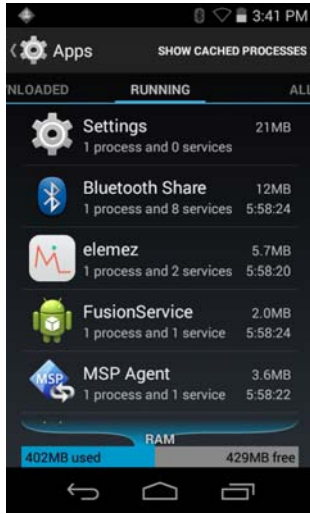




Figure 7-4 Running Screen

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

Internal Storage

The TC8000 has internal storage. The internal storage content can be viewed and files copied to and from when the TC8000 is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

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

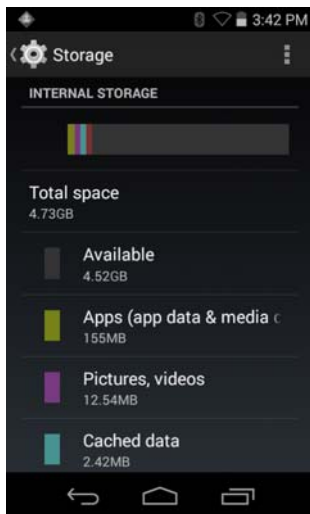


Figure 7-5 Internal Storage Screen

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

External Storage

The TC8000 can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the TC8000 is connected to a host computer.




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



Figure 7-6 *Storage Settings*



- **Total space** - Displays the total amount of space 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 TC8000 so that it can be safely removed. This setting is dimmed if there is no microSD card installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase external SD card** - Permanently erases everything on the installed microSD card.

Enterprise Folder

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

Application Management

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

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

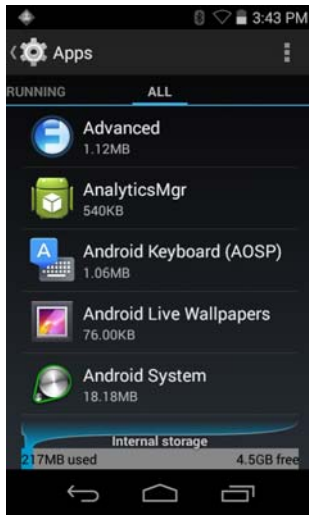


Figure 7-7 Apps Screen

The **Apps** screen has three 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.
- Touch the **Running** tab to view the applications and their processes and services that are running or cached
- Slide the screen to the **All** tab to view all the applications installed on the device, including factory installed applications and downloaded applications.

When on the **Downloaded** or **All** tab, press **⋮** > **Sort by size** to switch the order of the list.



Viewing Application Details

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

- Touch **Force stop** to stop an application.
- Touch **Uninstall** to remove the application and all of its data and settings from the device. See [Uninstalling an Application on page 7-5](#) for information about uninstalling applications.
- Touch **Clear data** to delete an application's settings and associated data.
- **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.

Stopping an Application

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

1. Touch  >  > **Apps**.
2. Swipe the screen to display the **Running** tab.

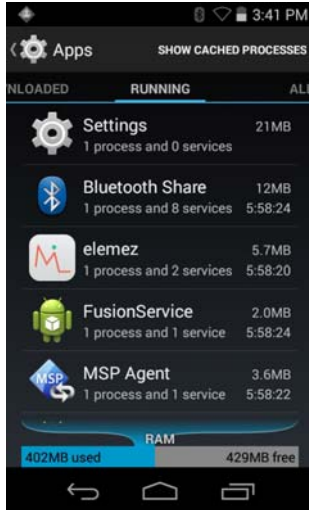


Figure 7-8 *Running Applications*




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.
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.

✓ **NOTE** Stopping an application or operating system processes and services disables one or more dependent functions on the device. The device may need to be reset to restore full functionality.

5. Touch **Stop**.

Managing Downloads

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

1. Touch  > .
2. Touch an item to open it.
3. Touch headings for earlier downloads to view them.
4. Check items to delete; then touch . The item is deleted from storage.
5. Touch **Sort by size** or **Sort by time** to switch back and forth.

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

CHAPTER 8 MAINTENANCE AND TROUBLESHOOTING

Introduction

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

Maintaining the TC8000

For trouble-free service, observe the following tips when using the TC8000:

- Protect the TC8000 from temperature extremes.
- Do not store or use the TC8000 in any location that is extremely dusty, damp, or wet.
- Use a soft lens cloth to clean the scan exit window of the TC8000. If the surface of the TC8000 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution. Do not use bleach or ammonia.
- Take care not to scratch the screen of the TC8000.
- The display of the TC8000 contains glass. Take care not to drop the TC8000 or subject it to strong impact.

Battery Safety Guidelines

- The area in which the device 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.
- Do not use incompatible batteries and chargers. If you have any questions about the compatibility of a battery or a charger, contact Zebra Support. See [Service Information on page xvi](#) for contact information.
- Do not crush, puncture, or place a high degree of pressure on the battery.
- Follow battery usage, storage, and charging guidelines found in the device Quick Reference Guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between +32°F and +104°F (0°C and +40°C)

- Do not 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 promptly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- Seek medical advice immediately if a battery has been swallowed.
- 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, call Customer Support to arrange for inspection. See [Service Information on page xvi](#) for contact information.

Cleaning



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 Symbol Technologies 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.

Materials Required

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

Cleaning the Device

Housing

Using the alcohol wipes, wipe the housing including the Scan key.

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 dried the display with a soft, non-abrasive cloth to prevent streaking.

Scan Exit Window

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

Power Connector

1. Remove the main battery from device.
2. Install the battery cover.
3. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.
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 3 through 6.
7. Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.



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

8. Inspect the area for any grease or dirt, repeat if required.

Cleaning Cradle Connectors

Use this procedure to clean the connectors on a cradle:

1. Remove power 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 let any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton tipped applicator.
5. Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.



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

6. Ensure that there is no lint left by the cotton tipped applicator, remove lint if found.

7. If grease and other dirt can be found on other areas of the cradle, use 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 device units are used. They may be cleaned as frequently as required. However when used in dirty environments it may be advisable to periodically clean the scanner exit window to ensure optimum scanning performance.

Troubleshooting

Device

Table 8-1 *Troubleshooting the TC8000*

Problem	Cause	Solution
TC8000 does not turn on.	Battery not charged.	Charge or replace the battery in the TC8000.
	Battery not installed properly.	Ensure battery is installed properly. See Installing the Battery on page 1-7 .
	System crash.	Perform a soft reset. If the TC8000 still does not turn on, perform a hard reset. See Resetting the TC8000 on page 1-10 .
Battery did not charge.	Battery failed.	Replace battery. If the TC8000 still does not operate, try a soft reset, then a hard reset. See Resetting the TC8000 on page 1-10 .
	TC8000 removed from cradle before charging completed.	Insert the TC8000 into the cradle and begin charging. The battery fully charges in approximately four hours.
	Ambient temperature of the cradle is too warm or too cold.	The ambient temperature must be between 0 °C and 40 °C (32 °F and 104 °F).
During data communication, no data was transmitted, or transmitted data was incomplete.	TC8000 unplugged from host computer during communication.	Reconnect the programming cable to the host computer and re-transmit.
	Communication software was incorrectly installed or configured.	See system administrator.
TC8000 turns itself off.	TC8000 is inactive.	The TC8000 turns off after a period of inactivity. If the TC8000 is running on battery power, this period can be set to 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or 30 minutes. Change the setting if you need a longer delay before the automatic shutoff feature activates.
	Battery is depleted.	Place the TC8000 in the cradle to re-charge the battery.
	Battery is not inserted properly.	Insert the battery properly (see Installing the Battery on page 1-7).
	The TC8000's battery is low and it powers down to protect memory content.	Place the TC8000 in the cradle to re-charge the battery.

Table 8-1 Troubleshooting the TC8000 (Continued)

Problem	Cause	Solution
A message appears stating that the TC8000 memory is full.	Too many files stored on the TC8000.	Delete unused memos and records. You can save these records on the host computer.
	Too many applications installed on the TC8000.	If you have installed additional applications on the TC8000, remove them to recover memory. See Uninstalling an Application on page 7-5 .
The TC8000 does not accept scan input.	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between scanner exit window and bar code is incorrect.	Move the TC8000 closer or further from the bar code to the proper scanning range.
	TC8000 is not programmed for the bar code.	Verify that the TC8000 can read the type of bar code being scanned (See Appendix A, Specifications). Ensure that the bar code parameters are set properly for the bar code being scanned.
	TC8000 is not programmed to generate a beep.	Verify that a beep on a good decode is used. See Bar Code Input on page 4-10 for more information.
During USB data communications, no data was transmitted, or transmitted data was incomplete.	Incorrect cable connection.	See Chapter 2, Accessories .
	Communications software is not installed or configured properly.	Perform setup as described in Chapter 2, Accessories .

Cradles

Table 8-2 Troubleshooting the Cradles

Symptom	Possible Cause	Solution
Device battery is not charging.	Device was removed from cradle or cradle was unplugged from AC power.	Ensure cradle is receiving power. Ensure device is seated correctly. Confirm main battery is charging. The battery fully charges in approximately four hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery (see Installing the Battery on page 1-7).
	The device is not fully seated in the cradle.	Remove and re-insert the device into the cradle, ensuring it is firmly seated.
	Ambient temperature of the cradle is too warm or too cold.	Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).

APPENDIX A SPECIFICATIONS

Technical Specifications

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

TC8000

Table A-1 *Technical Specifications*

Item	Description
Physical and Environmental Characteristics	
Dimensions (H x L x W)	233 mm x 76 mm x 64 mm 9.17 in. x 3.0 in. x 2.52 in.
Weight	Standard: 490 g (17.3 oz) Premium: 500 g (17.6 oz)
Display	Color Transflective LCD, 4 in. diagonal, 480 x 800 pixels, 24 bits (16 million pixels), 400 Nits.
Touch Panel	Multi-Touch projected capacitive; fingertip (bare or gloved) input; conductive stylus supported (sold separately)); Corning® Gorilla® Glass
Backlight	Configurable LED backlight control
Battery	PowerPrecision+ rechargeable 3.7 VDC 6,700 mAh Lithium-Ion battery.
Backup Power	Hot Swap backup
Expansion Slot	SDXC complaint microSD cards up to 32 GB (FAT32 format only).
Expansion Port	USB, Serial for ISV developers (optional)
Notification	Audible tone plus multi-color LEDs and vibration
Voice and Audio	Dual Speakers, Bluetooth wireless headset support

Table A-1 *Technical Specifications (Continued)*

Item	Description
Performance Characteristics	
CPU	Dual-Core 1.7 GHz processor
Operating System	Android AOSP 4.4.3 (KitKat) with Mobility Extensions (Mx), for true enterprise class operating system.
Memory	1 GB RAM Standard: 4 GB Flash (pSLC) Premium: 8 GB Flash (pSLC)
Application Development	Zebra Android EMDK
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)
Battery Charging Temperature	0° C to +40° C (32° F to 104° F) ambient temperature range.
Humidity	5% - 95% non-condensing
Drop Specification	Multiple 8 ft./2.4 m drop to concrete at room temperature per MIL-STD 810G; multiple 6 ft./1.8 m drop to concrete across full operating temperature range
Tumble	2,000 1 m (3.28 ft.) tumbles; meets and exceeds IEC tumble specifications
Sealing	IP65
Vibration	Sine 5-2000 Hz, 4 g peak, 1 hour per axis Random 20-2000 Hz, 6 g RMS or 0.04 g ² /Hz, 1 hour per axis
ESD	± 20k VDC air discharge ± 10k VDC contact discharge ± 10k VDC indirect discharge
Wireless LAN Data Communications	
Radio	IEEE ® 802.11a/b/g/n/d/h/i
Data Rates	5 GHz: 802.11a/n - up to 150 Mbps; 2.4 GHz: 802.11b/g/n - up to 72.2 Mbps
Operating Channels	Channels 36 - 165 (5180 - 5825 MHz) Channels 1 - 13 (2412 - 2472 MHz) Actual operating channels/frequencies depend on regulatory rules and certification agency
Security and Encryption	WEP, WPA - TKIP, WPA2- TKIP, WPA2-TKIP AES EAP TTLS, PAP, MSCHAP, MSCHAP v2, PEAPv0-MSCHAPv2, PEAPv1- EAP-GTC, EAP-TLS, EAP-FAST, LEAP
Multimedia	Wi-Fi Multimedia™ (WMM)

Table A-1 Technical Specifications (Continued)

Item	Description
Certifications	802.11n, WMM, WMM-PS, Cisco CCXv4, Wi-Fi Direct and Wi-Fi Display (Miracast).
Fast Roam	PMKID Caching, Opportunistic Key Caching (OKC), Cisco CCKM, 802.11r.
Wireless PAN Data Communications	
Bluetooth	Bluetooth 4.0 (Bluetooth Smart Technology)
USB	USB 2.0 Client for service and maintenance.
Data Capture	
Laser Scanning	SE965 1D standard range scan engine.
Imager	SE4750-SR Standard or SE4750-MR Medium Range omnidirectional 1D/2D imaging engine.
Camera	8MP Autofocus with flash, f/2.4 aperture (optional).
NFC	Multi-Protocol NFC (optional).
1D Laser Scanner Engine (SE965) Specifications	
Optical Resolution	0.005 in. minimum element width
Roll	± 35° from vertical
Pitch Angle	± 65° from normal
Skew Tolerance	± 40° from normal
Ambient Light	Tolerant to typical artificial indoor and natural outdoor (direct sunlight) lighting conditions. Fluorescent, Incandescent, Mercury Vapor, Sodium Vapor, LED: 450 Ft Candles (4,844 Lux) Sunlight: 10,000 Ft Candles (107,640 Lux)
Scan Repetition Rate	104 (± 14) scans/sec (bidirectional)
Scan Angle	Wide (Default): 47° (typical) Medium: 35° (typical) Narrow: 10° (typical)
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)

Table A-1 *Technical Specifications (Continued)*

Item	Description
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: 48.0° horizontal, 38.0° vertical
Illumination System	LEDs: Warm white LED Pattern Angle: 80° at 505 intensity
2D Imager Engine (SE4750-MR) 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: 48.0° horizontal, 38.0° vertical
Illumination System	LEDs: Warm white LED Pattern Angle: 80° at 505 intensity
Zebra Interactive Sensor Technology (IST)	
Motion Sensor	3-axis accelerometer; 3-axis gyroscope (optional).
Light Sensor	Automatically adjusts display backlight.
Navigation	Digital Compass (optional).
Proximity	Sensor for auto hands-free scanning.

Table A-2 Data Capture Options

Item	Description
1D Bar Codes	Chinese 2 of 5, Codabar, Code 11, Code 128, Code 39, Code 93, Discrete 2 of 5, EAN-8, EAN-13, GS1 DataBar, GS1 DataBar 14, GS1 DataBar Expanded GS1, GS1 DataBar Limited, Interleaved 2 of 5, Korean 2 of 5, Matrix 2 of 5, MSI, TLC39, Trioptic 39, UPCA, UPCE, UPCE1
2D Bar Codes	Australian Postal, Aztec, Canadian Postal, Composite AB, Composite C, Data Matrix, Dutch Postal, HAN XIN, Japanese Postal, Mail Mark, Maxi Code, Micro PDF-417, microQR, PDF-417, QR Code, US Planet, UK Postal, US Postnet, USPS 4-state (US4CB), US4state FICS

SE965 Standard Range Laser Decode Zones

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

Table A-3 SE965 Decode Distances

Symbol Density/ Bar Code Type/ W-N Ratio	Bar Code Content/ Contrast ^{Note 1}	Typical Working Ranges	
		Near	Far
5.0 mil Code 128	1234 80% MRD	1.2 in 3.05 cm	7.7 in 19.56 cm
5.0 mil Code 39; 2.5:1	ABCDEFGH 80% MRD	1.2 in 3.05 cm	12.5 in 31.75 cm
7.5 mil Code 39; 2.5:1	ABCDEF 80% MRD	1.1 in 2.79 cm	18.5 in 46.99 cm
10 mil Code 128	1234 80% MRD	1.2 in ^{Note 3} 3.05 cm ^{Note 3}	19.0 in 48.26 cm
13 mil 100% UPC	12345678905 80% MRD	1.6 in 4.06 cm	27.0 in 68.58 cm
15 mil Code 128	1234 80% MRD	1.0 in ^{Note 3} 2.54 cm ^{Note 3}	29.5 in 74.93 cm

Notes:

1. Contrast measured as Mean Reflective Difference (MRD) at 650 nm.
2. Working range specifications at ambient temperature (23°C), photographic quality symbols. Pitch=10°, roll=0°, skew=0°, ambient light < 150 ft-candles using Symbol or equivalent decoder.
3. Dependent on width of bar code.
4. Distances measured from front edge of scan engine chassis.

Table A-3 SE965 Decode Distances (Continued)

Symbol Density/ Bar Code Type/ W-N Ratio	Bar Code Content/ Contrast ^{Note 1}	Typical Working Ranges	
		Near	Far
20 mil Code 39; 2.2:1	123 80% MRD	1.4 in ^{Note 3} 3.56 cm ^{Note 3}	52.0 in 132.08 cm
55 mil Code 39; 2.2:1	CD 80% MRD	3.4 in ^{Note 3} 8.64 cm ^{Note 3}	100.0 in 254.00 cm
100 mil Code 39; 3.0:1 reflective	123456 80% MRD	2 ft ^{Note 3} 60.96 cm ^{Note 3}	17 ft 518.16 cm

Notes:

1. Contrast measured as Mean Reflective Difference (MRD) at 650 nm.
2. Working range specifications at ambient temperature (23°C), photographic quality symbols. Pitch=10°, roll=0°, skew=0°, ambient light < 150 ft-candles using Symbol or equivalent decoder.
3. Dependent on width of bar code.
4. Distances measured from front edge of scan engine chassis.

SE4750-SR Decode Distances

The table below lists the typical distances for selected bar code densities.

Table A-4 SE4750-SR Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
3 mil Code 39	2.8 in. 7.1 cm	6.2 in. 15.7 cm
5.0 mil Code 128	2.3 in. 5.8 cm	8.7 in. 22.0 cm
5 mil PDF417	3.0 in. 7.6 cm	8.1 in. 20.6 cm
6.67 mil PDF417	2.2 in. 5.6 cm	10.6 in. 26.9 cm
10 mil Data Matrix	2.4 in. 6.1 cm	10.6 in. 26.9 cm

* Limited by width of bar code in field of view.
 Note: Photographic quality bar code at 18° tilt pitch angle under 30 fcd ambient illumination.
 Distances measured from front edge of scan engine chassis.

Table A-4 SE4750-SR Decode Distances (Continued)

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
100% UPCA	1.6* in. 4.1* cm	23.0 in. 58.4 cm
15 mil Code 128	2.4* in. 6.1* cm	25.2 in. 64.0 cm
20 mil Code 39	1.6* in. 4.1* cm	36.3 in. 92.2 cm

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

Note: Photographic quality bar code at 18° tilt pitch angle under 30 fcd ambient illumination.
Distances measured from front edge of scan engine chassis.

SE4750-MR Decode Zones

Table A-5 lists the typical distances for selected bar code densities.

Table A-5 SE4750-MR Decode Distances

Symbology	Typical Working Range	
	Near	Far
5 mil Code 128	7.4 in. 18.8 cm	16.0 in. 40.6 cm
5 mil PDF417	8.1 in. 20.6 cm	13.1 in. 33.3 cm
7.5 mil Data Matrix	8.3 in. 21.1 cm	12.8 in. 32.5 cm
10 mil Data Matrix	7.0 in. 17.8 cm	17.0 in. 43.2 cm
13 mil UPCA	2.3* in. 5.8* cm	38.0 in. 96.5 cm
15 mil Code 128	4.0* in. 10.2* cm	40.0 in. 101.6 cm
20 mil Code 39	2.1* in. 5.3* cm	54.0 in. 137.2 cm
100 mil Code 39	11.0 in. 27.9 cm	172.0 in. 436.9 cm
160 mil Data Matrix	11.5 in. 29.2 cm	138.0 in. 350.5 cm

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

Note: Photographic quality bar code at 18° tilt pitch angle under 30 fcd ambient illumination. Distances measured from front edge of scan engine chassis.

I/O Connector Pin-Outs

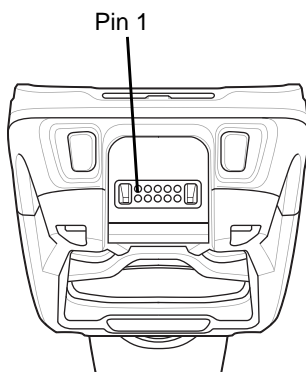


Figure A-1 I/O Connector

Table A-6 I/O Connector Pin-Outs

Pin	Signal	Description
1	DGND	Digital ground
2	MUX_RX_HMIC	External headset microphone/RX
3	POWER_IN	Adapter voltage in
4	HST_PLUGDETN	Headset or accessory detection
5	DGND	Audio path Ground
6	USB_ID	USB OTG ID pin.
7	MUX_TX_HSL	External headset speaker/TX
8	USB_PWR	USB VBUS Power
9	OTG_DP	USB OTG D+
10	OTG_DM	USB OTG D-

2-Slot USB Charge Cradle Technical Specifications

Table A-7 2-Slot USB Charge Cradle Technical Specifications

Item	Description
Dimensions	Height: 137.5 mm (5.41 in.) Width: 195.6 mm (7.70 in.) Depth: 134.5 mm (5.29 in.)
Weight	838 g (29.6 oz.)
Input Voltage	12 VDC
Power Consumption	20 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 +/- 10 kV contact +/- 10 kV indirect discharge

5-Slot Charge Only Cradle Technical Specifications

Table A-8 5-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 108.1 mm (4.26 in.) Width: 489.0 mm (19.25 in.) Depth: 134.5 mm (5.30 in.)
Weight	2.14 kg (4.71 lbs.)
Input Voltage	12 VDC
Power Consumption	60 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)

Table A-8 5-Slot Charge Only Cradle Technical Specifications (Continued)

Item	Description
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

5-Slot Charge Only Cradle with Battery Charger Technical Specifications

Table A-9 5-Slot Charge Only Cradle with Battery Charger Technical Specifications

Item	Description
Dimensions	Height: 137.0 mm (5.39 in.) Width: 489.0 mm (19.25 in.) Depth: 134.5 mm (5.30 in.)
Weight	2.33 kg (5.13 lbs.)
Input Voltage	12 VDC
Power Consumption	75 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

5-Slot Ethernet Cradle Technical Specifications

Table A-10 *5-Slot Ethernet Cradle Technical Specifications*

Item	Description
Dimensions	Height: 108.1 mm (4.26 in.) Width: 489.0 mm (19.25 in.) Depth: 134.5 mm (5.30 in.)
Weight	2.22 kg (4.89 lbs.)
Input Voltage	12 VDC
Power Consumption	67 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 Ethernet Cradle with Battery Charger Technical Specifications

Table A-11 *5-Slot Ethernet Cradle with Battery Charger Technical Specifications*

Item	Description
Dimensions	Height: 137.0 mm (5.39 in.) Width: 489.0 mm (19.25 in.) Depth: 134.5 mm (5.30 in.)
Weight	2.36 kg (5.20 lbs.)
Input Voltage	12 VDC
Power Consumption	82 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)

Table A-11 5-Slot Ethernet Cradle with Battery Charger Technical Specifications (Continued)

Item	Description
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

4-Slot Battery Charger Technical Specifications

Table A-12 4-Slot Battery Charger Technical Specifications

Item	Description
Dimensions	Height: 129.6 mm (5.10 in.) Width: 97.5 mm (3.84 in.) Depth: 134.5 mm (5.30 in.)
Weight	570 g (20.11 oz.)
Input Voltage	12 VDC
Power Consumption	27 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

USB and Charging Cable Technical Specifications

Table A-13 USB and Charging Cable Technical Specifications

Item	Description
Length	150 cm (5.90 in.)
Input Voltage	5.4 VDC (external power supply)
Operating Temperature	-20 °C to 50 °C (-4 °F to 122 °F)

Table A-13 *USB and Charging Cable Technical Specifications (Continued)*

Item	Description
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

Quick Disconnect Audio Cable Technical Specifications

Table A-14 *Quick Disconnect Audio Cable Technical Specifications*

Item	Description
Length	40 cm (15.75 in.)
Input Voltage	5.4 VDC
Operating Temperature	-20 °C to 50 °C (-4 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

3.5 mm Audio Cable Technical Specifications

Table A-15 *3.5 mm Audio Cable Technical Specifications*

Item	Description
Length	21.7 cm (8.54 in.)
Operating Temperature	-20 °C to 50 °C (-4 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

INDEX

Numerics

Numerics

2-slot USB charge cradle 2-4

A

accessories

 2-slot USB charge cradle 2-4

 four slot charge only cradle . . . 2-7, 2-10, 2-13, 2-20

android versionxiv

B

battery charging temperature A-2

build numberxiv

bullets xv

C

cleaning 8-1

configurationxiv

conventions

 notational xv

CPU A-2

cradles

 2-slot 2-4

 four slot charge only 2-7, 2-10, 2-13, 2-20

D

decode distances A-5

decode zones A-8

dimensions A-1

displayxiv, A-1

drop specification A-2

F

four slot charge only cradle 2-7, 2-10, 2-13, 2-20

H

humidity A-2

I

information, servicexvi

L

lithium-ion battery 1-1

M

maintenance 8-1

memory A-2

mobile computer

 starting 1-9

model numberxiv

O

operating system A-2

operating temperature A-2

P

parts of the mobile computer 1-1

R

related documentsxvi

related softwarexvi

S

screen
 Symbol splash screen 1-9
serial numberxiv
starting the mobile computer 1-9
storage temperature A-2

T

troubleshooting 8-5

U

unpacking 1-1

W

weight A-1
WLAN radio A-2



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

© 2017 ZIH Corp and/or its affiliates. All rights reserved. ZEBRA and the stylized Zebra head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.