



ET5X



Enterprise Tablet

Integrator Guide for Android Version 5.1.1



ET5X INTEGRATOR GUIDE FOR ANDROID VERSION 5.1.1

MN-002776-02

Rev. A

November 2016

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Zebra. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Zebra grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Zebra. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Zebra. The user agrees to maintain Zebra’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Zebra reserves the right to make changes to any software or product to improve reliability, function, or design.

Zebra does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Zebra Technologies Corporation, intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Zebra products.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	8/2016	Initial release.
-02 Rev A	11/2016	Update for software with Zebra added features.

TABLE OF CONTENTS

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

About This Guide

Introduction	xi
Documentation Set	xi
Configurations	xi
Chapter Descriptions	xii
Notational Conventions	xii
Related Documents and Software	xiii
Service Information	xiii

Chapter 1: Getting Started

Introduction	1-1
Unpacking	1-1
Getting Started	1-1
Installing a micro SIM Card (ET55 Only)	1-1
Installing a microSD Card	1-5
Charging the ET5X	1-6
Resetting the ET5X	1-6

Chapter 2: Accessories

Introduction	2-1
Charge Only Cradle	2-4
Installing the Insert	2-4
Charging the ET5X	2-5
Communication and Charging Cradle	2-7
Installing the Insert	2-8
Charging the ET5X	2-8
Rugged Communication and Charging Cradle	2-11
Charging the ET5X	2-12
4-Slot Charge Only Cradle	2-15

Insert Installation	2-15
Guide Installation	2-17
Battery Charger Installation	2-18
Power Setup	2-19
Charging the Battery	2-20
4-Slot Battery Charger	2-21
Rugged Frame	2-24
Expansion Back	2-27
Installation	2-27
Configuring the SE4750 Expansion Backs	2-29
Expansion Back Conversion Procedures	2-29
Replacement Hand Strap	2-31
Attaching the Stylus to the Expansion Back	2-34

Chapter 3: USB Communication

Connecting to a Host Computer via USB	3-1
Connecting to the ET5X as a Media Device	3-1
Disconnect from the Host Computer	3-1

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	4-2
Output Plug-ins	4-3
Profiles Screen	4-3
Profile Context Menu	4-4
Options Menu	4-4
Disabling DataWedge	4-5
Creating a New Profile	4-5
Profile Configuration	4-6
Associating Applications	4-7
Data Capture Plus	4-9
Bar Code Input	4-12
Enabled	4-12
Scanner Selection	4-12
Decoders	4-12
Decoder Params	4-14
HAN XIN	4-17
Decode Lengths	4-19
UPC EAN Params	4-19
Reader Params	4-21
Scan Params	4-23
Keystroke Output	4-23
Intent Output	4-24

Intent Overview	4-25
IP Output	4-26
Usage	4-27
Using IP Output with IPWedge	4-27
Using IP Output without IPWedge	4-28
Generating Advanced Data Formatting Rules	4-29
Configuring ADF Plug-in	4-30
Creating a Rule	4-30
Deleting a Rule	4-30
Defining Criteria	4-31
Defining an Action	4-32
Deleting a Rule	4-33
Order Rules List	4-33
Deleting an Action	4-34
ADF Example	4-35
DataWedge Settings	4-37
Importing a Configuration File	4-38
Exporting a Configuration File	4-39
Importing a Profile File	4-39
Exporting a Profile	4-39
Restoring DataWedge	4-39
Configuration and Profile File Management	4-40
Enterprise Folder	4-40
Auto Import	4-40
Programming Notes	4-40
Overriding Trigger Key in an Application	4-40
Capture Data and Taking a Photo in the Same Application	4-41
Soft Scan Feature	4-41
Sample	4-41
Scanner Input Plugin	4-41
Function Prototype	4-41
Parameters	4-42
Return Values	4-42
Example	4-42
Comments	4-42
Enumerate Scanners	4-43
Function Prototype	4-43
Parameters	4-43
Return Values	4-43
Example	4-44
Comments	4-44
Set Default Profile	4-44
Default Profile Recap	4-44
Usage Scenario	4-45
Function Prototype	4-45
Parameters	4-45
Return Values	4-45
Example	4-46
Comments	4-46
Reset Default Profile	4-47

Function Prototype	4-47
Parameters	4-47
Return Values	4-47
Example	4-47
Comments	4-47
Switch To Profile	4-48
Profiles Recap	4-48
Usage Scenario	4-48
Function Prototype	4-48
Parameters	4-48
Return Values	4-49
Example	4-49
Comments	4-49

Chapter 5: Settings

Screen Unlock Settings	5-1
Single User Mode	5-1
Set Screen Unlock Using PIN	5-2
Set Screen Unlock Using Password	5-2
Set Screen Unlock Using Pattern	5-3
Passwords	5-5
Accounts	5-5
Language Usage	5-5
Changing the Language Setting	5-6
Adding Words to the Dictionary	5-6
Keyboard Settings	5-6
About Tablet	5-6

Chapter 6: Application Deployment

Security	6-1
Secure Certificates	6-1
Installing a Secure Certificate	6-1
Development Tools	6-2
Android	6-2
EMDK for Android	6-3
StageNow	6-3
ADB USB Setup	6-3
Application Installation	6-3
Installing Applications Using the USB Connection	6-4
Installing Applications Using the Android Debug Bridge	6-4
Uninstalling an Application	6-4
System Update	6-5
Storage	6-10
Random Access Memory	6-11
Internal Storage	6-11
External Storage	6-12
Enterprise Folder	6-14
Application Management	6-14

Viewing Application Details	6-15
Stopping an Application	6-16
Managing Downloads	6-16

Chapter 7: Maintenance and Troubleshooting

Introduction	7-1
Maintaining the ET5X	7-1
Battery Safety Guidelines	7-1
Cleaning	7-2
Materials Required	7-2
Cleaning the ET5X	7-2
Housing	7-2
Display	7-3
Power Connector	7-3
Cleaning Cradle Connectors	7-3
Cleaning Expansion Back Connectors	7-3
Cleaning Frequency	7-4
Troubleshooting	7-5
ET5X	7-5
Charge Only Cradle	7-6
Communication and Charging Cradles	7-7
Expansion Back	7-7

Appendix A: Specifications

Technical Specifications	A-1
ET5X	A-1
SE4750 Expansion Back Decode Range	A-4
SE4750 SR Decode Ranges	A-4
SE4750 MR Decode Ranges	A-5
Accessory Specifications	A-6
Charge Only Cradle	A-6
Communication and Charging Cradle	A-6
Rugged Communication and Charging Cradle	A-7
Expansion Backs	A-7

ABOUT THIS GUIDE

Introduction

This guide provides information about configuring and setting up the ET5X 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 ET5X is divided into guides that provide information for specific user needs.

- **ET5X Quick Reference Guide** - describes how to get the ET5X tablet up and running.
- **ET5X User Guide** - describes how to use the ET5X tablet.
- **ET5X Integrator Guide** - describes how to setup, the ET5X and accessories.

Configurations

This guide covers the following configurations:

Configuration	Operating System	Radios	Display	Memory	Data Capture
ET50PE	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth	8" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs
ET50PT	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth	10" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs
ET55BE	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth WWAN: NA - LTE	8" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs

Configuration	Operating System	Radios	Display	Memory	Data Capture
ET55BT	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth WWAN: NA - LTE	10" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs
ET55TE	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth WWAN: ROW - LTE	8" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs
ET55TT	Version 5.1.1	WLAN: 802.11a/b/g/n/ac/d/h/i WPAN: Bluetooth WWAN: ROW - LTE	10" color	2 GB RAM/ 32 GB Flash	SE4750 Expansion Backs

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started*, provides information on getting the tablet up and running for the first time.
- *Chapter 2, Accessories*, describes the accessories available for the tablet and how to use the accessories with the tablet.
- *Chapter 3, USB Communication*, describes how to connect the ET5X to a host computer using USB.
- *Chapter 4, DataWedge Configuration*, describes how to use and configure the DataWedge application.
- *Chapter 5, Settings*, provides the settings for configuring the ET5X.
- *Chapter 6, Application Deployment*, provides information for developing and managing applications.
- *Chapter 7, Maintenance and Troubleshooting*, includes instructions on cleaning and storing the tablet, and provides troubleshooting solutions for potential problems during tablet operation.
- *Appendix A, Specifications*, includes a table listing the technical specifications for the tablet.

Notational Conventions

The following conventions are used in this document:

- “tablet” refers to the Zebra ET5X tablet.
- *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 ET5X tablets.

- *ET5X Quick Reference Guide*, p/n MN001844Axx
- *ET5X User Guide*, p/n MN-002838-xx

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

Service Information

If you have a problem with 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 explains how to set the device up for the first time.

Unpacking

Carefully remove all protective material from around the ET5X and save the shipping container for later storage and shipping.

Verify that you received all equipment listed below:

- Table with lithium-ion battery
- Quick Reference Guide.

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact the Zebra Support Center immediately. See [page xiii](#) for contact information.

Getting Started

In order to start using the ET5X for the first time:

- install the micro SIM Card (ET55 only)
- install microSD card (optional)
- start the ET5X
- configure the ET5X.

Installing a micro SIM Card (ET55 Only)



CAUTION Do not use nano to micro SIM card adapters.

To install a micro SIM card:

1. Press the Power button to turn off the ET55.
2. Lift the notched corner of the battery cover.

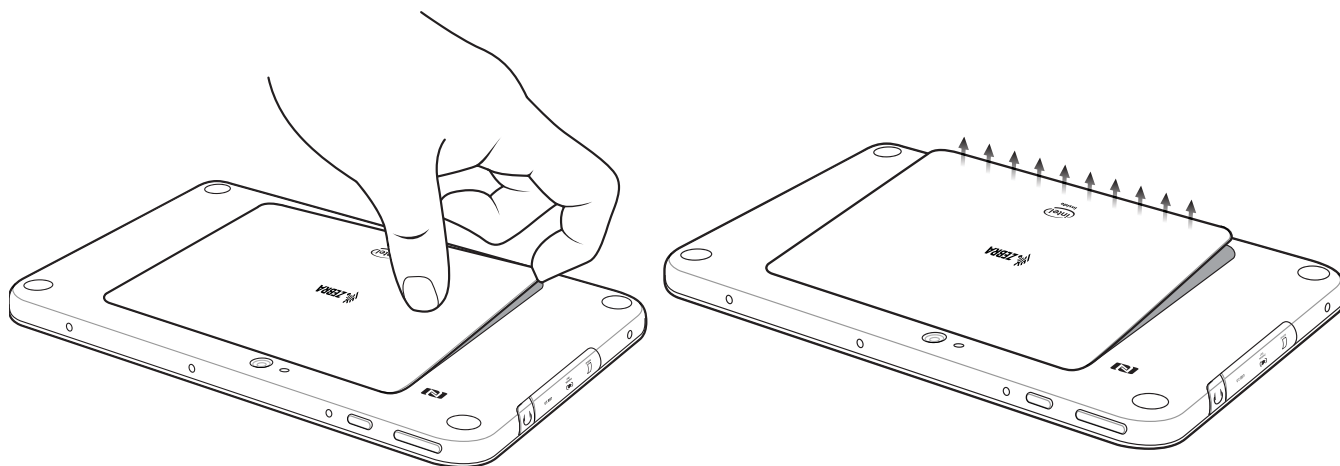


Figure 1-1 *Removing the Battery Cover*

3. Carefully lift the battery cover off the ET55.
4. On the 8" version, push the two locking tabs up, then pull up on the tab to remove battery.
On the 10" version, push the two locking tabs up (1), then, using index fingers, lift the battery up (2).

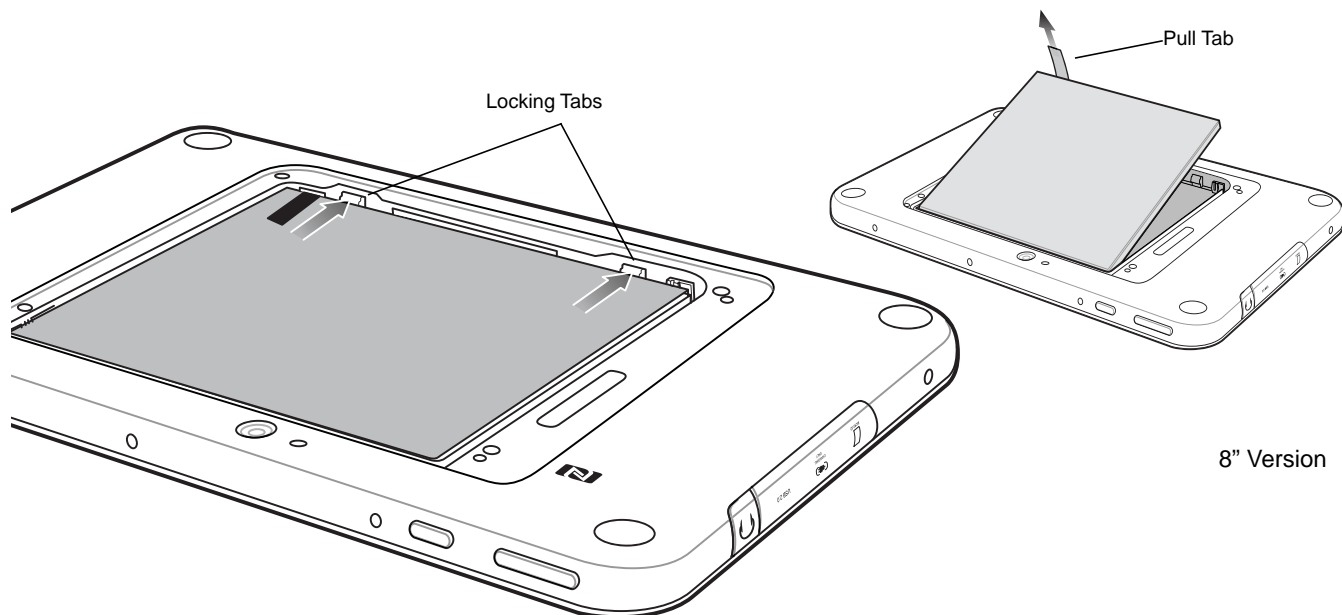


Figure 1-2 *Removing the Battery - 8"*

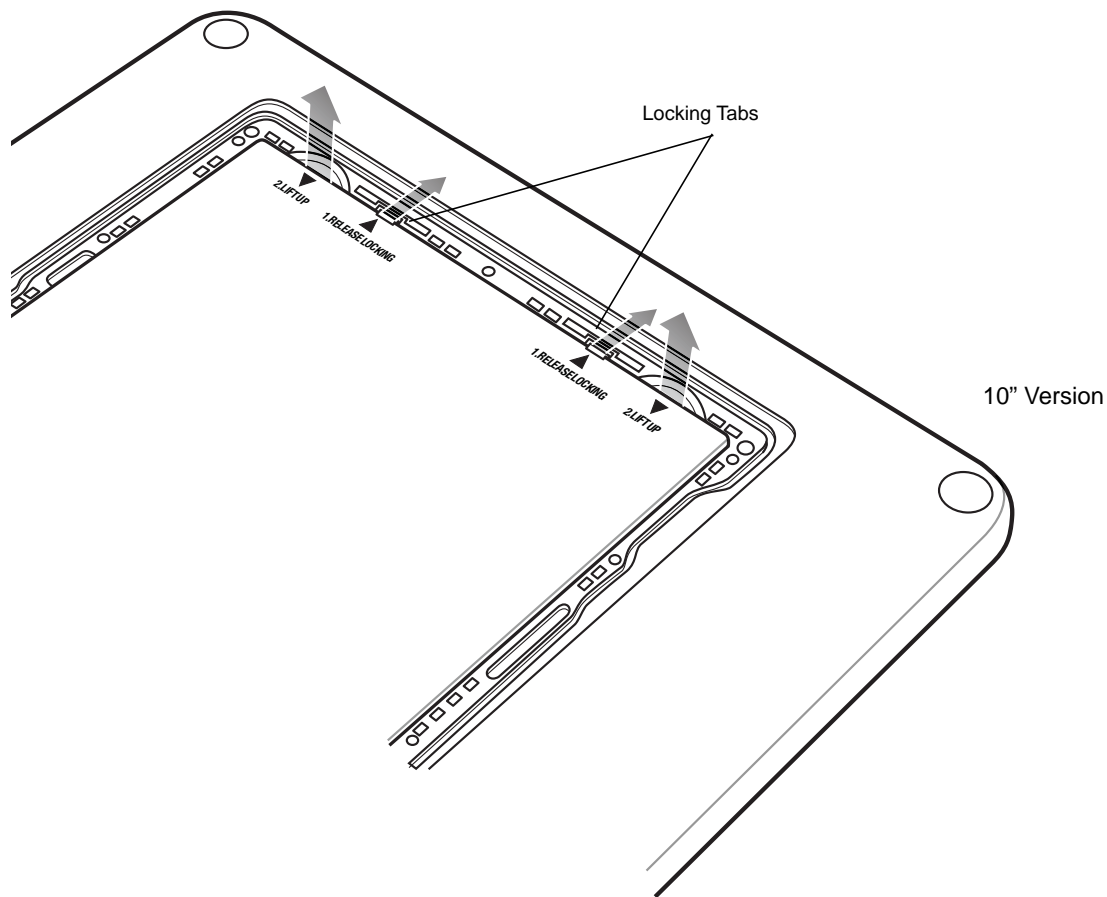


Figure 1-3 *Removing the Battery - 10"*

5. Insert the micro SIM card with contacts facing down.

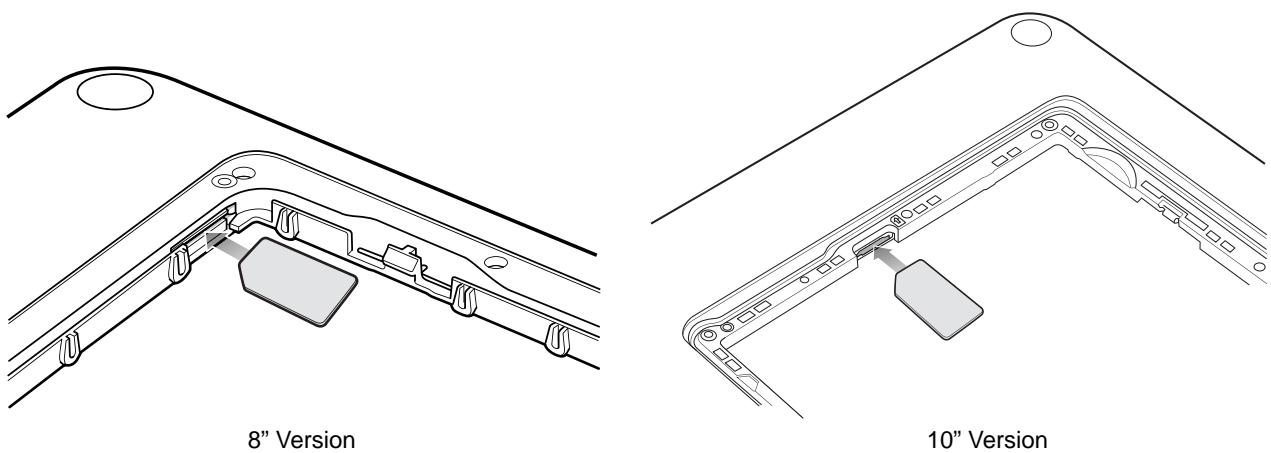


Figure 1-4 *Insert SIM Card*

6. Push the SIM card in and ensure that it locks into place.
7. Replace the battery.
On the 10" version, ensure that the two battery latches engage.

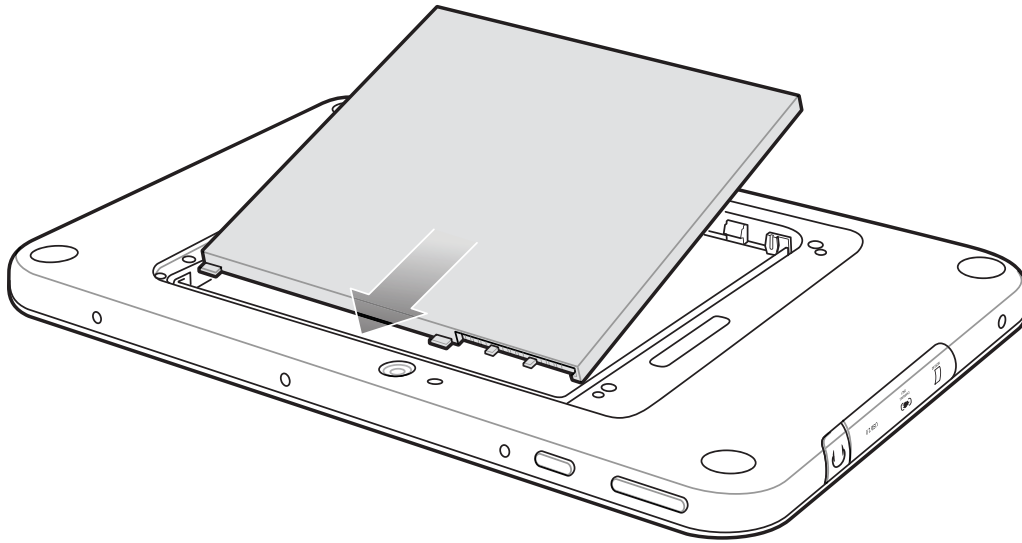


Figure 1-5 *Insert Battery*



CAUTION Be aware of the orientation of the battery cover. Failure to replace the battery cover properly may damage the battery cover.

8. Align the tabs on the underside of the cover with the slot around the battery well. Make sure that the notch on the battery cover is at the bottom left corner of the ET5X.

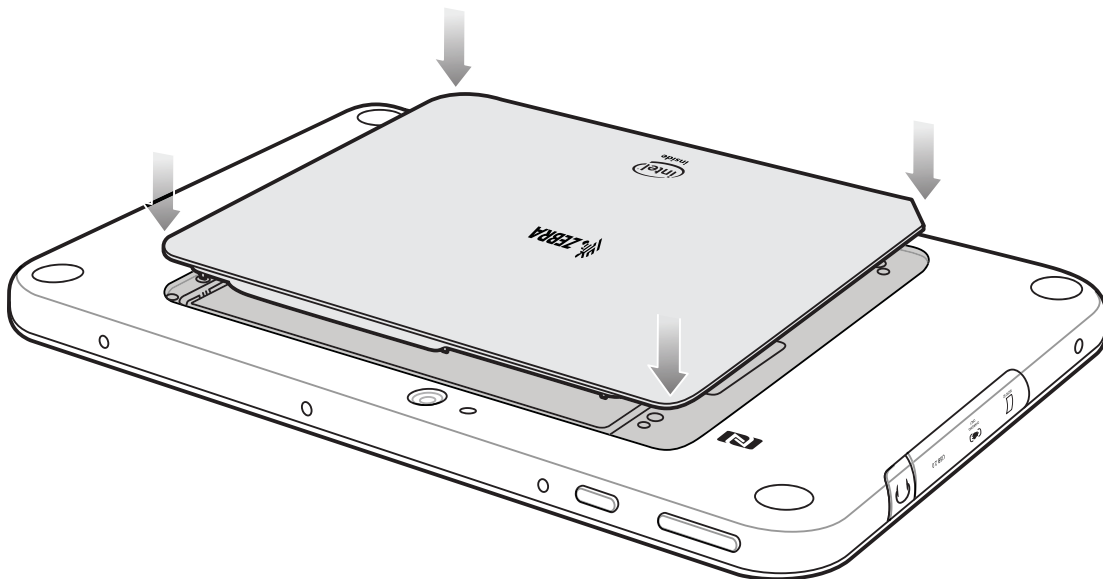


Figure 1-6 *Align Battery Cover*

9. Carefully press down around the edge of the cover. Make sure that the cover is seated properly.

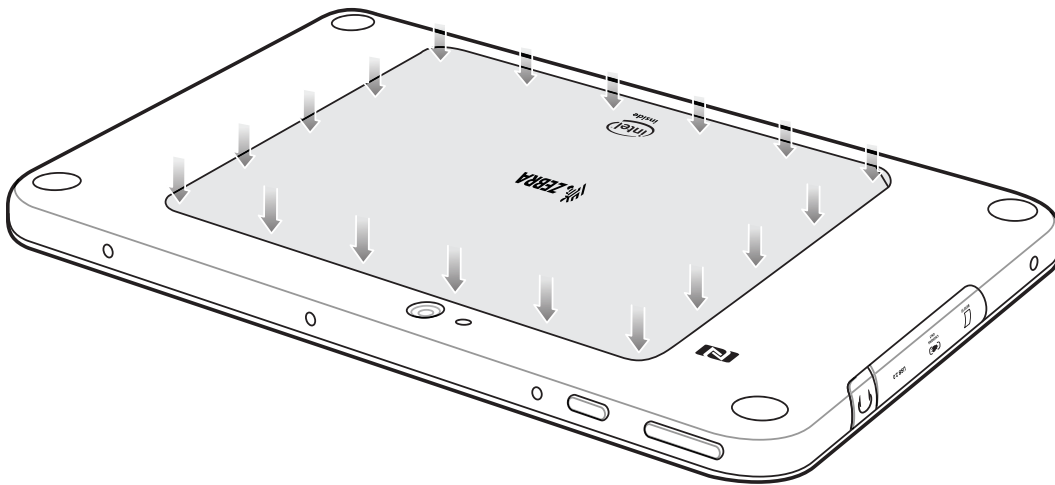


Figure 1-7 *Press Down on Battery Cover*

10. Press Power button to turn on the ET55.

Installing a microSD Card

To install a microSD card:

1. Open access door.

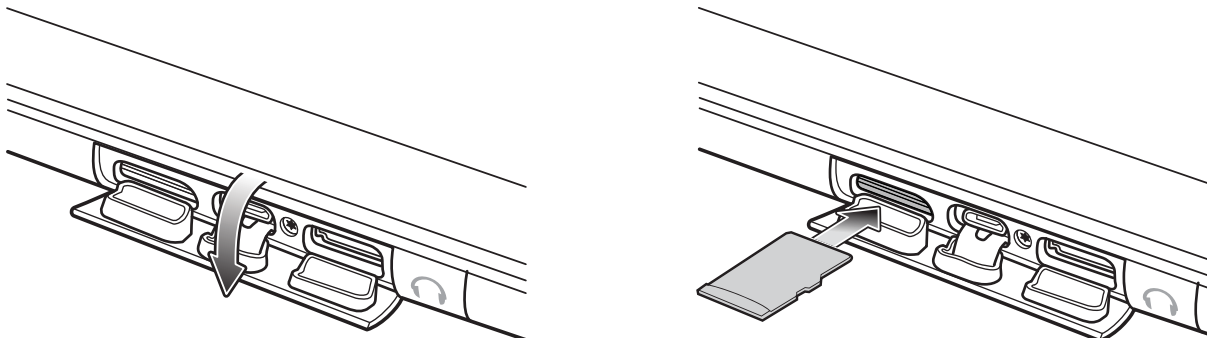


Figure 1-8 *Open Access Door*

2. Insert microSD card into slot with contacts facing down.
3. Press the card in to ensure that it is seated properly.
4. Close access door.

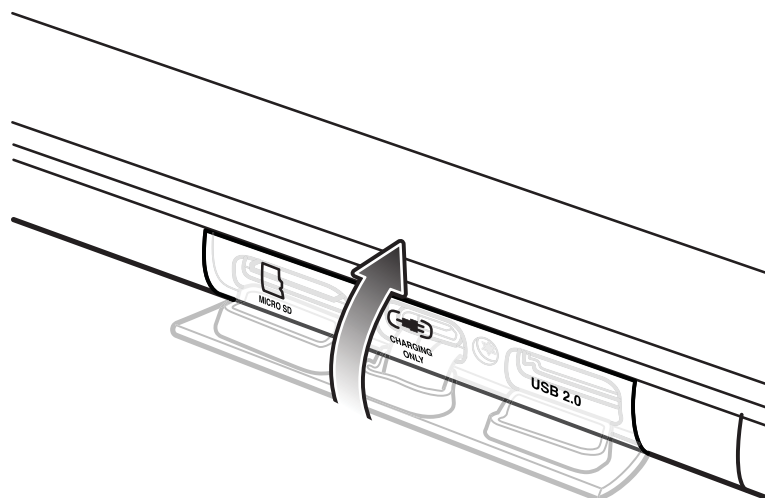


Figure 1-9 Close Access Door

Charging the ET5X

✓ **NOTE** Use only Zebra approved accessories listed in this guide when charging the ET5X.

Use one of the available accessories to charge the ET5X. Refer to Chapter 6, Accessories for charging accessories.

The main battery usually fully charges in less than three hours. If an Expansion Back is attached, the main battery fully charges in less than 4.5 hours.

Table 1-1 Charging Indicator

LED	Indication
Off	ET5X is not in cradle. ET5X is not seated properly. Cradle is not powered.
Orange	ET5X is charging.
Green	Charging complete. Note: When the battery is initially inserted in the ET5X, the amber LED flashes once if the battery power is low or the battery is not fully inserted.
Red	Error in charging; check placement of the ET5X.

Resetting the ET5X



CAUTION Resetting the ET5X erases all data from the ET5X, including your account configuration, applications, music, pictures and files. Make sure that you back up all the required data before you proceed.

Resetting the ET5X returns the device to original factory settings.

To reset the ET5X:

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch **Backup & rest.**
3. Touch **Factory data reset.**



CAUTION Resetting the ET5X erases all data from the ET5X, including your account configuration, applications, music, pictures and files.

4. Touch **RESET TABLET.**
5. If required, enter PIN, or password and touch **Continue.**
6. Touch **ERASE EVERYTHING.** The ET5X erases all data then reboots.

CHAPTER 2 ACCESSORIES

Introduction

The ET5X accessories provide a variety of product support capabilities. [Table 2-1](#) lists the accessories available.

Table 2-1 ET5X Accessories

Accessory	Part Number	Description
Cradles		
Charge Only Cradle	CRD-ET5X-1SCG1	Charges the ET5X main battery and optional Power Pack installed in the Expansion Back. Requires power supply PWRS-14000-148R and country-specific AC line cord.
Communication and Charging Cradle	CRD-ET5X-1SCOM1	Charges the ET5X main battery and optional Power Pack installed in the Expansion Back. Requires power supply PWRS-14000-148R and country-specific AC line cord.
Rugged Communication and Charging Cradle	CRD-ET5X-1SCOM1R	Charges the ET5X main battery and optional Power Pack installed in the Expansion Back. Supports ET5X with rugged frame and rugged IO Adapter. Requires power supply PWRS-14000-148R and country-specific AC line cord.
4-Slot Cradle Only Cradle	CRD-ET5X-SE4CO1-01	Charges up to four ET5X main battery and optional Power Pack installed in the Expansion Back and up to four Power Pack in the optional 4-Slot Battery Charger. Requires power supply PWRS-14000-241R, DC line cord and country-specific AC line cord.
Chargers		
Power Supply	PWRS-14000-148C	Provides power to the 4-Slot Battery Charger.

Table 2-1 ET5X Accessories

Accessory	Part Number	Description
Power Supply	PWRS-14000-148R	Provides power to the Charge Only Cradle, the Communication and Charging Cradles, and Rugged Charge Connector.
4-Slot Battery Charger	SAC-ET5X-4PPK1-01	Chargers up to four Power Packs. Requires power supply PWRS-14000-148C and country-specific AC line cord.
Rugged Charge Connector	CHG-ET5X-CBL1-01	Charges the ET5X main battery and optional Power Pack installed in the Expansion Back. Requires power supply PWRS-14000-148R and country-specific AC line cord.
Miscellaneous		
Replacement 8" Internal Battery	BTRY-ET5X-8IN1-01	Replacement battery for 8" tablet.
Replacement 10" Internal Battery	BTRY-ET5X-10IN1-01	Replacement battery for 10" tablet.
Replacement 8" Battery Cover	KT-ET5X-8BTDR1-01	Replacement battery cover for 8" tablet.
Replacement 10" Battery Cover	KT-ET5X-10BTDR1-01	Replacement battery cover for 10" tablet.
8" Rugged Frame with IO Adapter	SG-ET5X-8RCSE1-02	Add extra protection for the 8" tablet and IO Adapter for connection to the Rugged Communication and Charging Cradle.
10" Rugged Frame with IO Adapter	SG-ET5X-10RCSE1-01	Add extra protection for the 10" tablet and IO Adapter for connection to the Rugged Communication and Charging Cradle.
Replacement Rugged IO Connector	SG-ET5X-RGIO1-01	Replacement rugged IO connector for the Rugged Frames.
8" SE4750 Expansion Back	ZBK-ET5X-8SCN5-02	Provides data capture using the SE4750 scan engine, rotating hand strap and slot for optional Power Pack.
8" Expansion Back	ZBK-ET5X-8RH1-01	Provides rotating hand strap and slot for optional Power Pack.
10" SE4750 Expansion Back	ZBK-ET5X-10SCN5-02	Provides data capture using the SE4750 scan engine, rotating hand strap and slot for optional Power Pack.
10" Expansion Back	ZBK-ET5X-10RH1-01	Provides rotating hand strap and slot for optional Power Pack.
Power Pack	BTRY-ET5X-PRPK1-01	Provides additional power for charging the ET5X battery using an Expansion Back.

Table 2-1 *ET5X Accessories*

Accessory	Part Number	Description
Active Stylus	KT-ET5X-ASTY2-01	Provides easy writing, drawing, and navigation and accuracy with the thin tip.
Replacement Expansion Back Hand Strap	SG-ET5X-RHTP1-01	Replacement hands strap for Expansion Backs.
Coiled Stylus Tether	SG-ET5X-SLTETR-01	Secures a stylus to the hand strap on the Expansion Backs.
10" Screen Protector	KT-ET5X-10SCRN1-01	Provides additional screen protection for 10" tablet (5-pack).
8" Screen Protector	KT-ET5X-8SCRN1-01	Provides additional screen protection for 8" tablet (5-pack).
10" Screen Protector (Rugged Frame)	KT-ET5X-8SCRN1-01	Provides additional screen protection for 10" tablet with Rugged Frame (5-pack).
8" Screen Protector (Rugged Frame)	KT-ET5X-10SCRN1-02	Provides additional screen protection for 8" tablet with Rugged Frame (5-pack).
8" Operations Case	SG-ET5X-8HLST-01	Provides carrying solution for 8" tablet.
10" Operations Case	SG-ET5X-10HLST-01	Provides carrying solution for 10" tablet.
Universal Shoulder Strap	58-40000-007R	Use with the 8" Operations Case and D-clips to carry tablet on shoulder.

Charge Only Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines* on page 7-1.

This section describes how to use a Charge Only Cradle with the ET5X. The Charge Only Cradle ships with an insert that must be installed when inserting an ET5X without the protective boot installed.

The Charge Only Cradle:

- Provides power for operating the ET5X.
- Charges the ET5X's battery.

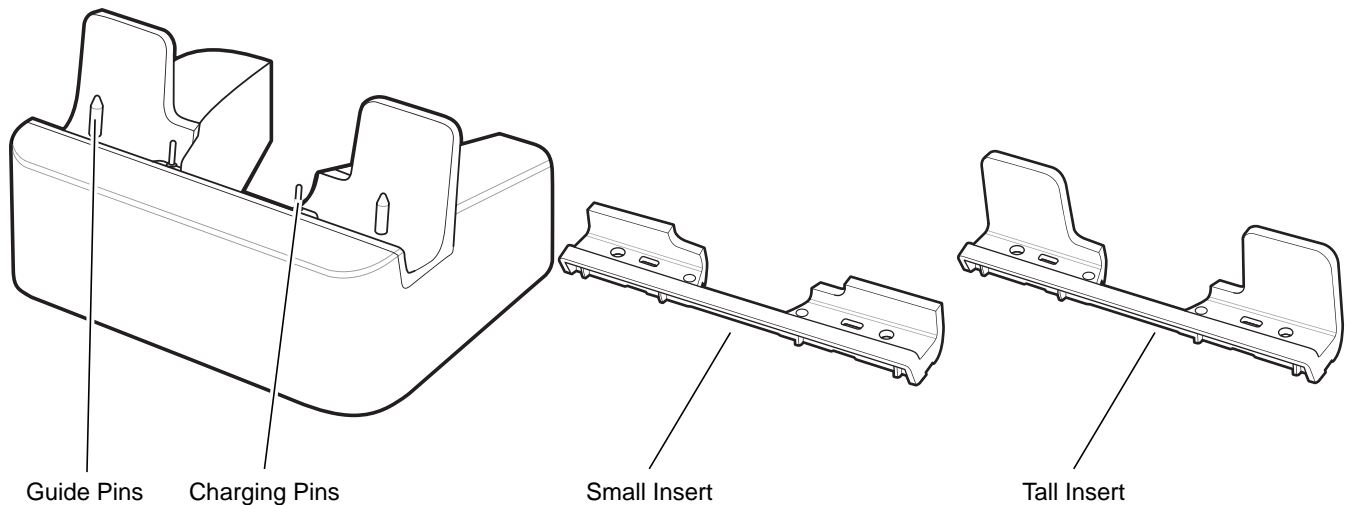


Figure 2-1 Charge Only Cradle - Front View

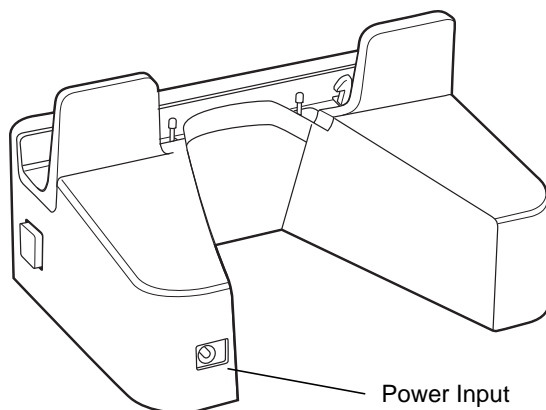


Figure 2-2 Charge Only Cradle - Rear View

Installing the Insert

The insert must be installed onto the cradle when docking an ET5X without a protective boot.

1. Align the insert over the pins.

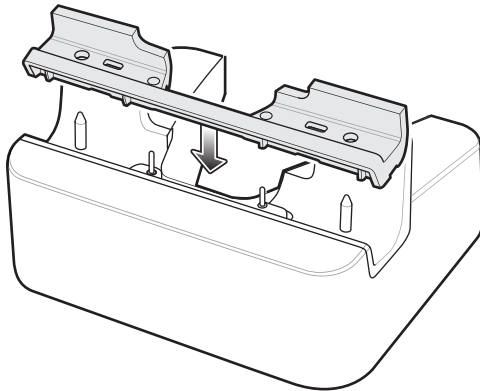


Figure 2-3 *Align Insert with Cradle*

2. Press the insert down until it seats flush in the cradle.

Charging the ET5X

To charge the ET5X in the Charge Only Cradle:

1. Align the ET5X with the alignment pins on the cradle.
2. Insert the ET5X into the cradle.

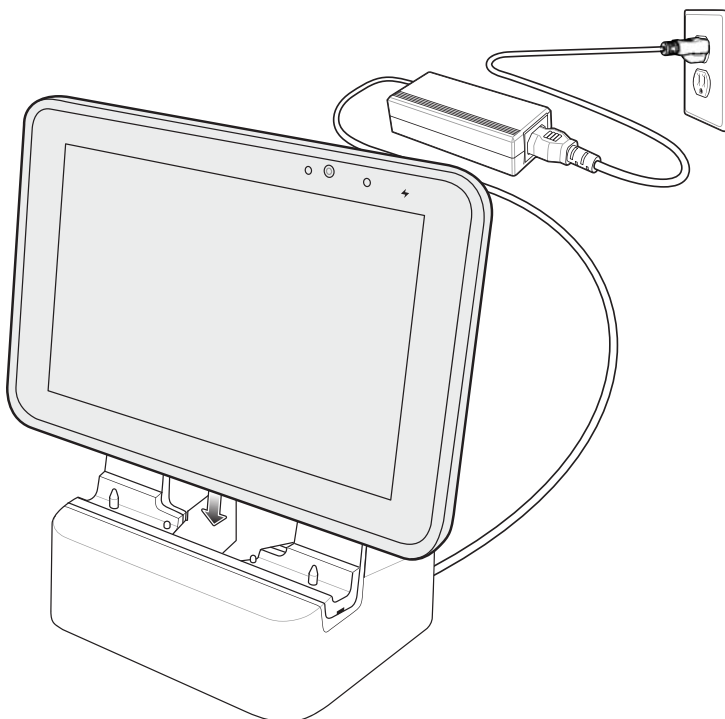


Figure 2-4 *Insert ET5X into Charge Only Cradle*

3. The ET5X Charging LED indicates charging.
4. To remove the ET5X from the Charge Only Cradle, hold the cradle down with one hand and lift the ET5X.

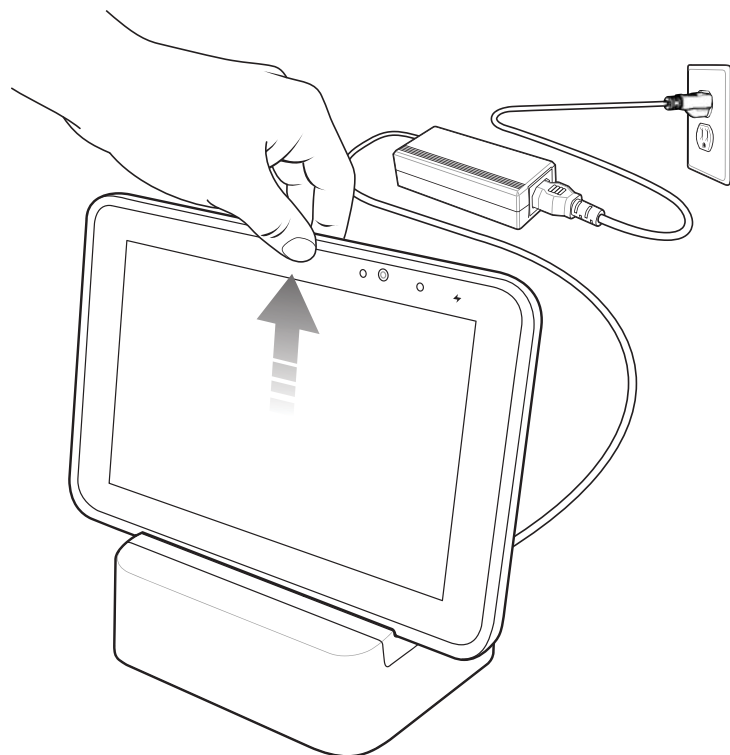


Figure 2-5 Remove ET5X from Charge Only Cradle

Charge batteries in ambient temperatures from 0°C to 40°C (32°F to 104°F) as reported by the battery. Charging is intelligently controlled by the charger. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures.

The ET5X’s amber charge LED shows the status of the battery charging in the ET5X. See [Table 1-1 on page 1-6](#) for charging status indications.

The battery charges in less than three hours. If an Expansion Back is attached with Power Pack, the main battery fully charges in less than 4.5 hours and the Power Pack charges in less than 3.5 hours.

✓ **NOTE** The Charging indicator only illuminates when the ET5X is connected to AC power.

Table 2-2 Charging Indicator

LED	Indication
Off	ET5X is not in cradle. ET5X is not seated properly. Cradle is not powered.
Orange	ET5X is charging.
Green	Charging complete.
Red	Error in charging; check placement of the ET5X.

Communication and Charging Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines* on page 7-1.

This section describes how to use a Communication and Charging Cradle with the ET5X.

The Communication and Charging cradle:

- Provides power for operating the ET5X.
- Provides ports for connecting USB devices to the tablet, video output and connection to a LAN.

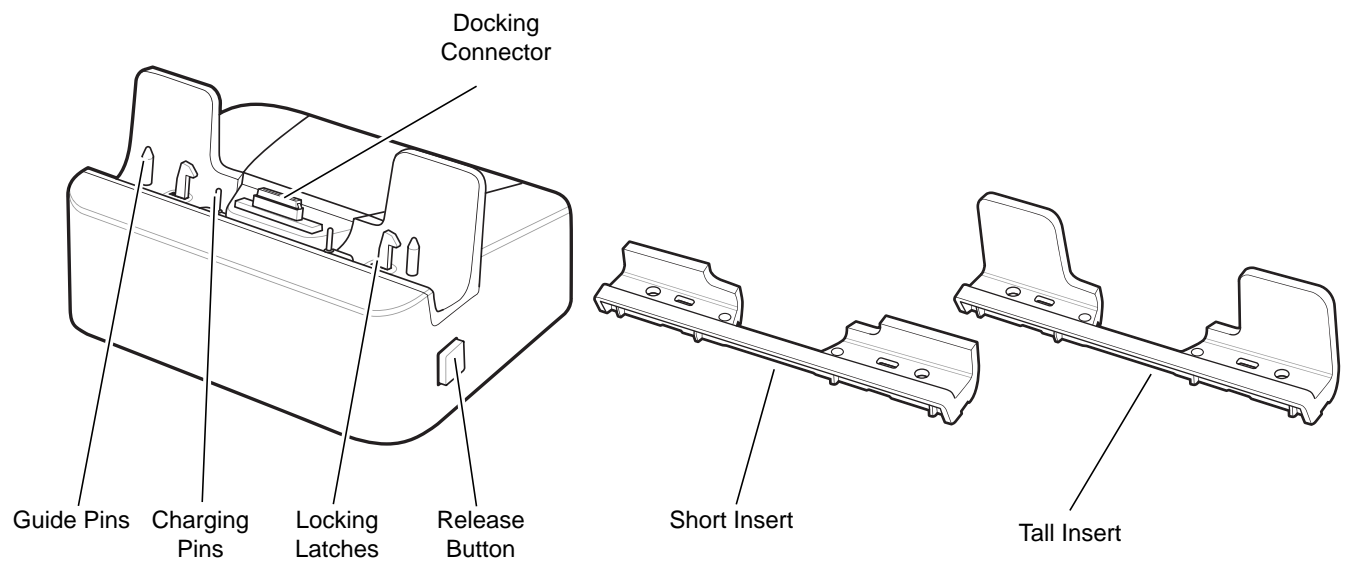


Figure 2-6 Communication and Charging Cradle - Front View

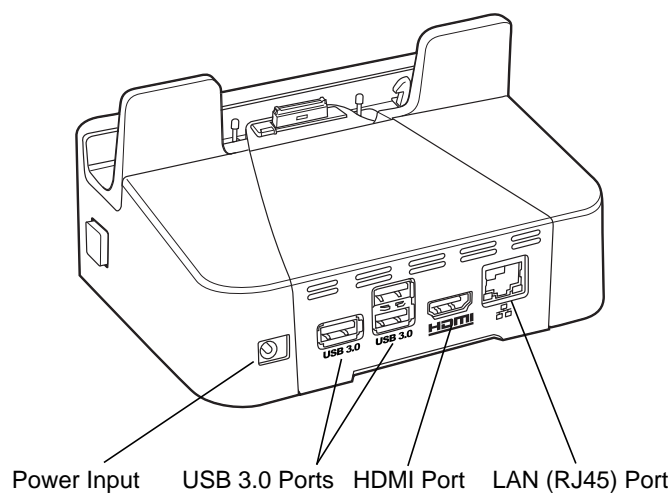


Figure 2-7 Communication and Charging Cradle - Rear View

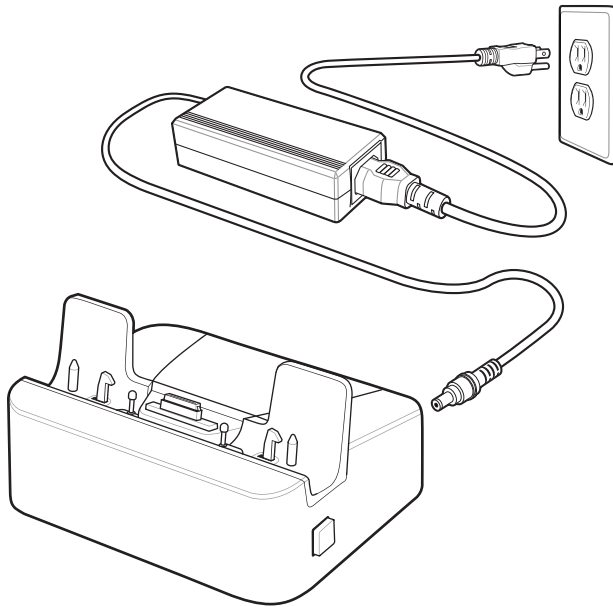


Figure 2-8 *Communication and Charging Cradle - Setup*

Installing the Insert

The insert must be installed onto the cradle when docking an ET5X without a protective boot.

1. Align the insert over the pins.

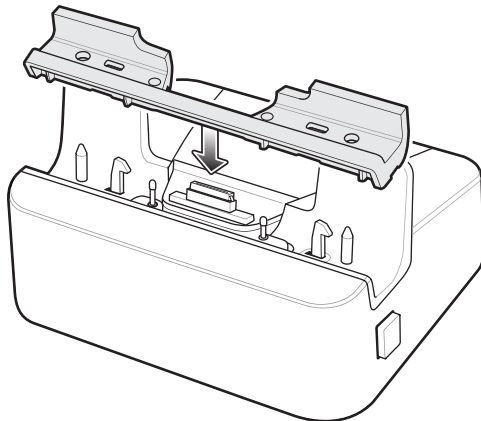


Figure 2-9 *Align Insert with Cradle*

2. Press the insert down until it seats flush in the cradle.

Charging the ET5X

To charge the ET5X in the Communication and Charging Cradle:

1. Open the bottom access door and hold it to the back of the tablet.
2. Align the ET5X with the alignment pins on the cradle.
3. Insert the ET5X into the cradle. Note that the Communication and Charging Cradles contains a locking mechanism that locks the ET5X to the cradle.

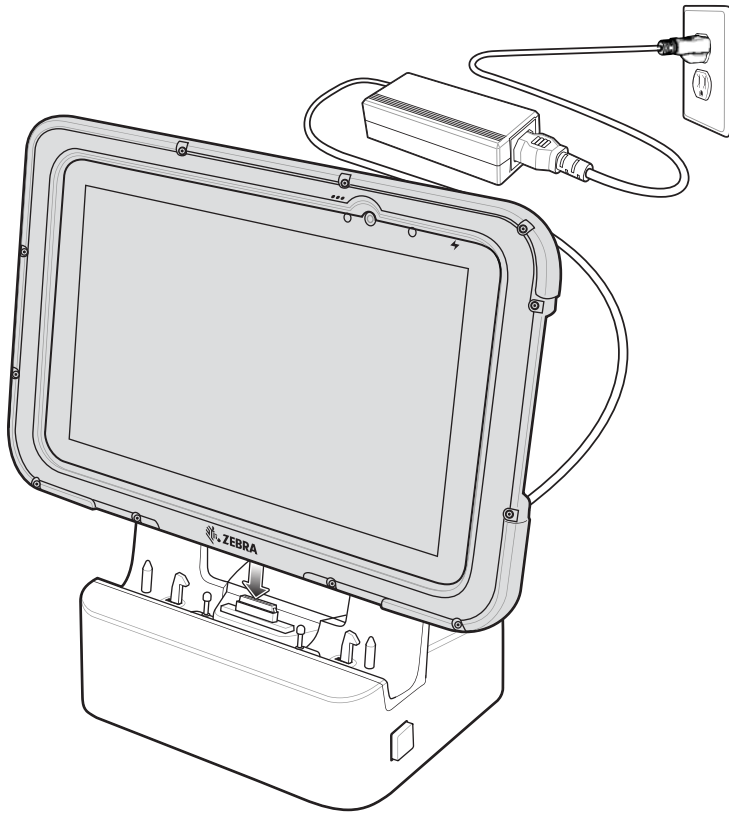


Figure 2-10 *Insert ET5X with Rugged Frame into Communication and Charging Cradle*

4. The ET5X Charging LED indicates charging.
5. To remove the ET5X from the Communication and Charging Cradle, press the release button on the right side of the cradle and lift the ET5X. Use thumb to hold down the cradle.

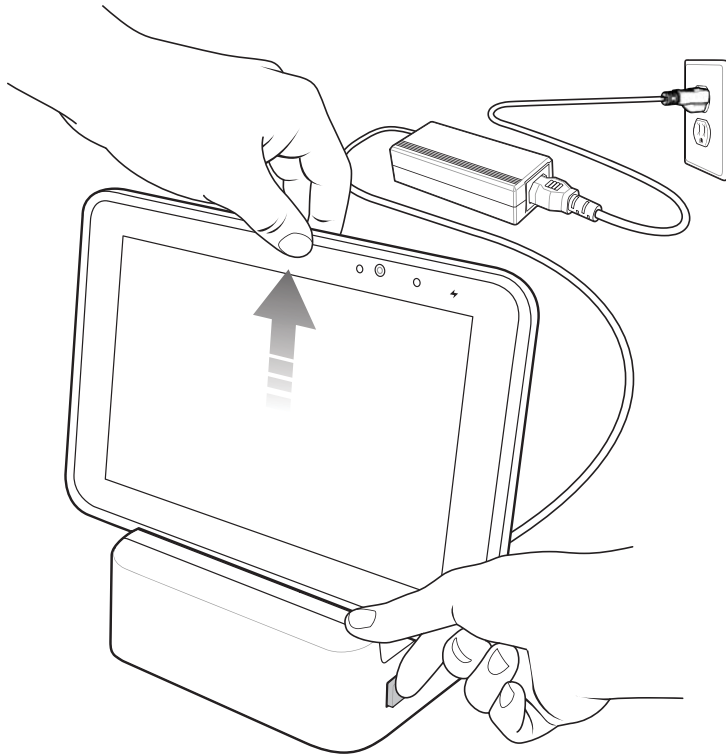


Figure 2-11 *Remove ET5X from Communication and Charging Cradles*

Charge batteries in ambient temperatures from 0°C to 40°C (32°F to 104°F) as reported by the battery. Charging is intelligently controlled by the charger. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures.

The ET5X's amber charge LED shows the status of the battery charging in the ET5X. See [Table 1-1 on page 1-6](#) for charging status indications.

The battery charges in less than three hours. If an Expansion Back is attached with Power Pack, the main battery fully charges in less than 4.5 hours and the Power Pack charges in less than 3.5 hours.

Rugged Communication and Charging Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-1*.

This section describes how to use a Rugged Communication and Charging Cradle with the ET5X.

The Rugged Communication and Charging cradle:

- Provides power for operating the ET5X.
- Provides ports for connecting USB devices to the tablet, video output and connection to a LAN.
- Charges the ET5X's battery and optional Power Pack installed in an Expansion Back.

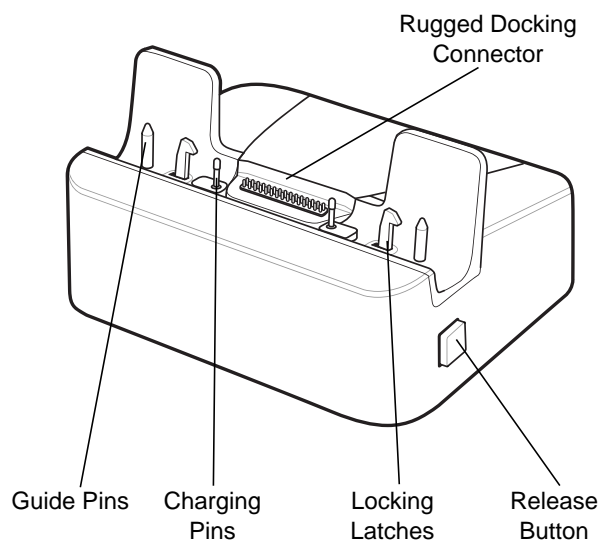


Figure 2-12 *Rugged Communication and Charging Cradle - Front View*

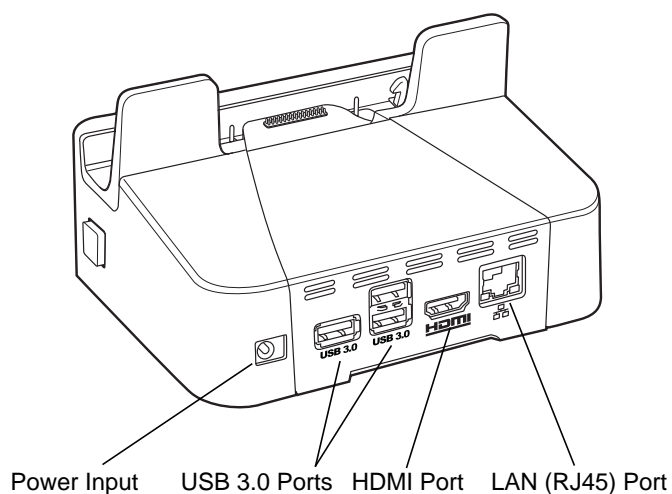


Figure 2-13 *Rugged Communication and Charging Cradle - Rear View*

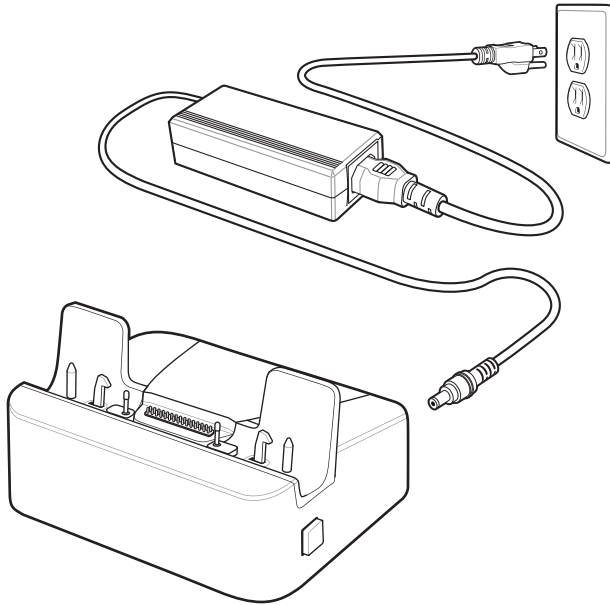


Figure 2-14 *Rugged Communication and Charging Cradle - Setup*

Charging the ET5X

To charge the ET5X using the Rugged Communication and Charging Cradle:

1. Align the ET5X with the alignment pins on the cradle.
2. Insert the ET5X into the cradle. Note that the Rugged Communication and Charging Cradles contains a locking mechanism that locks the ET5X to the cradle.

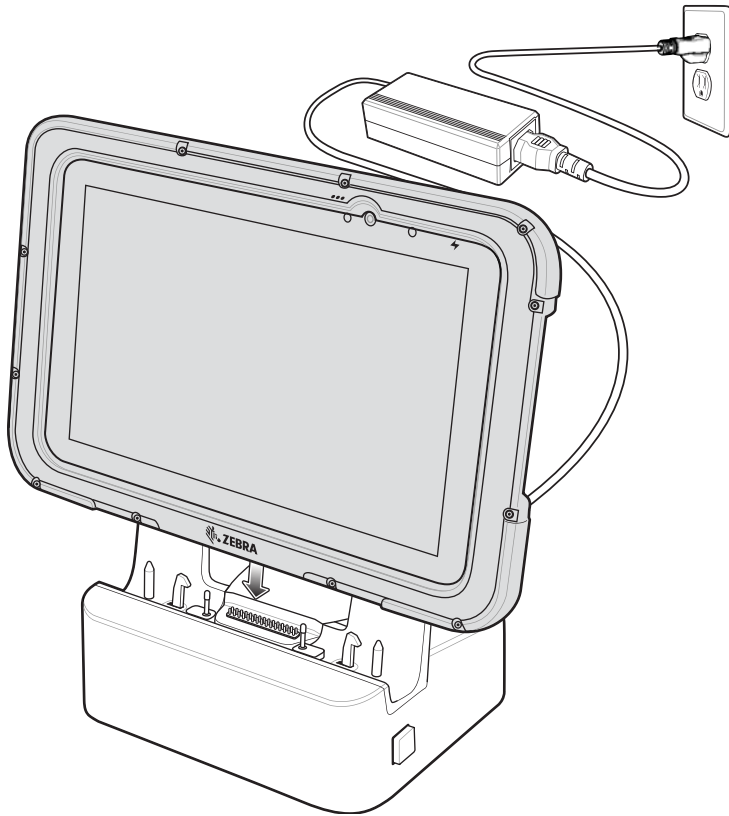


Figure 2-15 *Insert ET5X with Rugged Frame and IO Adapter into Rugged Communication and Charging Cradle*

3. The ET5X Charging LED indicates charging.
4. To remove the ET5X from the Rugged Communication and Charging Cradle, press the release button on the right side of the cradle and lift the ET5X. Use thumb to hold down the cradle.

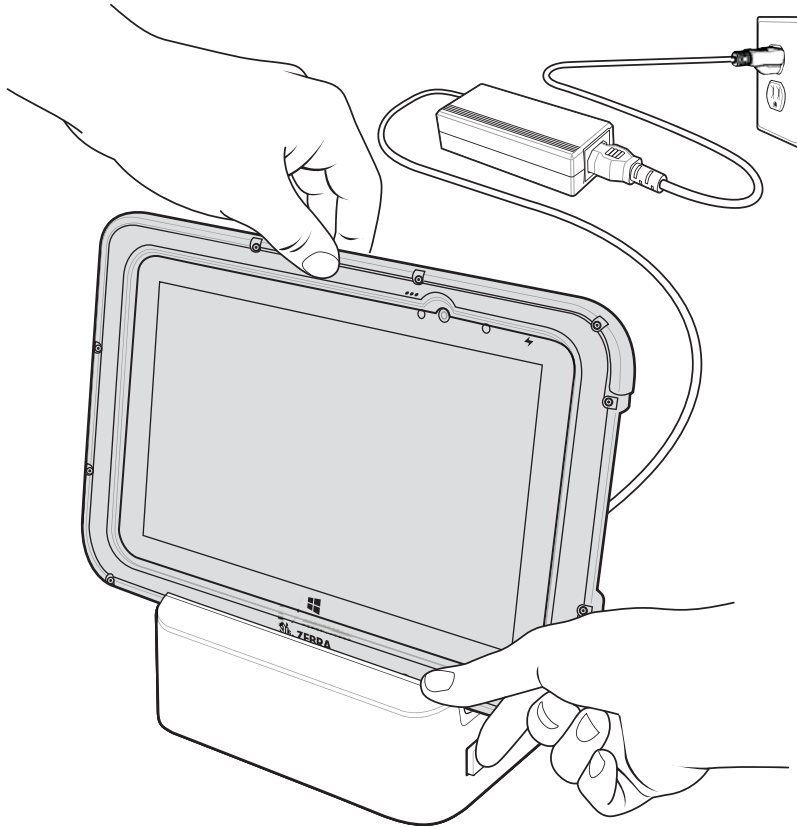


Figure 2-16 *Remove ET5X from Rugged Communication and Charging Cradles*

Charge batteries in ambient temperatures from 0°C to 40°C (32°F to 104°F) as reported by the battery. Charging is intelligently controlled by the charger. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures.

The ET5X's amber charge LED shows the status of the battery charging in the ET5X. See [Table 1-1 on page 1-6](#) for charging status indications.

The battery charges in less than three hours. If an Expansion Back is installed, the main battery fully charges in less than 4.5 hours and the Power Pack charges in less than 3.5 hours.

4-Slot Charge Only Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-1*.

- Provides 5 VDC power for operating the ET5X.
- Simultaneously charges up to four ET5Xs and up to four Power Packs using the optional Battery Charger Adapter.

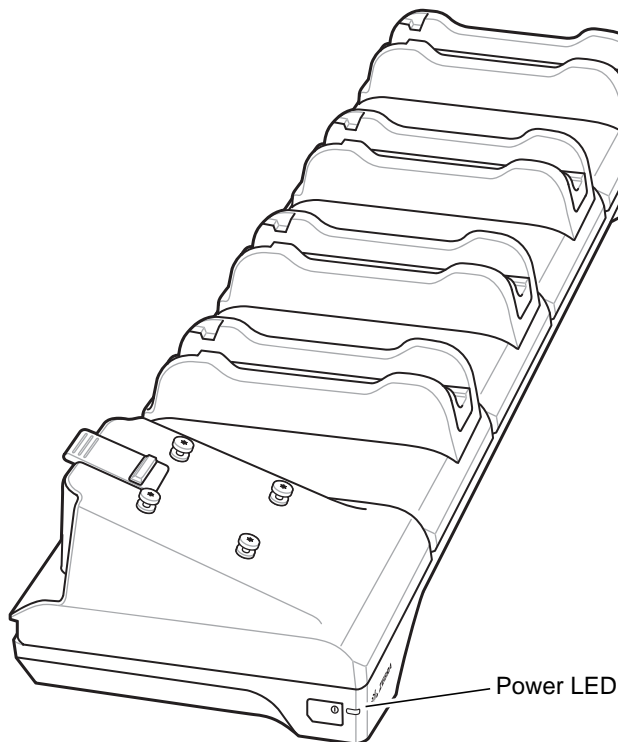


Figure 2-17 4-Slot Charge Only Cradle

Insert Installation

Install inserts into slots for ET5X tablets without Rugged Frame.

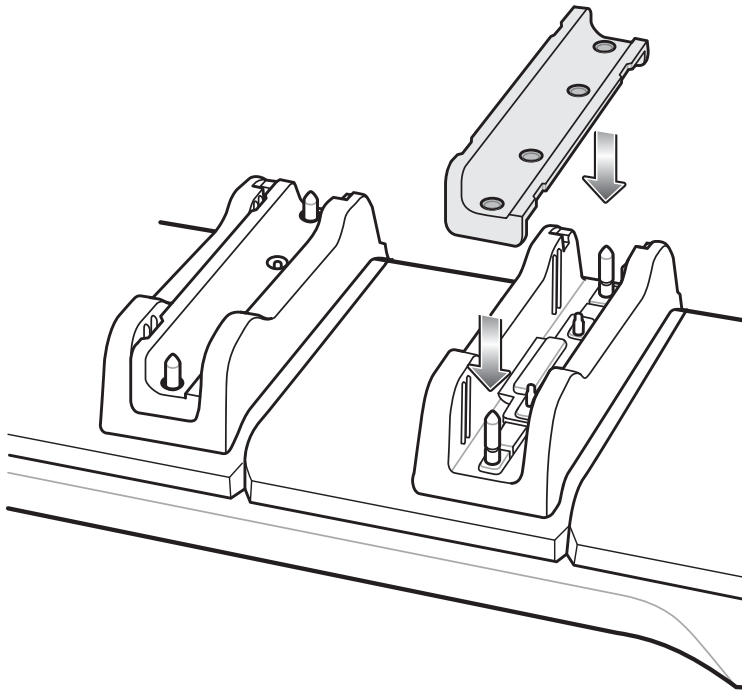


Figure 2-18 *Install Insert in Slot*

Guide Installation

The cradle comes with four 8" tablets guide and four 10" tablet guides. Install the appropriate guides for the tablets.

1. Align the two tabs on the guide with the two slots in the cradle.

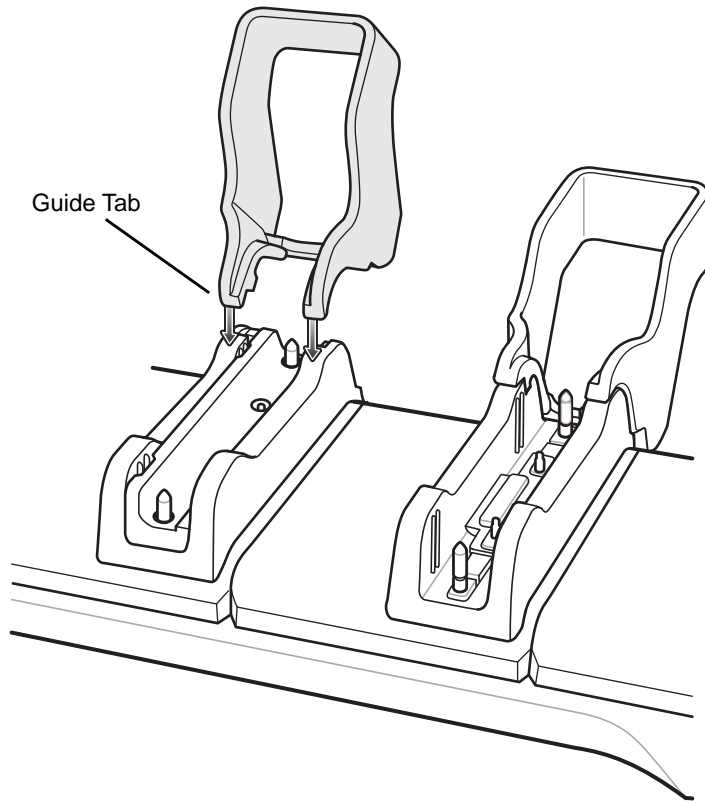


Figure 2-19 *Align Guide with Slot*

2. Place the guide down onto the cradle and then rotate the guide until it snaps into the cradle.

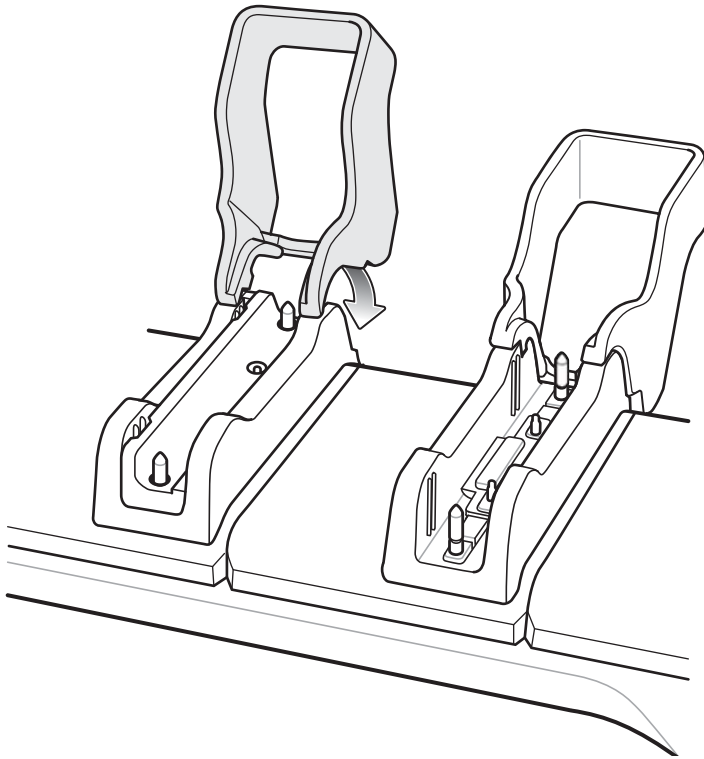


Figure 2-20 *Rotate Guide onto Slot*

Battery Charger Installation

Install optional 4-Slot Battery Charger onto cradle:

1. Align the mounting holes on the bottom of the charger with the four studs on the cradle.

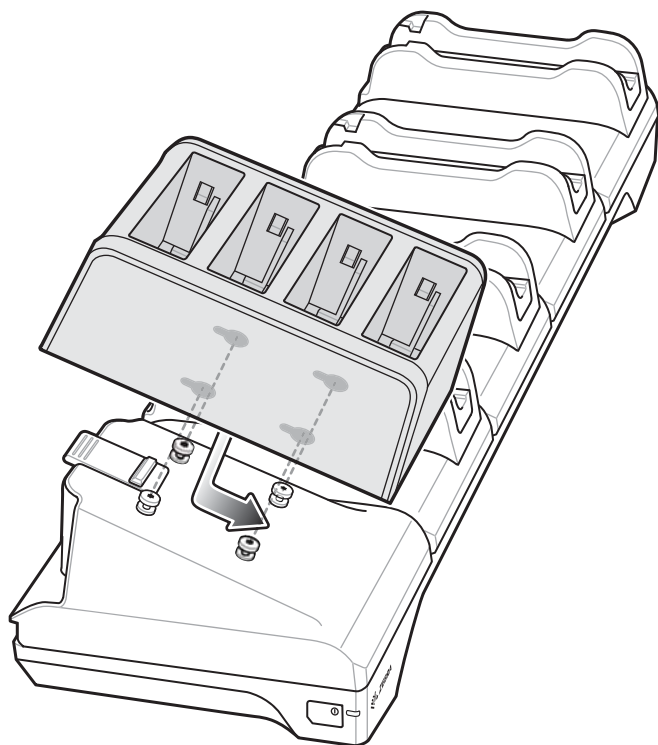


Figure 2-21 *Align Battery Charger on Adapter*

2. Place the charger on the cradle and then slide toward the front of the cradle.

Power Setup

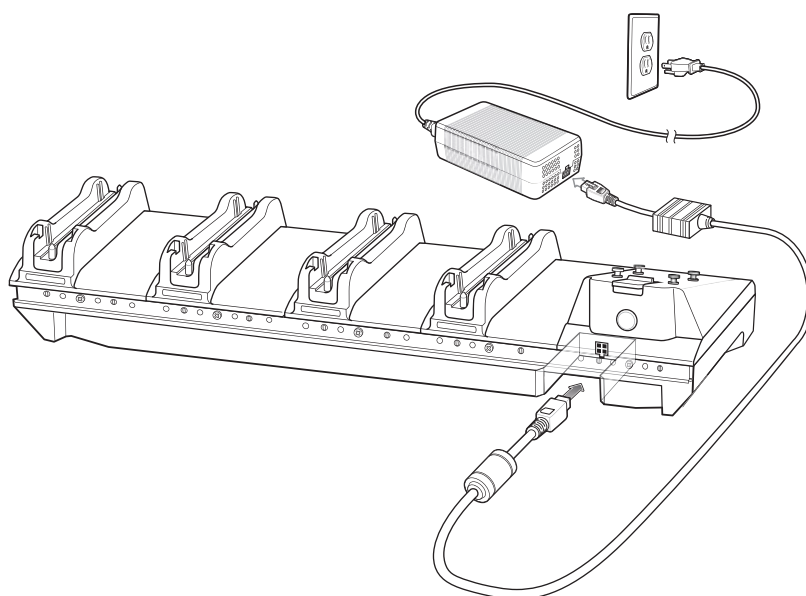


Figure 2-22 *4-Slot Charge Only Cradle Setup*

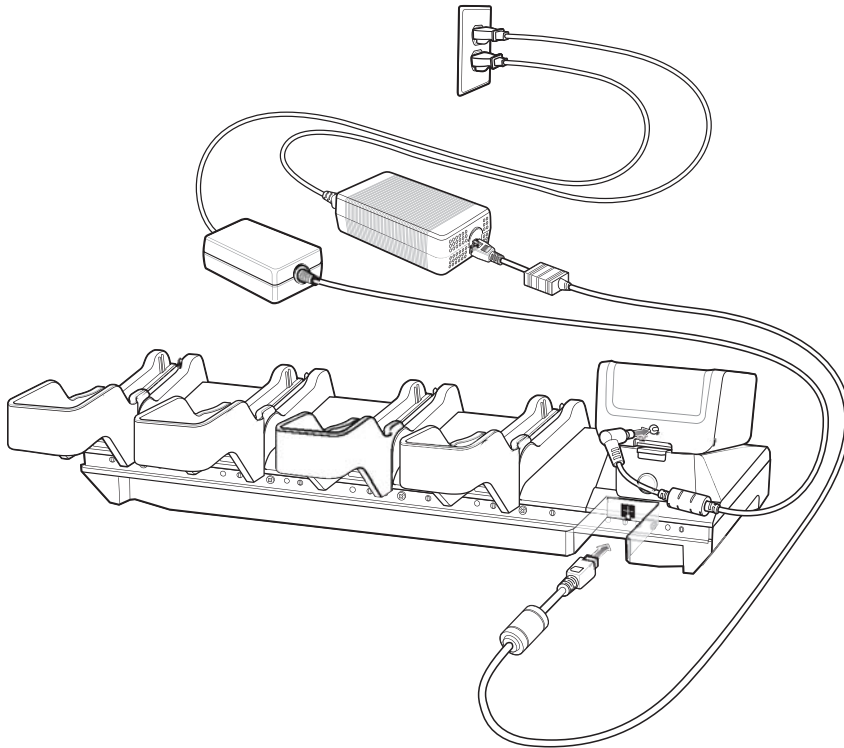


Figure 2-23 4-Slot Charge Only Cradle with Battery Charger Setup

Charging the Battery

Charge batteries in ambient temperatures from 0°C to 40°C (32°F to 104°F) as reported by the battery. Charging is intelligently controlled by the charger. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures.

The ET5X's amber charge LED shows the status of the battery charging in the ET5X. See [Table 1-1 on page 1-6](#) for charging status indications.

The battery charges in less than three hours. If an Expansion Back is attached with Power Pack, the main battery fully charges in less than 4.5 hours and the Power Pack charges in less than 3.5 hours.

4-Slot Battery Charger



CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 7-1*.

The 4-Slot Battery Charger:

- Provides 12 VDC power for charging the Power Packs.
- Simultaneously charges up to four Power Packs.

To charge a Power Pack:

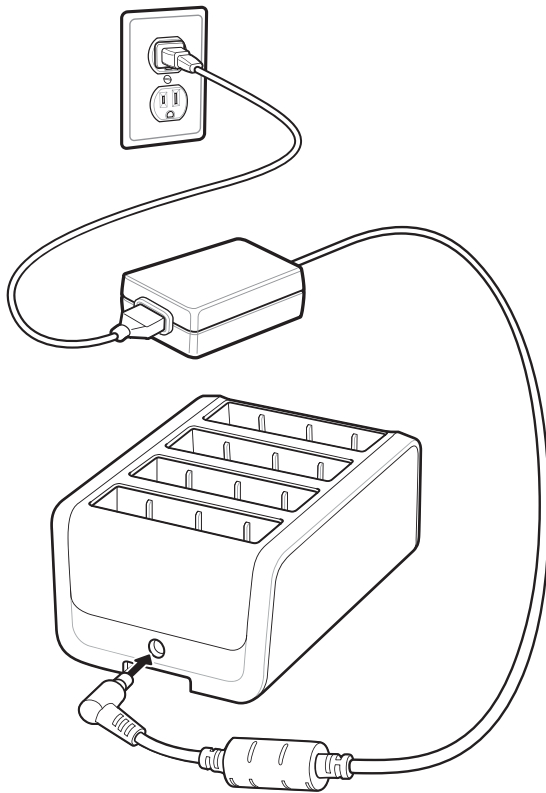


Figure 2-24 4-Slot Battery Charger

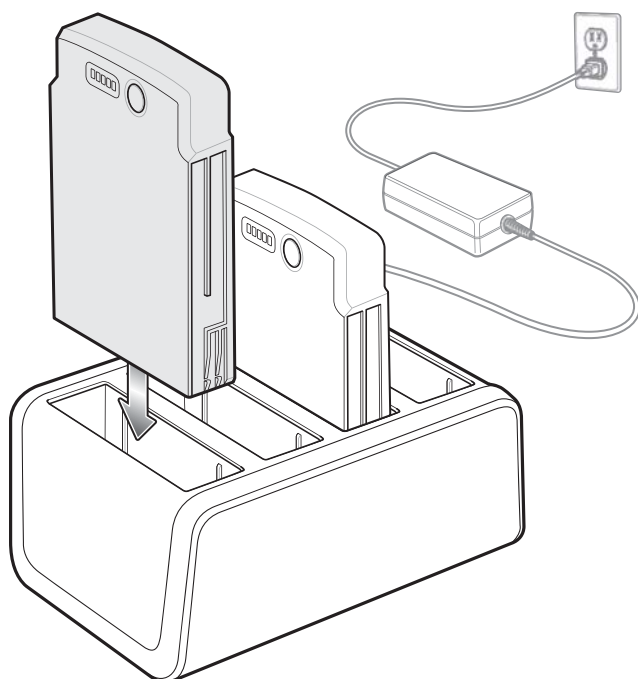


Figure 2-25 *Insert Power Pack*

When charging, the Power Pack Charge Level Indicators indicate the charge level.

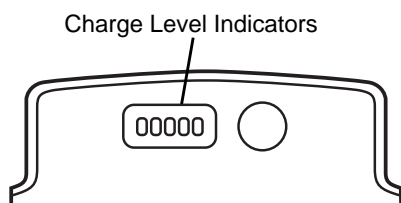






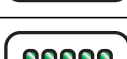
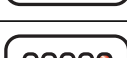





Figure 2-26 *Power Pack Charge LEDs*

Table 2-3 *Power Pack Charge Status Indicators*

Power Pack Indicators	Description
	Power not applied to Power Pack.
	Charge level is between 0% and 20%.
	Charge level is between 20% and 40%.
	Charge level is between 40% and 60%.
	Charge level is between 60% and 80%.
	Charge level is between 80% and 100%.
	Fully charged.
	Charging error.
	Solid Green LED
	Blinking Green LED
	Blinking Red LED

Charge batteries in ambient temperatures from 0°C to 40°C (32°F to 104°F) as reported by the battery. Charging is intelligently controlled by the charger. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures.

Rugged Frame

The Rugged Frame (8 inch and 10 inch) adds additional protection to the ET5X. Use the Rugged I/O Adapter when docking the ET5X into the Rugged Communications and Charging Cradle.

1. Open the access cover.

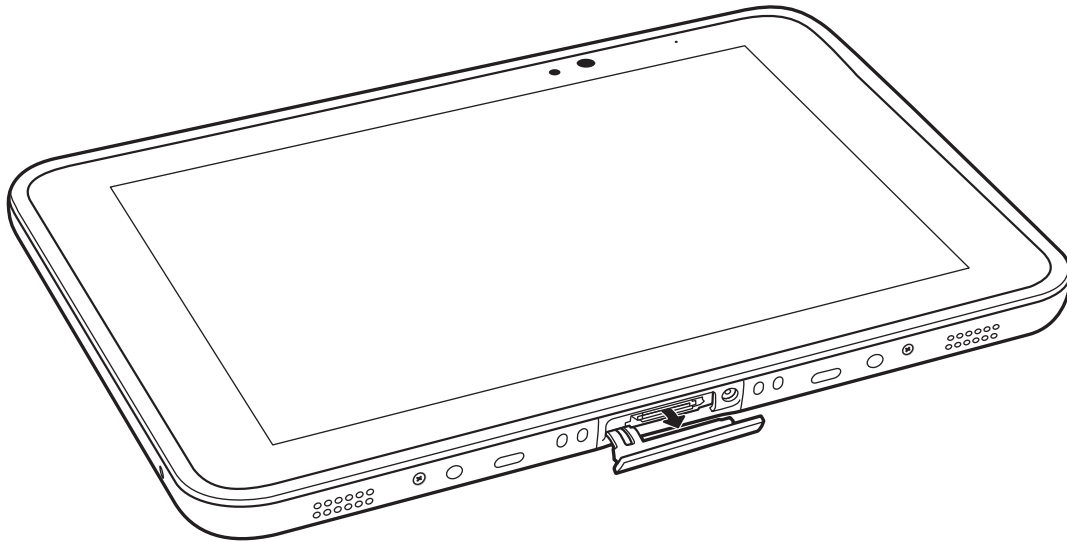


Figure 2-27 *Open Access Door*

2. If installing the Rugged IO Adapter, pull the access cover away from the ET5X until it separates from the ET5X.

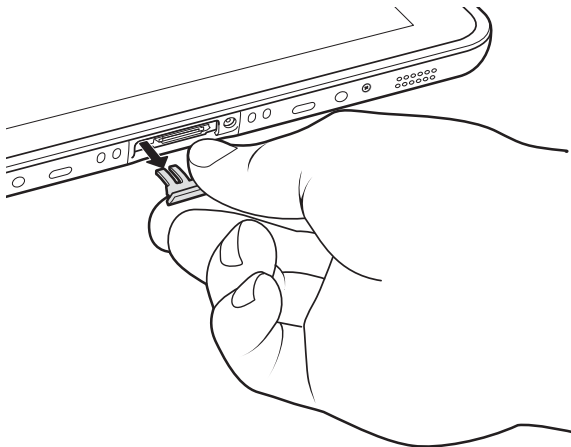


Figure 2-28 *Remove Access Door*

3. Insert the Rugged IO Adapter onto the tablet.

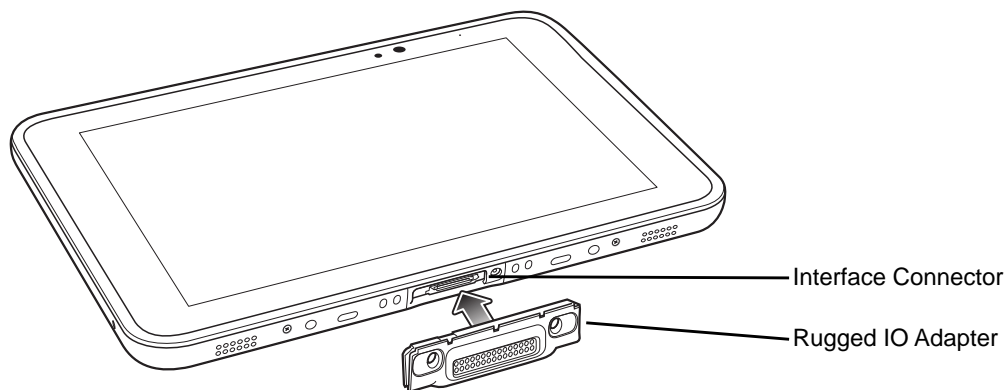


Figure 2-29 *Insert Rugged IO Adapter*

4. Remove the Rugged Frame and screws from box.
5. Separate the top and bottom sections of the Rugged Frame.
6. Place the bottom section on a flat surface.

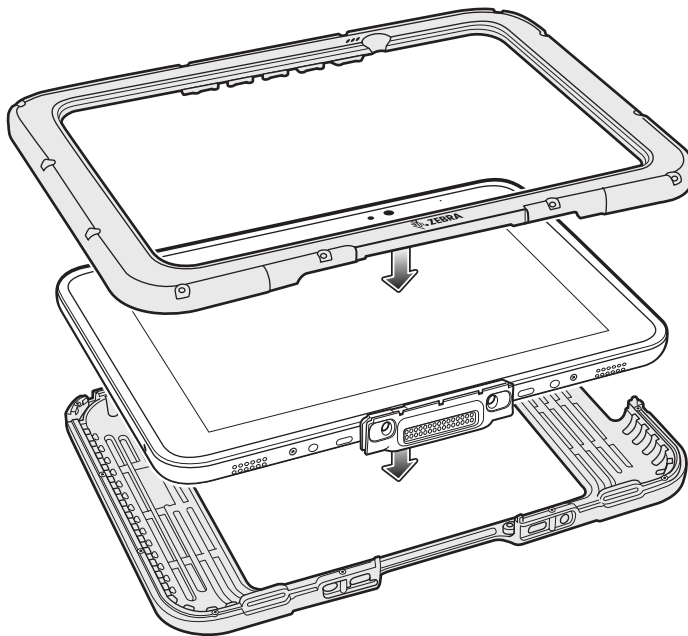


Figure 2-30 *Protective Boot Assembly*

7. Place the ET5X into the bottom section.
8. Align the top section over the bottom section.
9. Press the top section down onto the bottom section.
10. Using a T6 Torx screwdriver, secure the Rugged Frame together using the provided M1.6 Torx screws.

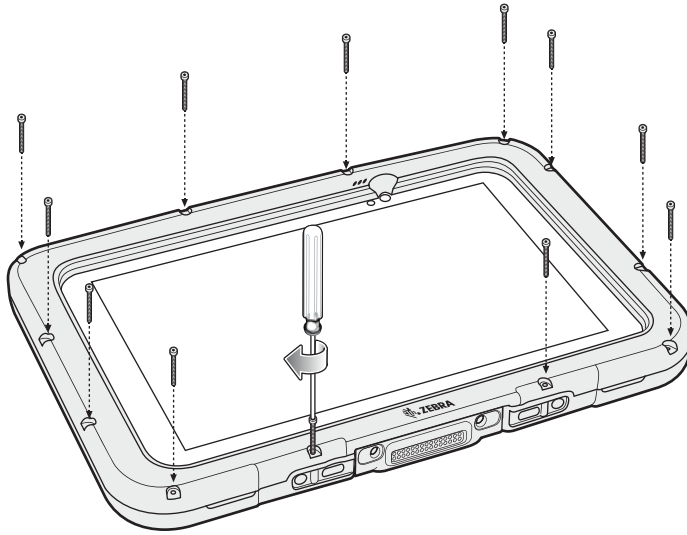


Figure 2-31 *Secure 8" Rugged Frame*

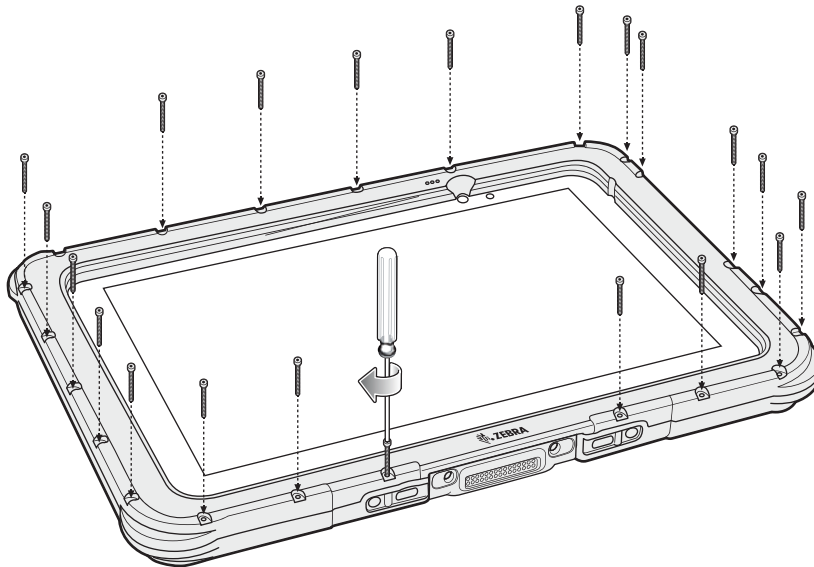


Figure 2-32 *Secure 10" Rugged Frame*

11. Torque the screws to 12 N-cm.

Expansion Back

The Expansion Backs provide data capture and or Power Pack slot for the ET5X.

Installation

To install an Expansion back:

1. Remove battery cover and store in safe place.

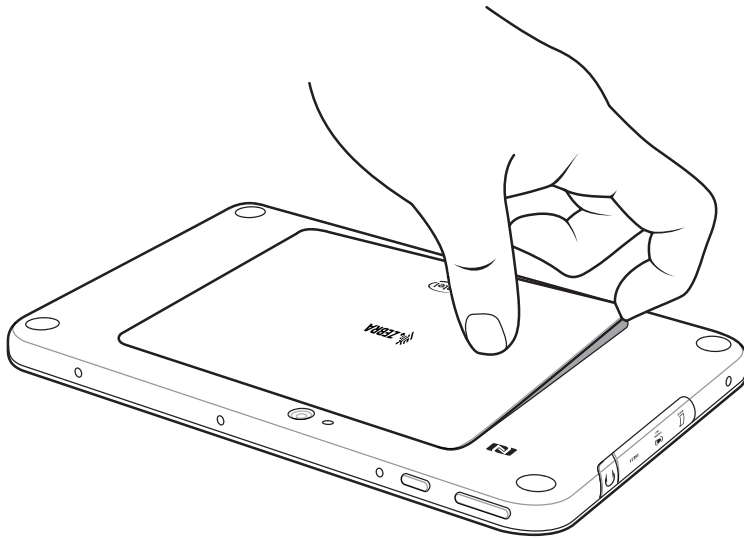


Figure 2-33 *Remove Battery Cover*

2. On 8" version only, remove rubber gasket.

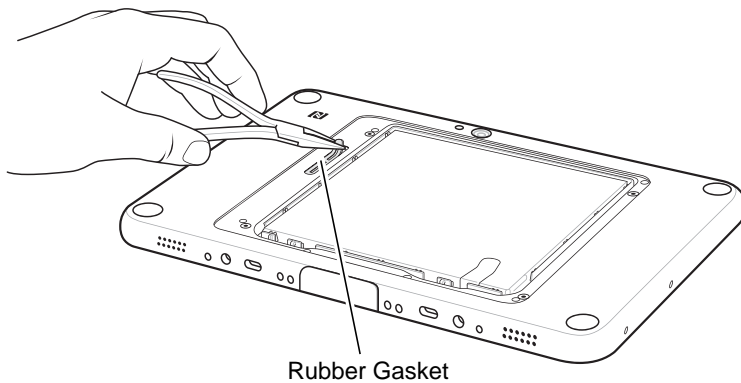


Figure 2-34 *Remove Rubber Gasket*

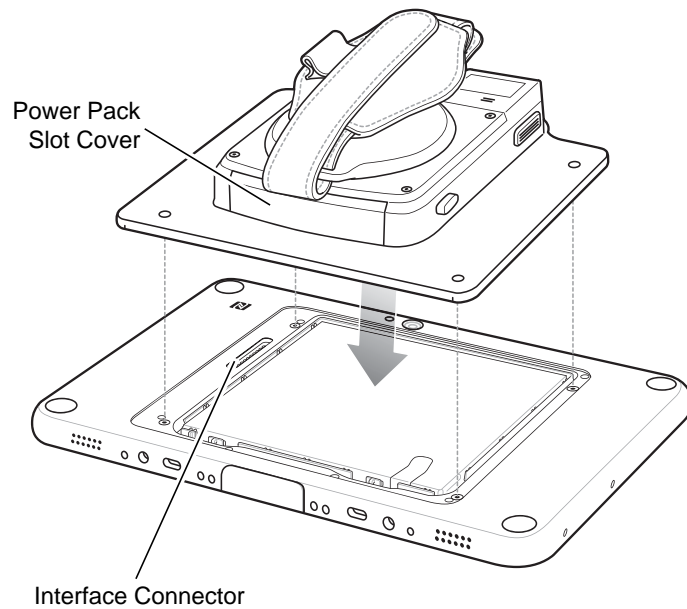


Figure 2-35 *Align Expansion Back with 8" Configuration*

3. Align expansion back with device. Ensure that the power pack slot cover is aligned with the bottom of the device and the interface connector on expansion back aligns with interface connector on device.

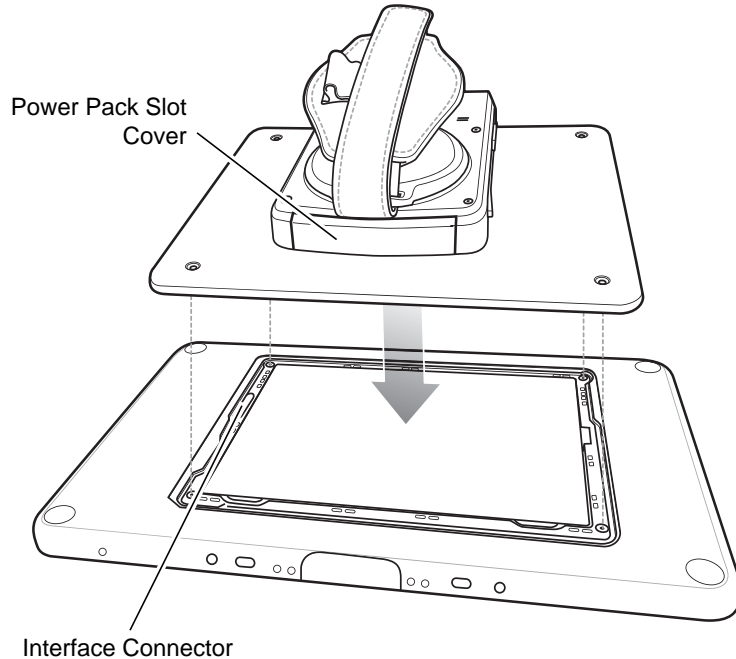


Figure 2-36 *Align Expansion Back with 8" Configuration*

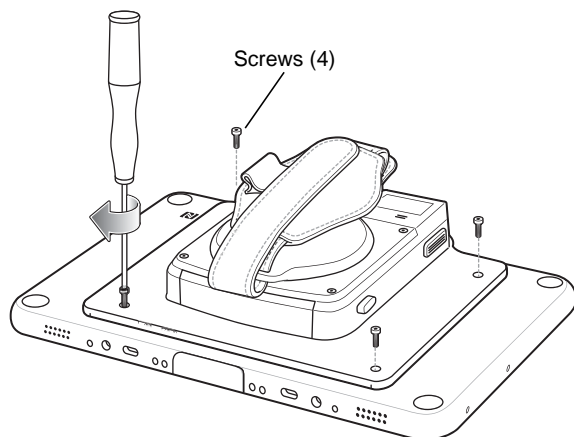


Figure 2-37 *Secure Screws*

4. Using a T6 Torx screwdriver, secure expansion back to device using four screws. Torque to 14 n-cm.

Configuring the SE4750 Expansion Backs

Use only the 8" SE4750 Expansion Back (ZBK-ET5X-8SCN5-02) or 10" SE4750 Expansions Back (ZBK-ET5X-10SCN5-02) with the ET5X running the Android operating system. If using SE4750 Expansion Back (ZBK-ET5X-8SCN5-01 or ZBK-ET5X-10SCN5-01) convert the Expansion Back for use with the ET5X running Android. See conversion procedures below.

Expansion Back Conversion Procedures

The 8" SE4750 Expansion Back (ZBK-ET5X-8SCN5-01) or 10" SE4750 Expansions Back (ZBK-ET5X-10SCN5-01) cannot be used with the ET5X running Android operating system. If using SE4750 Expansion Back (ZBK-ET5X-8SCN5-01 or ZBK-ET5X-10SCN5-01) convert the Expansion Back for use with the ET5X running Android.

1. Install the Expansion Back onto the tablet.
2. Ensure that the ET5X has the latest Android operating system version.
3. Ensure that the battery charge level is greater than 30%.
4. Check if the Expansion Back scanner is in SSI Mode.
 - a. Open the **DataWedge** application.
 - b. Touch **⋮** > **About**.
 - c. Check if the **Scanner Firmware** information displays.
 - d. Open the **DWDemo** application.
 - e. Try to scan a bar code using soft-key on the **DWDemo** application.



NOTE The Trigger button on the Expansion Back [Hard key] might not work to scan because the Expansion Back scanner may not have the latest scanner firmware.

- f. If the scanner firmware version displays and the bar code is scanned successfully, the scanner is in SSI mode.

5. If the Expansion Back scanner is in SSI Mode and the firmware version in **DataWedge** application ends with PAABLC44-001-R00, the Expansion Back scanner is in SSI Mode and the scanner has the latest firmware.
6. If the Expansion Back scanner is already in SSI Mode and the scanner firmware version does not end with PAABLC44-001-R00, then proceed to step 12, otherwise continue to next step to convert the Expansion Back scanner to SSI Mode.
7. Scan the below bar code using the Expansion Back trigger button.



Figure 2-38 *Set Defaults*

8. Wait five seconds. You will hear a disconnect indication (2 short beeps) followed by a boot indication (3 beeps) from the Expansion Back.
9. Scan the below bar code using the Expansion Back trigger button.

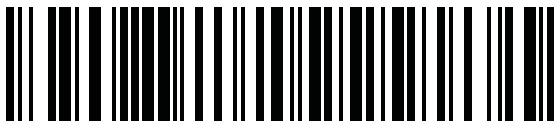



Figure 2-39 *SSI Over USB DCDC Bar Code*

10. Wait five seconds. You will hear a disconnect indication (2 short beeps) followed by a boot indication (3 beeps) from the Expansion Back.
11. Wait five seconds. The Expansion Back scanner should now be in SSI Mode.
12. Open **DataWedge** application.
13. Touch  > **About**.
14. Check the Scanner Firmware version. The firmware version should be PAABLC44-001-R00.
15. Once the scanner is in SSI mode, reboot the ET5X.
 - a. Press the Power button until the menu appears.
 - b. Touch **Power Off**.
 - c. Wait for the ET5X to turn off.
 - d. Press the Power button to turn on the ET5X.



CAUTION After the ET5X turns on, do not suspend or reboot the device using the Power button as this would stop the firmware update process. Unlock the screen by swiping the lock screen up.

16. The firmware update occurs as a background process and takes approximately five minutes. Do not open **DataWedge** or **DWDemo** applications during this time.
17. After the update is completed successfully you would hear bootup indication (3 beeps) from the Expansion Back.
18. Wait 15 seconds.
19. Open the **DataWedge** application.

20. Touch **⋮** > **About**.
21. The Scanner Firmware version displays PAABLC44-001-R00.
The Expansion Back is ready for normal use.

Replacement Hand Strap

To replace the hand strap:

1. If the Power Pack is installed, remove the Power Pack.
2. Rotate the disk so that the strap end without the eyelet is aligned with the Power Pack opening.
3. Open both ends of the hand strap.

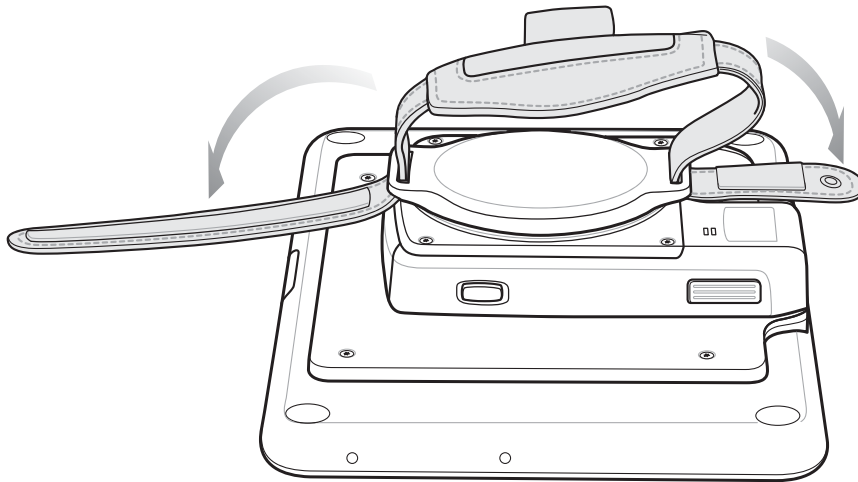


Figure 2-40 *Open Straps*

4. Pull the strap end without the eyelet through the slot on the Expansion Back.

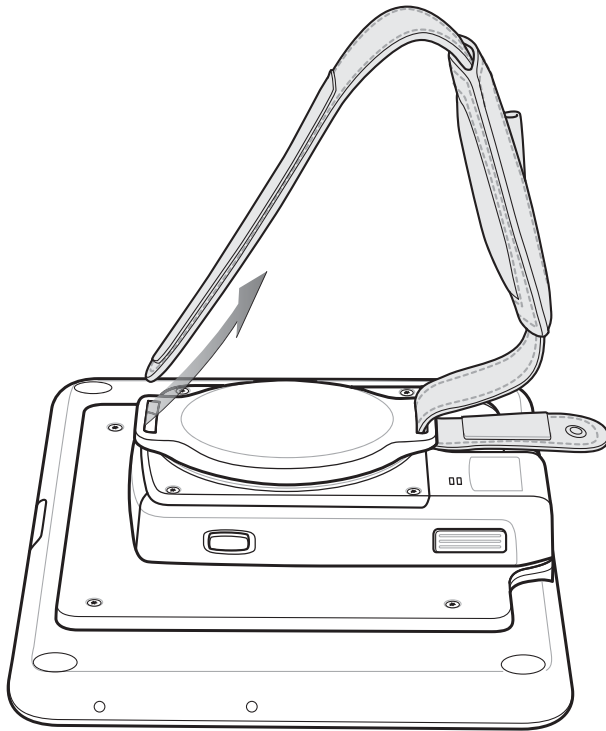


Figure 2-41 *Remove Strap*

5. Rotate the disk 180°.
6. Slide the pad off the hand strap.
7. Pull the eyelet end through the slot on the Expansion Back.

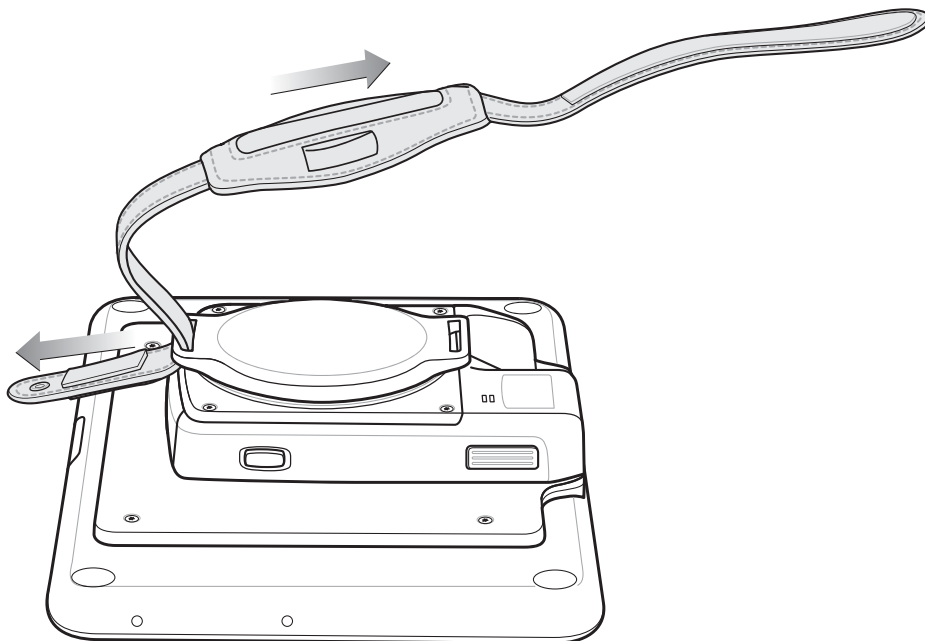


Figure 2-42 *Pull Eyelet End*

8. Remove pad from new replacement hand strap.

9. Rotate the disk so that one of the slots is aligned with the Power Pack opening.
10. Feed the new hand strap through the slot at the Power Pack opening.

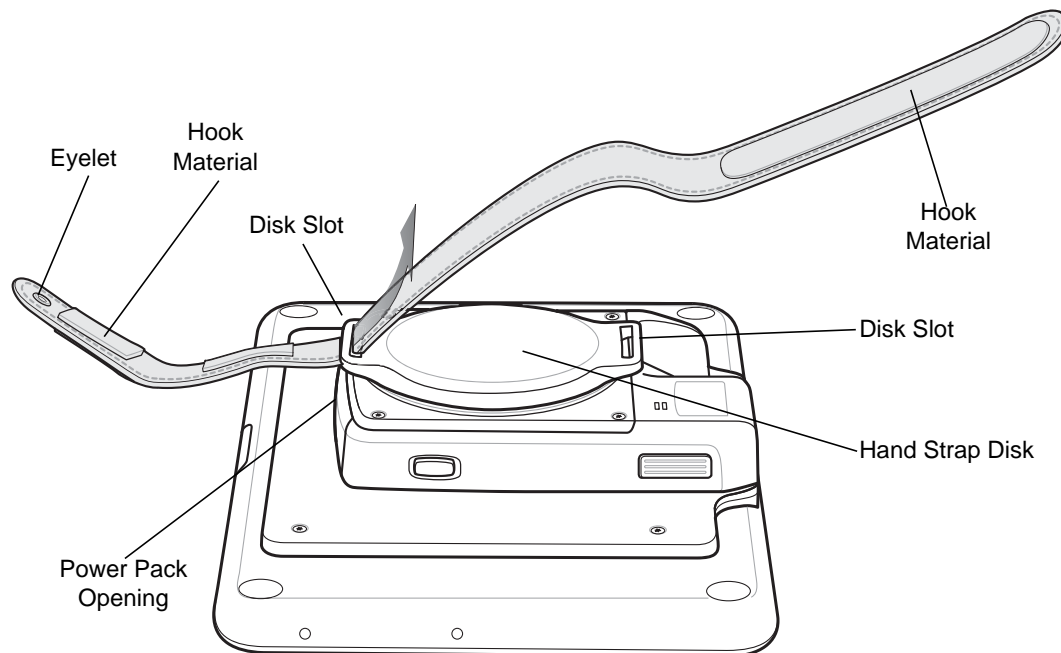


Figure 2-43 *Feed New Strap*

11. Slide pad onto hand strap with the stylus holder facing up.
12. Fold the eyelet end of the strap up and press hook and loop material together.

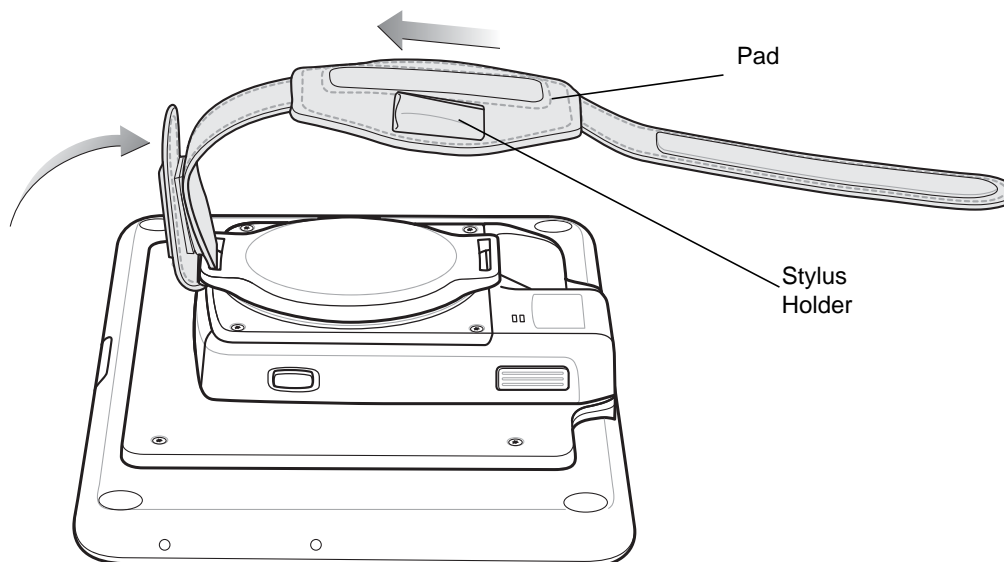


Figure 2-44 *Secure Eyelet End*

13. Rotate disk 180° so that the empty slot is aligned with the Power Pack opening.
14. Feed strap through the slot.

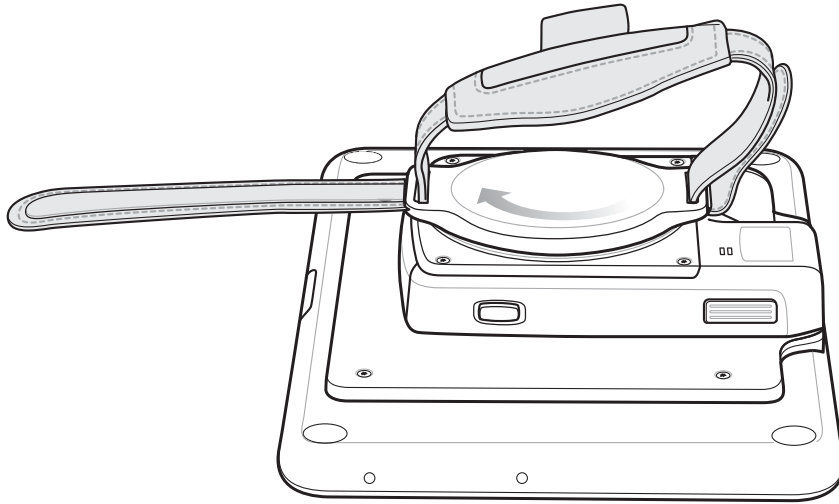


Figure 2-45 *Feed Strap*

15. Fold the end of the strap up and press hook and loop material together.

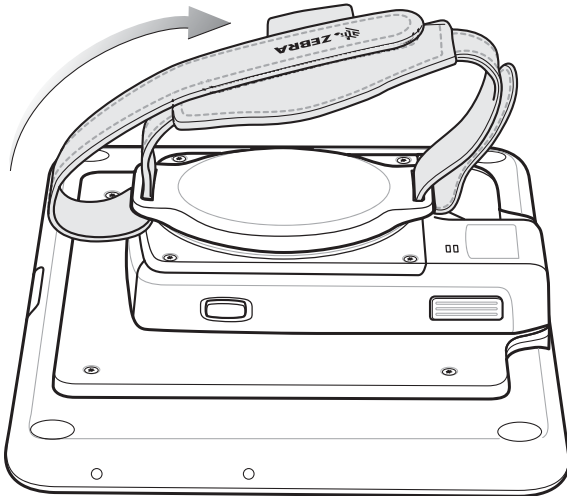


Figure 2-46 *Secure Strap*

Attaching the Stylus to the Expansion Back

The Expansion Backs provide a holder for the stylus. To install the stylus onto the Expansion Back with the option tether:

1. Insert one loop of the tether into the hole in the stylus end cap.

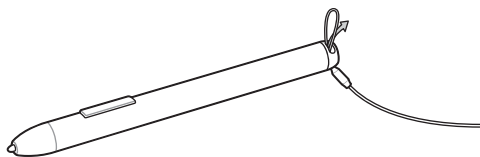


Figure 2-47 *Insert Loop*

2. Feed the other end of the tether through the loop.

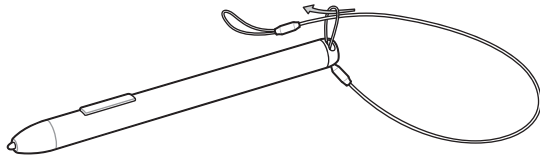


Figure 2-48 *Feed Tether Through Loop*

3. Pull the tether all the way through the loop.
4. Insert the loop of the tether through the eyelet on the hand strap of the Expansion Back.
5. Feed the stylus through the loop.

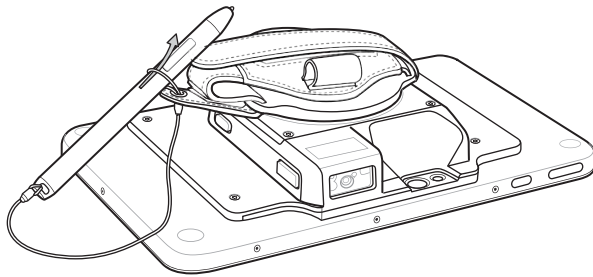


Figure 2-49 *Feed Stylus through Loop*

6. Pull the stylus all the way through the loop.
7. Slide the stylus into the holder for storing the stylus.

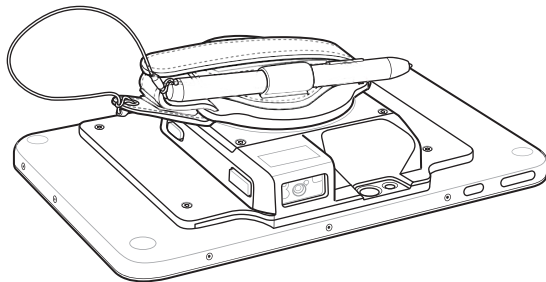


Figure 2-50 *Insert Stylus into Holder*

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 ET5X to a host computer using a USB cable to transfer files between the ET5X and the host computer.



CAUTION When connecting the ET5X 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 ET5X as a Media Device

1. Connect the USB cable to the ET5X and then to the host computer.
2. On the host computer, open a file explorer application.
3. Locate the **ET5X** as a portable device.
4. Open the **Internal storage** folder.
5. Copy or delete files 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.

6. On the host computer, unmount the device.
7. Remove the USB 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 ET5X 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
- data capture plus configurations
- Input plug-in configurations
- Output plug-in configurations
- Process plug-in configurations.

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

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

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

- **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.

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

Profile0

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

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

Plug-ins

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

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

Input Plug-ins

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

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

Process Plug-ins

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

- **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.

- **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.

Output Plug-ins

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

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

Profiles Screen

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

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

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

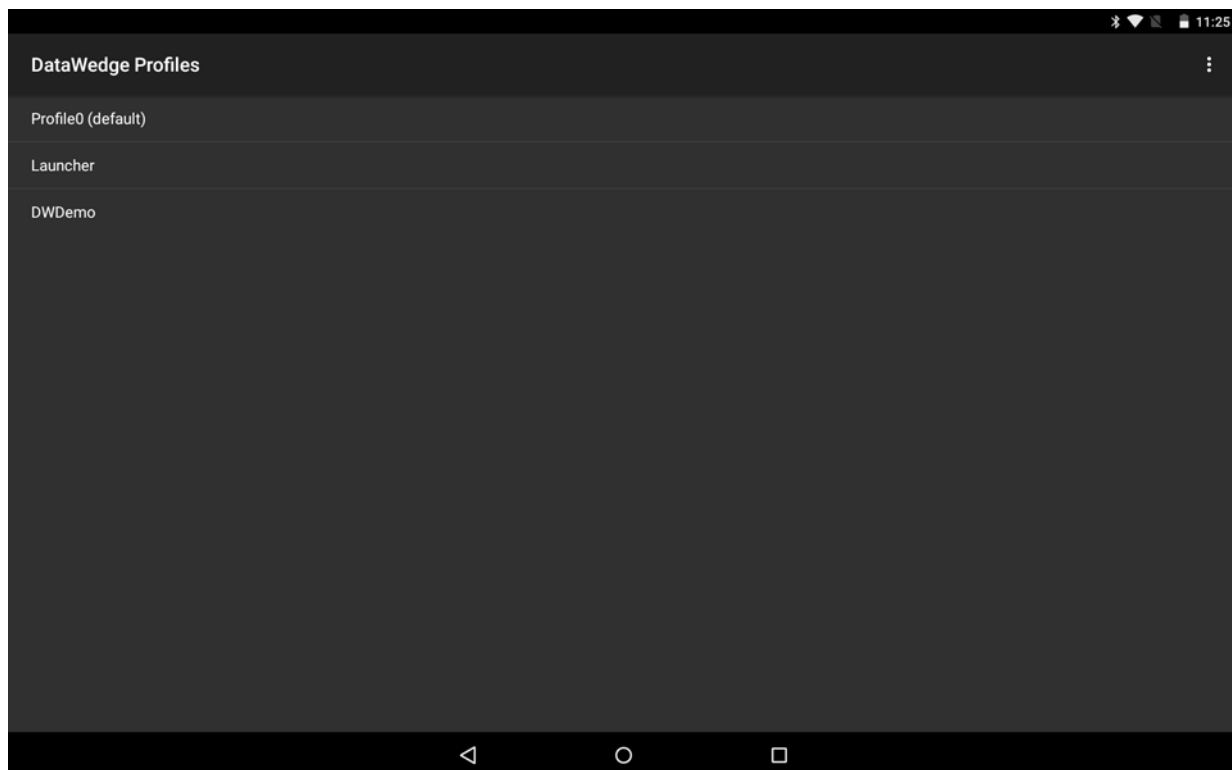


Figure 4-1 *DataWedge Profiles Screen*

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.

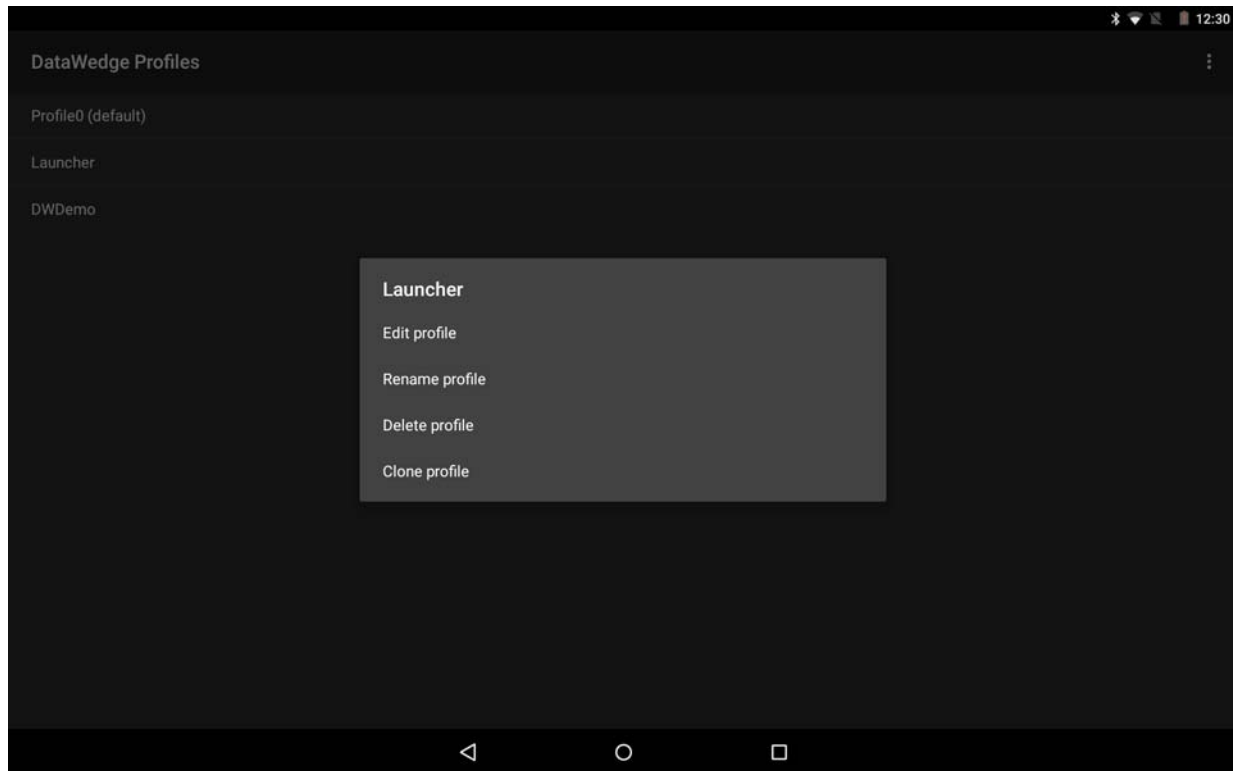



Figure 4-2 *Profile Context Menu*

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.

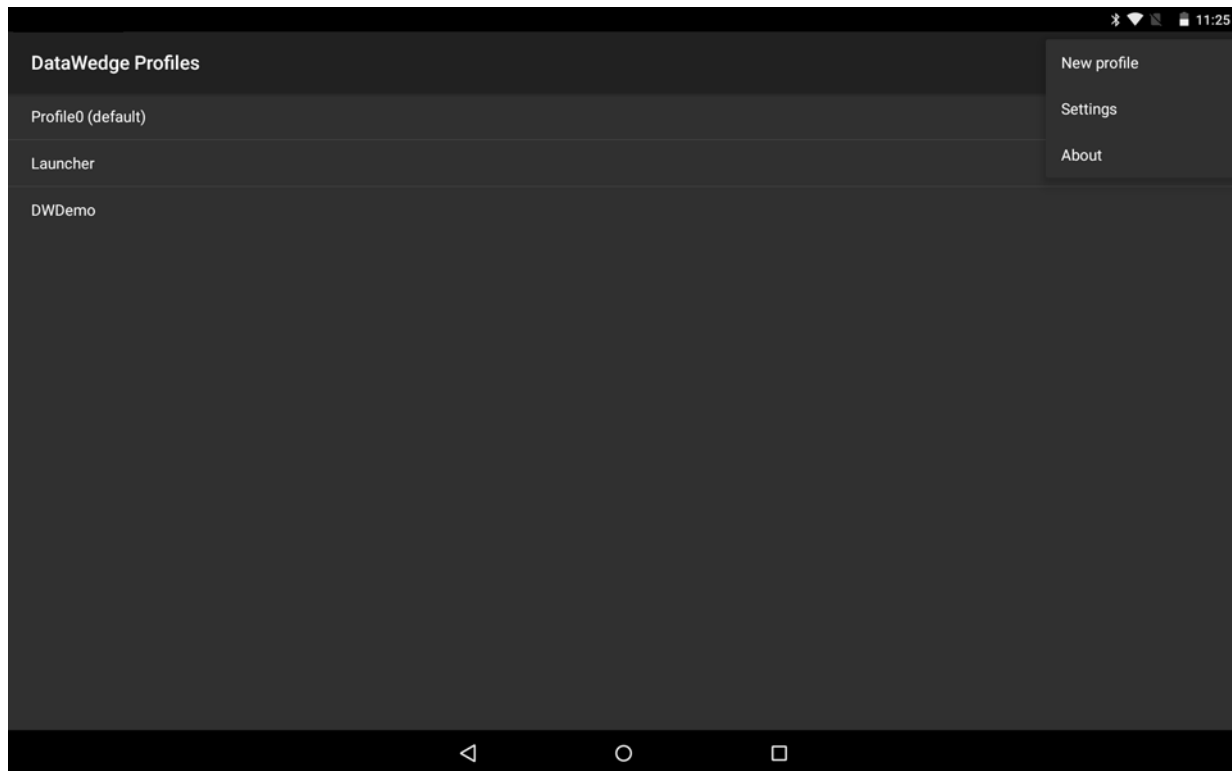





Figure 4-3 *DataWedge Options Menu*




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).

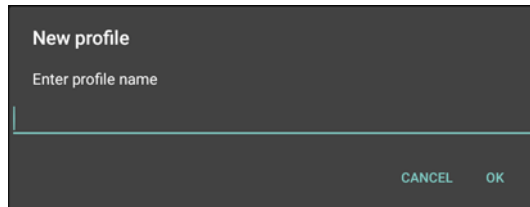


Figure 4-4 *New Profile Name Dialog Box*

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.

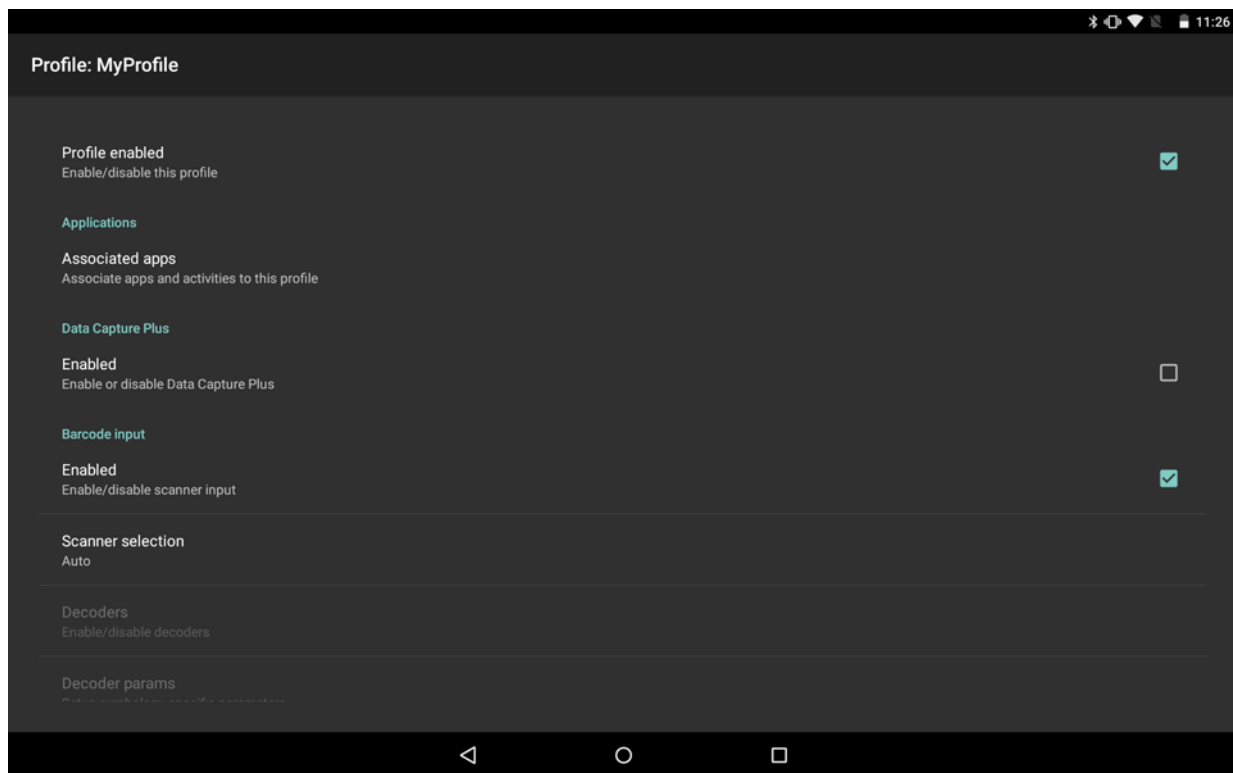


Figure 4-5 *Profile Configuration Screen*

The configuration screen lists the following sections:

- Profile enabled
- Applications
- Data Capture Plus (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.

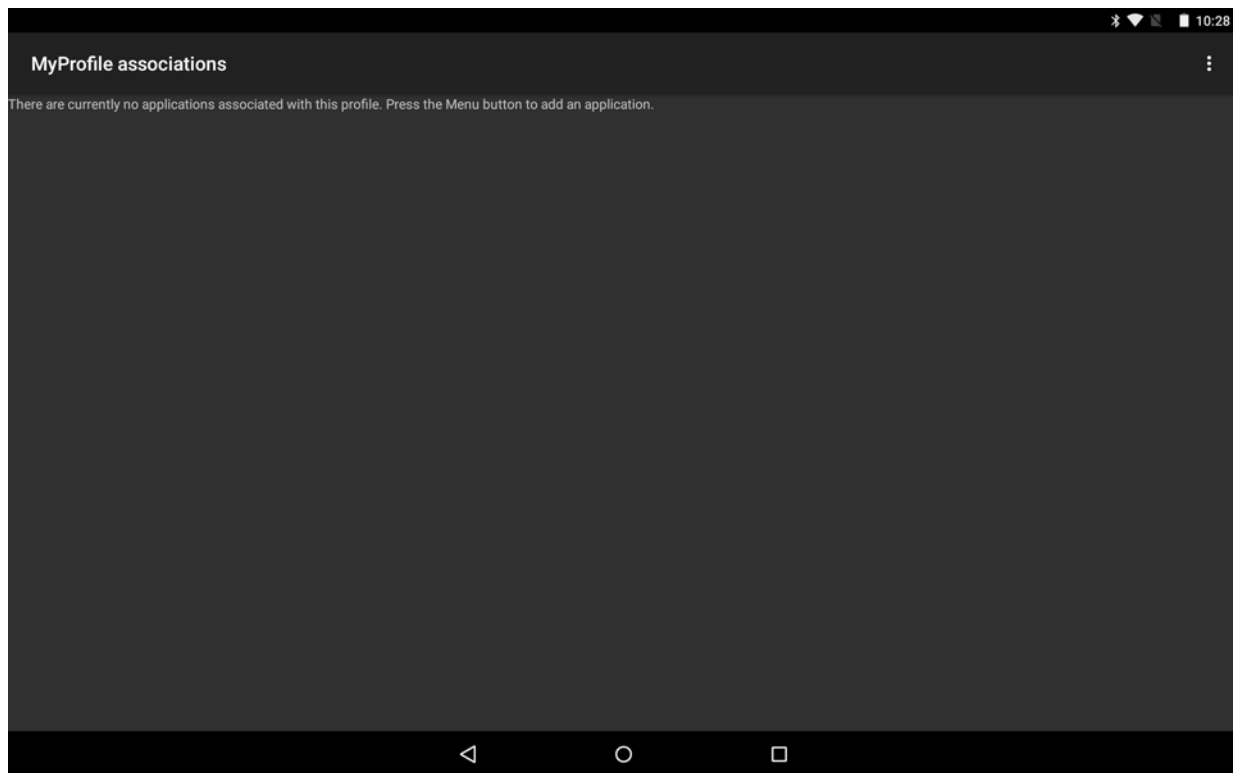


Figure 4-6 *Associated Apps Screen*

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

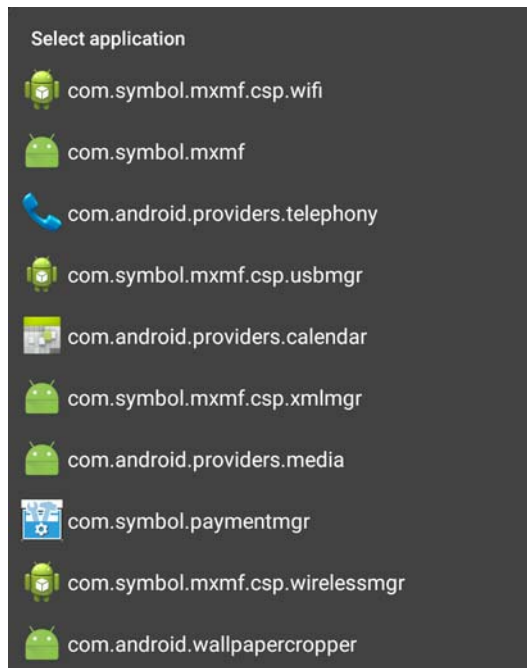


Figure 4-7

Figure 4-8 *Select Application Menu*

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

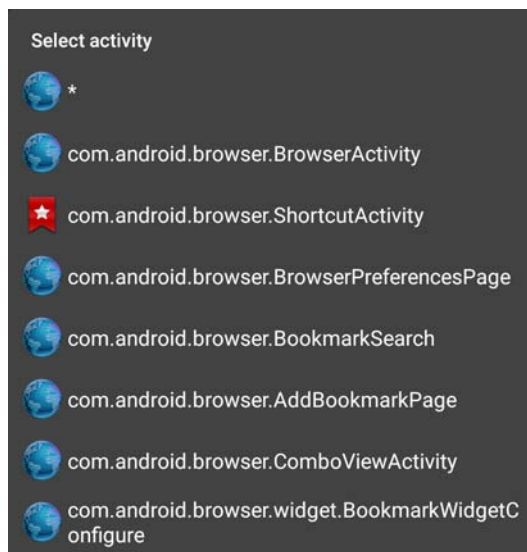



Figure 4-9 *Select Activity Menu*

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 .

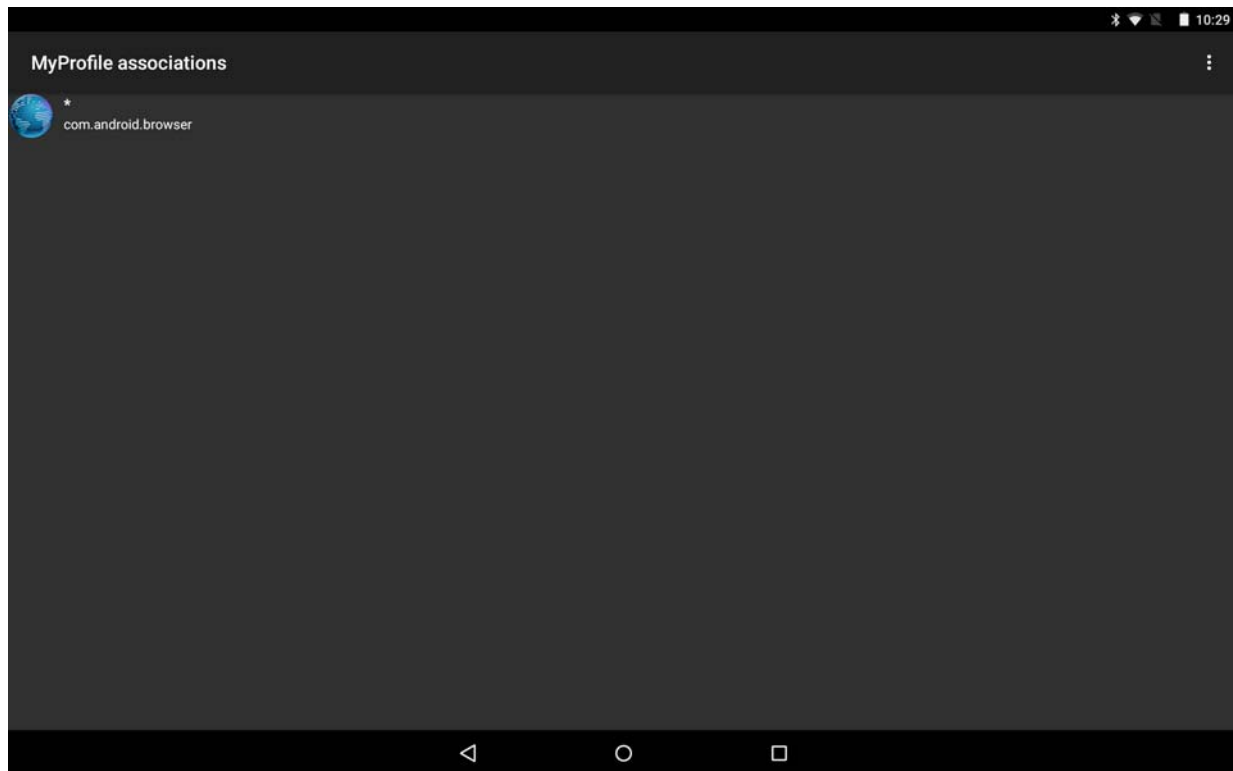


Figure 4-10 *Selected Application/Activity*

Data Capture Plus

The Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching an area on the screen. A button or screen overlay acts like a scan button.

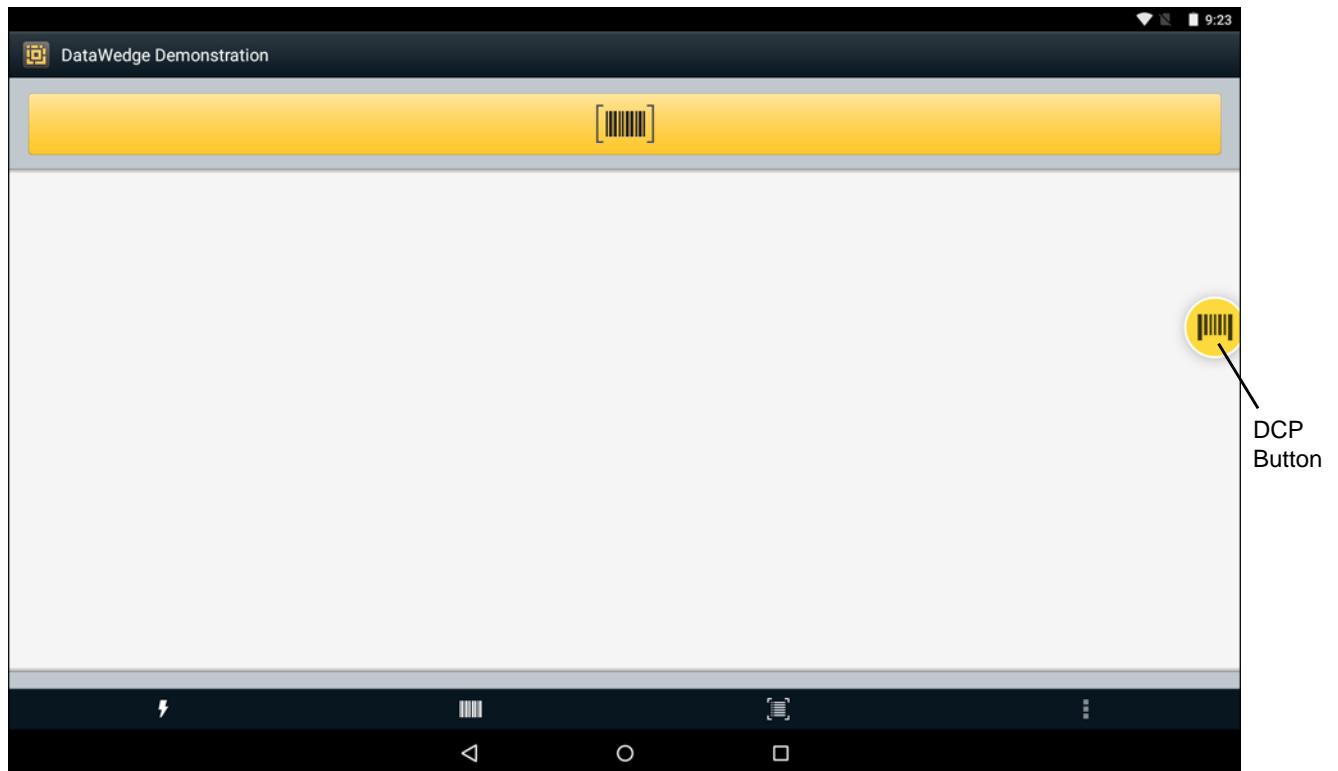


Figure 4-11 *Data Capture Plus Dock Button*

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 additional configuration parameters.

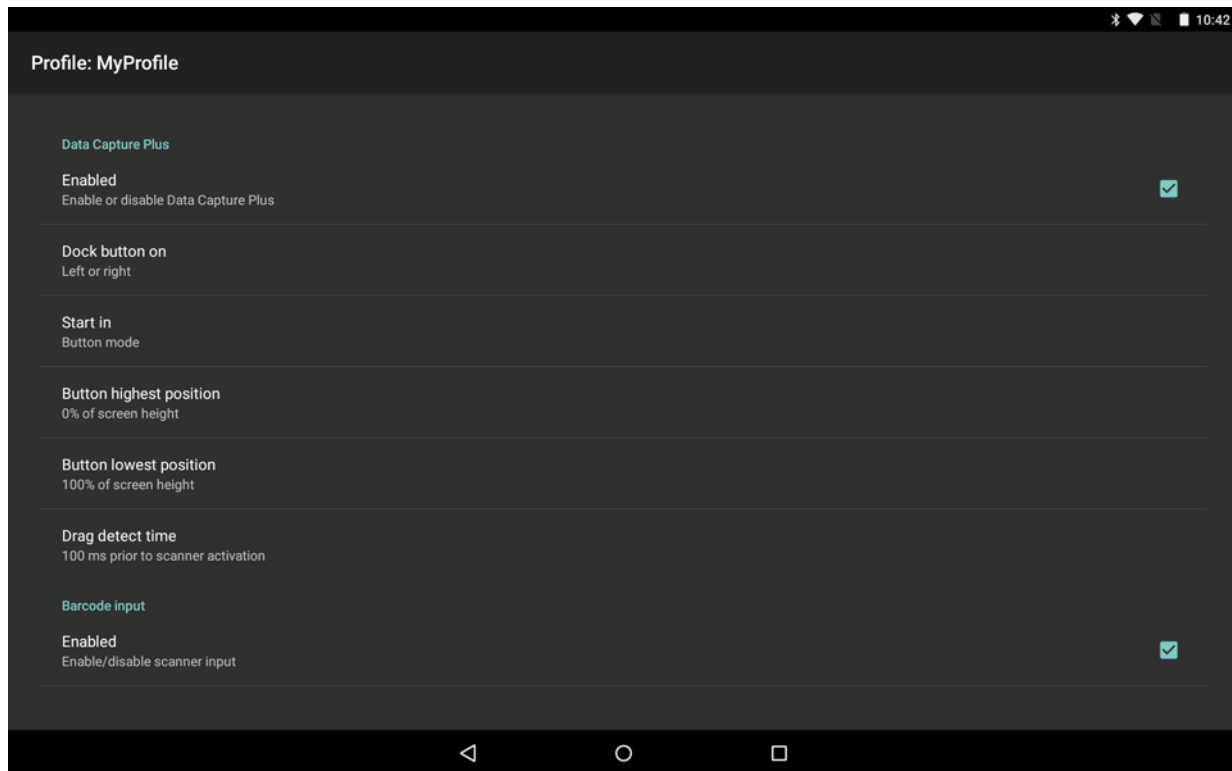


Figure 4-12 *Data Capture Plus Settings*

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



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

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

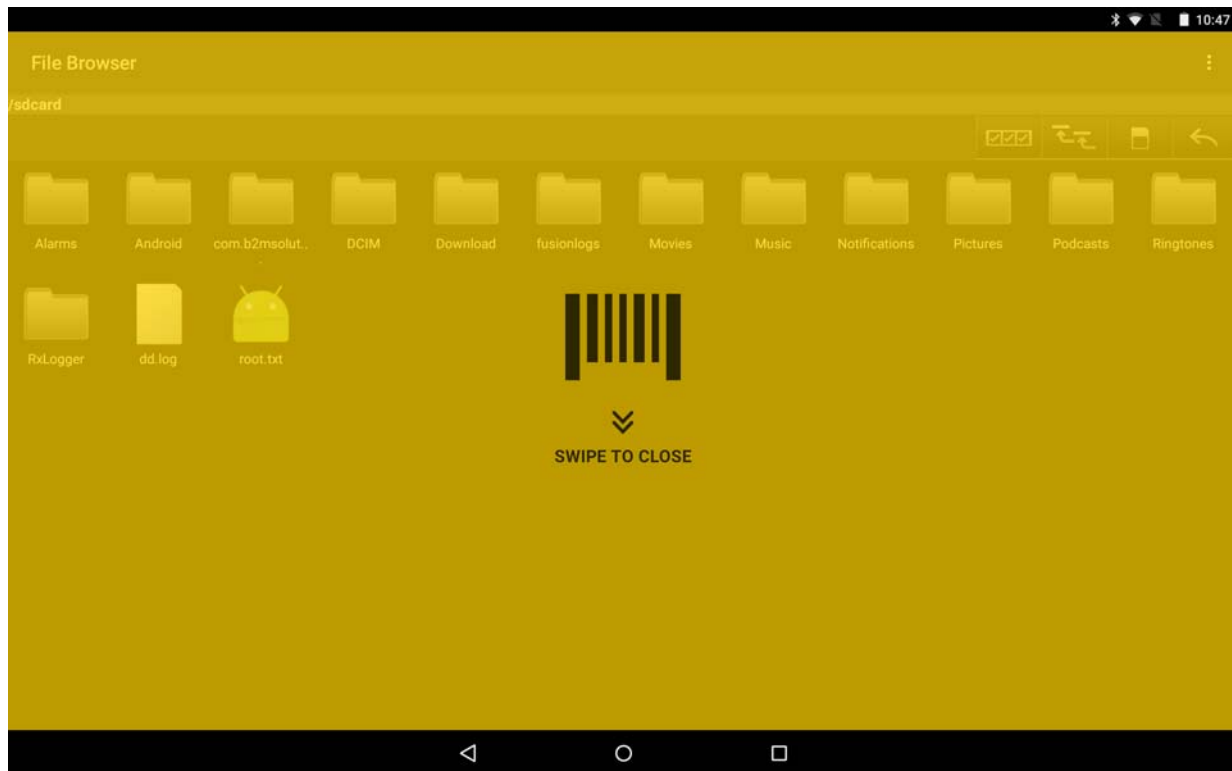


Figure 4-13 *Fullscreen Mode*

Swipe down to return to button mode.

Bar Code Input

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

Enabled

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

Scanner Selection

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

- **Auto** - The software automatically selects the best scanner.
- **Pluggable Serial SSI Scanner** - Scanning is performed using the Expansion Back.

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.

Table 4-1 *Supported Decoders*

Symbology	SE4750 Expansion Back Default
Australian Postal	Disabled
Aztec	Enabled
Canadian Postal	Disabled
Chinese 2 of 5	Disabled
Codabar	Enabled
Code 11	Disabled
Code 128	Enabled
Code 39	Enabled
Code 93	Disabled
Composite AB	Disabled
Composite C	Disabled
Discrete 2 of 5	Disabled
Datamatrix	Enabled
Decoder Signature	Disabled
Dutch Postal	Disabled
EAN13	Enabled
EAN8	Enabled
GS1 DataBar	Enabled
GS1 DataBar Expanded	Enabled
GS1 DataBar Limited	Disabled
HAN XIN	Disabled
Interleaved 2 of 5	Disabled
Japanese Postal	Disabled
Korean 2 of 5	Disabled
Matrix 2 of 5	Disabled
Maxicode	Enabled
MicroPDF	Disabled

Table 4-1 *Supported Decoders (Continued)*

Symbology	SE4750 Expansion Back Default
MicroQR	Disabled
MSI	Disabled
PDF417	Enabled
QRCode	Enabled
TLC39	Disabled
Trioptic 39	Disabled
UK Postal	Disabled
UPCA	Enabled
UPCE0	Enabled
UPCE1	Disabled
US4state	Disabled
US4state FICS	Disabled
US Planet	Disabled
US Postnet	Disabled

Decoder Params

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

Codabar

- **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 4-19* 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).
- **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 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).

- **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code.
 - **No Check Digit** - Do not verify check digit.
 - **1 Check Digit** - Bar code contains one check digit (default).
 - **2 Check Digits** - Bar code contains two check digits.

Code128

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 bar codes.
- **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.
- **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:
 - **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
 - **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
 - **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.
 - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
 - **Security Level 1** - This setting eliminates most misdecodes (default).
 - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
 - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.

Code39

- **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 bar codes.

- **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
- **Full ASCII** - Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled).
- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
- **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character "A" to all Code 32 bar codes (default - disabled).
- **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).
 - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" bar codes.
 - **Security Level 1** - This setting eliminates most misdecodes (default).
 - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
 - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the bar codes.
- **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).

Code93

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

Composite AB

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

Discrete 2 of 5

- **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 4-19* for more information.

- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

GS1 DataBar Limited

- **GS1 Limited Security Level**
 - **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.

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.

Interleaved 2 of 5

- **Check Digit**
 - **No Check Digit** - A check digit is not used. (default)
 - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
 - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
- **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).
- **I2of5 Security Level** - Options: **I2of5 Security level 0**, **I2of5 Security Level 1**, **I2of5 Security Level 2** and **I2of5 Security Level 3** (default - I2of5 Security level 1).
- **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
- **I2of5 Reduced Quiet Zone** - Enables decoding of margin-less I2of5 bar codes.

Matrix 2 of 5

- **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 4-19* for more information.
- **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

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

MSI

- **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
 - **One Check Digit** - Verify one check digit (default).
 - **Two Check Digits** - Verify two check digits.
- **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
 - **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
 - **Mod-10-10** - Both check digits are MOD 10.
- **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 4-19* for more information.
- **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 4-19* for more information.
- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).

Trioptic 39

- **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

UK Postal

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

UPCA

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

There are three options for transmitting a UPCA preamble:

 - **Preamble None** - Transmit no preamble.
 - **Preamble Sys Char** - Transmit System Character only (default).
 - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA). Select the appropriate option to match the host system.
- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - enabled).

UPCE0

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

- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.
There are three options for transmitting a UPCE0 preamble:
 - **Preamble Sys Char** - Transmit System Character only.
 - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
 - **Preamble None** - Transmit no preamble (default).
- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

UPCE1

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

US Planet

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

Decode Lengths

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

UPC EAN Params

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

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled.
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC bar codes.
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **Bookland Format** - If Bookland EAN is enabled, select one of the following formats for Bookland data:
 - **Format ISBN-10** - The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
 - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled.
- **Coupon 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.
- **Linear Decode** - This option applies to code types containing two adjacent blocks (e.g., UPC-A, EAN-8, EAN-13). Enable this parameter to transmit a bar code only when both the left and right blocks are successfully decoded within one laser scan. Enable this option when bar codes are in proximity to each other.
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto, Supplementals Smart, Supplementals 378-379, Supplementals 978-979, Supplementals 977 or Supplementals 414-419-434-439** (2 to 20, default 10).
- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
 - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding “in-spec” UPC/EAN bar codes (default).
 - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
 - **Level 2** - If the scanner is misdecoding poorly printed bar codes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
 - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec bar codes. Selecting this level of security

can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.

- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
 - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
 - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
 - **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.

Reader Params

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

- **1D Quiet Zone Level** - Sets the level of aggressiveness in decoding bar codes with a reduced quiet zone (the area in front of and at the end of a bar code), and applies to symbologies enabled by a Reduced Quiet Zone parameter. Because higher levels increase the decoding time and risk of misdecodes, Zebra strongly recommends enabling only the symbologies which require higher quiet zone levels, and leaving Reduced Quiet Zone disabled for all other symbologies. Options are:
 - **0** - The scanner performs normally in terms of quiet zone.
 - **1** - The scanner performs more aggressively in terms of quiet zone (default).
 - **2** - The scanner only requires one side EB (end of bar code) for decoding.
 - **3** - The scanner decodes anything in terms of quiet zone or end of bar code.

- **Aim mode** - Turns the scanner cross-hairs on or off.
 - **On** - Cross-hair is on (default).
 - **Off** - Cross-hair is off.
- **Character Set Selection**
 - **ISO-8859-1** - part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
 - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
 - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
- **Time Delay to Low Power** - Sets the time the decoder remains active after decoding. After a scan session, the decoder waits this amount of time before entering Low Power Mode. Options: **1 Second** (default), **30 Seconds**, **1 Minute** or **5 Minutes**.
- **Illumination mode** - Turns imager illumination on and off. This option is only available when **Bluetooth Scanner** is selected in the **Barcode input, Scanner selection** option.
 - **On** - Illumination is on.
 - **Off** - Illumination is off (default).
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D bar codes.
 - **Disable** - Disables decoding of inverse 1D bar codes (default).
 - **Enable** - Enables decoding of only inverse 1D bar codes.
 - **Auto** - Allows decoding of both twice positive and inverse 1D bar codes.
- **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.
- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.
 - **Disabled** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
 - **Enabled** – Enables Picklist mode so that only the bar code under the projected reticle can be decoded.
- **Aim Timer** - Sets the maximum amount of time that aiming remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the aim to stay on indefinitely (default - 500).
- **Aim Type** - Set the aiming usage.
 - **Trigger** - A trigger event activates decode processing, which continues until the trigger event ends or a valid decode occurs.
 - **Timed Hold** - A trigger pull and hold activates the laser for aiming, which continues until the trigger is released, a valid decode, or the decode session time-out is expired.
 - **Timed Release** - A trigger pull activates the laser for aiming, which continues until a valid decode or the remaining decode session time has expired.
 - **Press and Release** - A trigger pull and release activates the laser for aiming, which continues until a trigger is pressed again, a valid decode, or the decode session time-out is expired.
 - **Continuous Read** - When the imager detects an object in its field of view, it triggers and attempt to decode.
- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -15000).

- **Different Symbol Timeout** - Controls the time the scanner is inactive between decoding different symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.
- **Same Symbol Timeout** - Controls the time the scanner is inactive between decoding same symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.

Scan Params

Allows the configuration of Code ID and decode feedback options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned bar code. This is useful when the reader is decoding more than one code type. Select a code ID character to insert between the prefix and the decoded symbol.
 - **Code ID Type None** - No prefix (default)
 - **Code ID Type AIM** - Insert AIM Character prefix.
 - **Code ID Type Symbol** - Insert Symbol character prefix.
- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Beep Volume Control** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.



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

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

Keystroke Output

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

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).
- **Action key character** - Enables decoding of a special character embedded within a bar code data for use in native Android applications. This feature is helpful when populating or executing a form.
 - **None** - Action key character feature is disabled (default).
 - **Tab** - Tab character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
 - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
 - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
- **Multi byte character display** - Set the amount of time (in milliseconds) of the inter character delay for multi byte characters. (default - 0.)

- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
 - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
 - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See *Generating Advanced Data Formatting Rules on page 4-29* 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 4-29* 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 4-29* 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**.

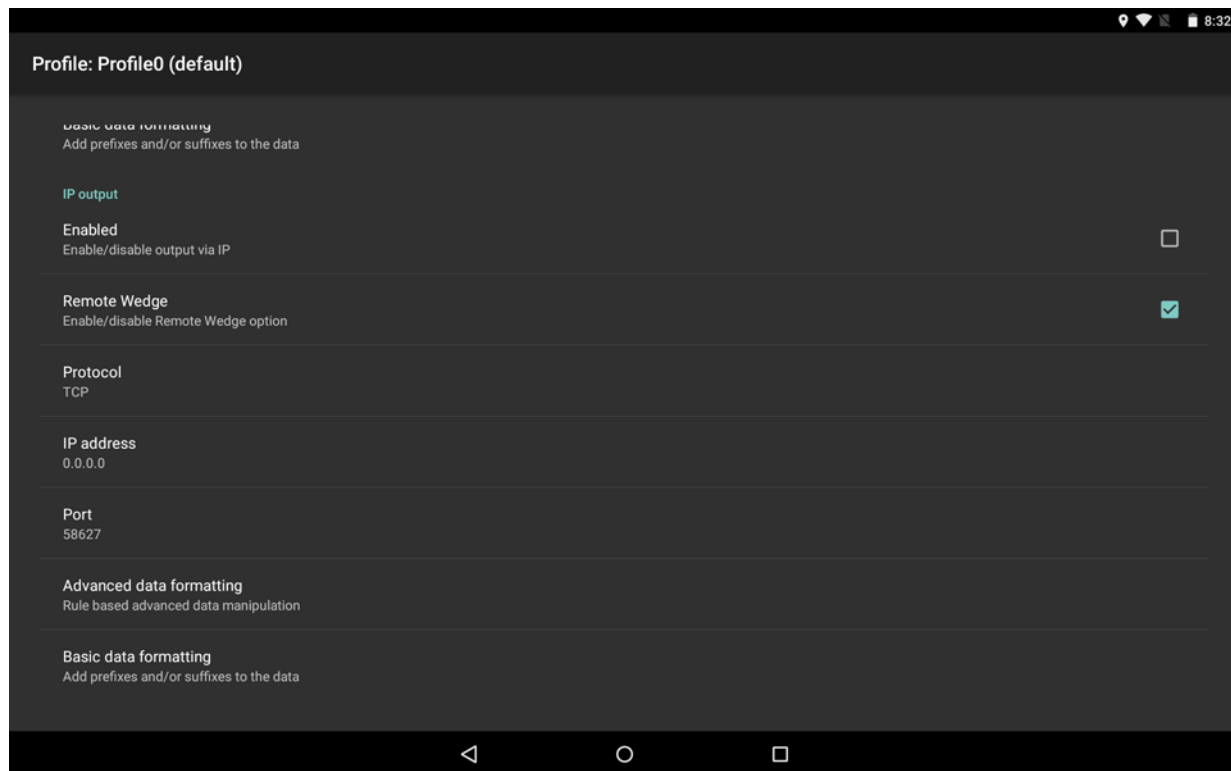


Figure 4-14 IP Output Screen

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).

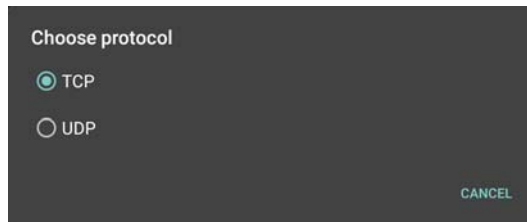


Figure 4-15 *Protocol Selection*

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

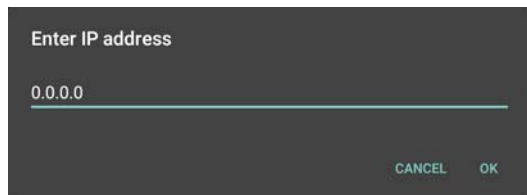


Figure 4-16 *IP Address Entry*

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

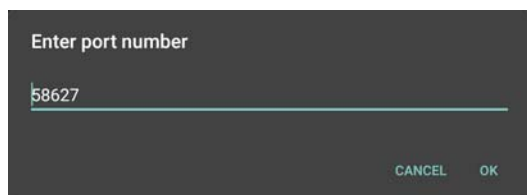


Figure 4-17 *Port Number Entry*

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).

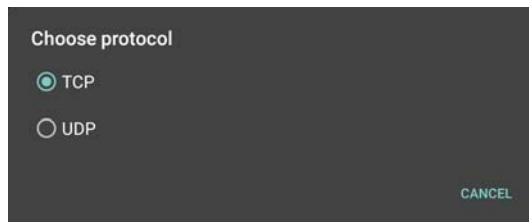


Figure 4-18 *Protocol Selection*

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

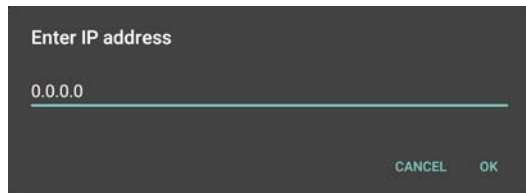


Figure 4-19 *IP Address Entry*

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

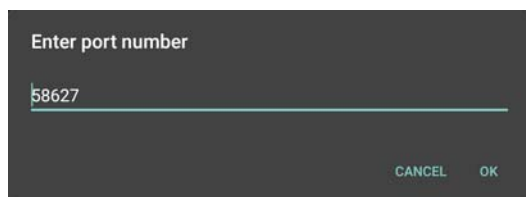


Figure 4-20 *Port Number Entry*

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**.

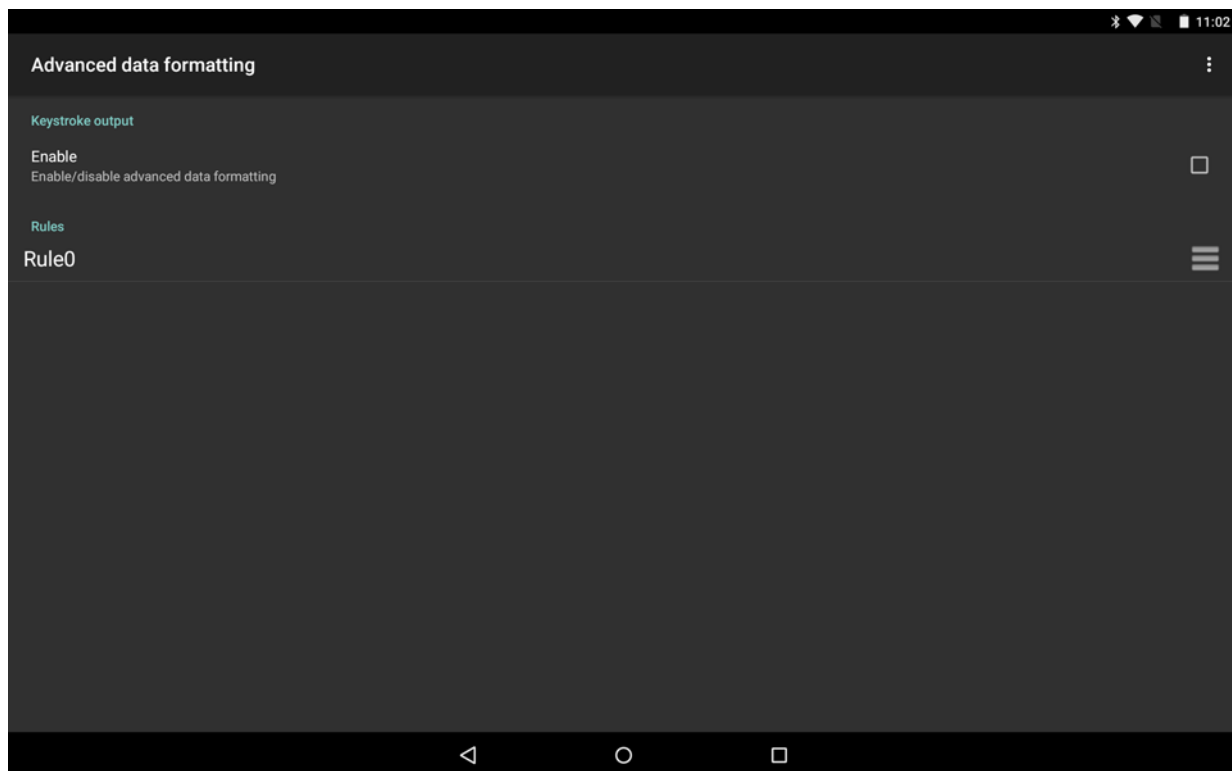



Figure 4-21 Advanced Data Formatting Screen

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 **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.

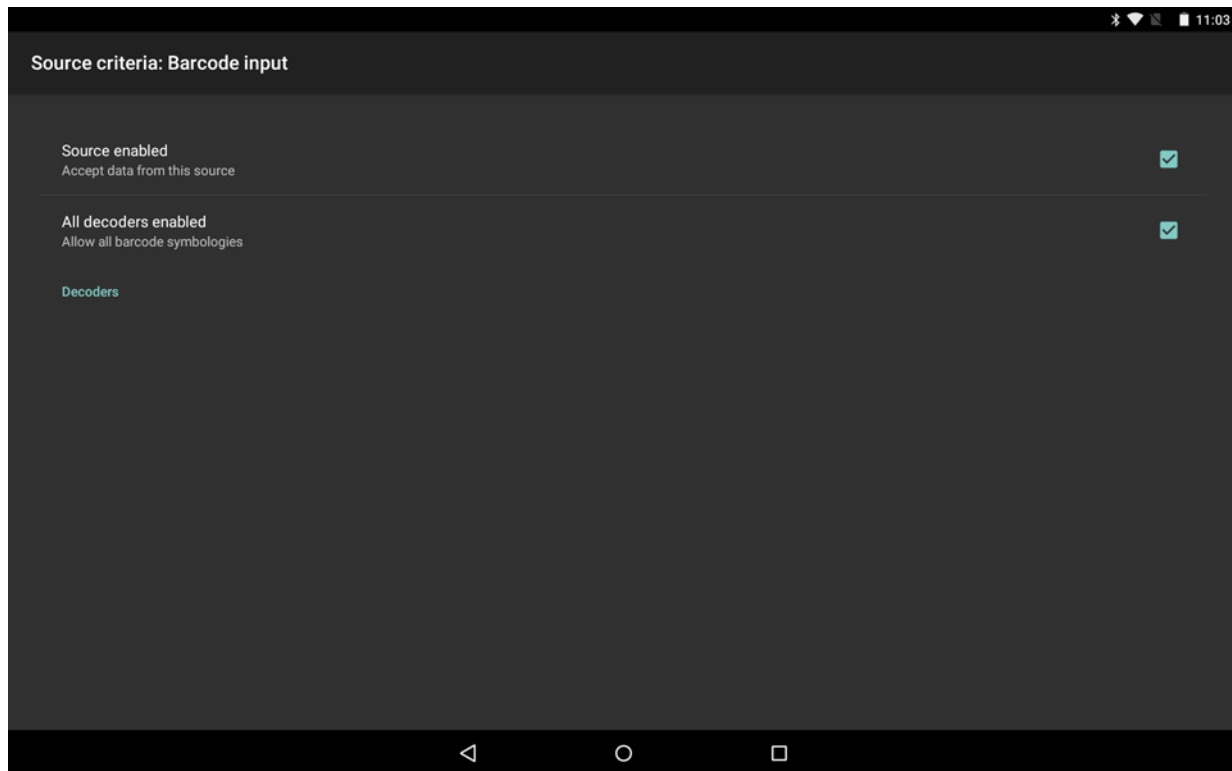







Figure 4-23 Barcode Input Screen

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 4-2 on page 4-33](#) 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 4-2 ADF Supported Actions

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

Table 4-2 ADF Supported Actions (Continued)

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

Deleting an Action

1. Touch and hold the action name.

2. Select **Delete action** from the context menu.

ADF Example

The following illustrates an example of creating Advanced Data Formatting:




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






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

Modify the data as follows:

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

To create an ADF rule for the above example:

1. Touch  > **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 **Actions**.
20. Touch and hold on the **Send remaining rule** until a menu appears.
21. Touch **Delete action**.
22. Touch .
23. Touch **New action**.
24. Select **Pad with zeros**.
25. Touch the **Pad with zeros** rule.

26. Touch **How many**.
27. Change value to 8 and then touch **OK**.
28. Touch .
29. Touch .
30. Touch **New action**.
31. Select **Send up to**.
32. Touch **Send up to** rule.
33. Touch **String**.
34. In the **Enter a string** text box, enter x.
35. Touch **OK**.
36. Touch .
37. Touch .
38. Touch **New action**.
39. Select **Send char**.
40. Touch **Send char** rule.
41. Touch **Character code**.
42. In the **Enter character code** text box, enter 32.
43. Touch **OK**.
44. Touch .

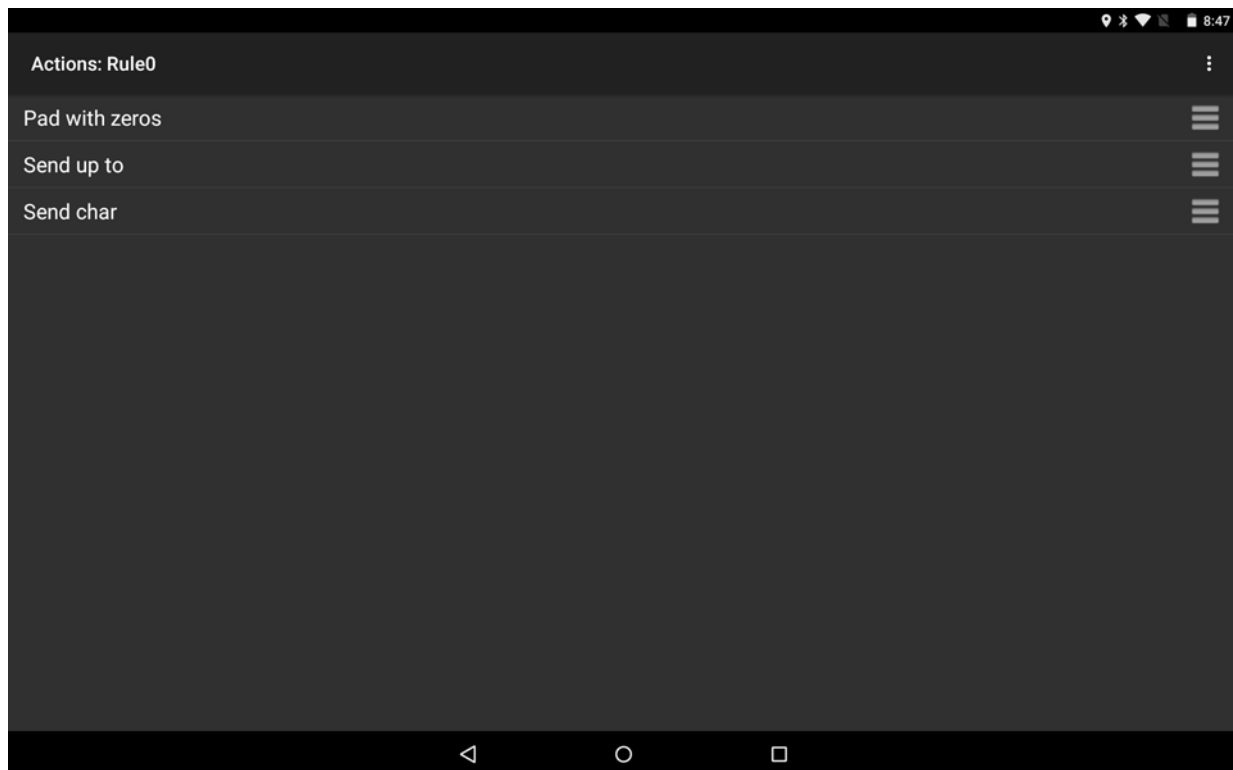


Figure 4-24 ADF Sample Screen

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



Figure 4-25 Sample Bar Code

48. Press and hold the scan key.
The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern. The LED light red to indicate that data capture is in process.
49. A beep sounds to indicate the bar code was decoded successfully. The formatted data 00001299 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.

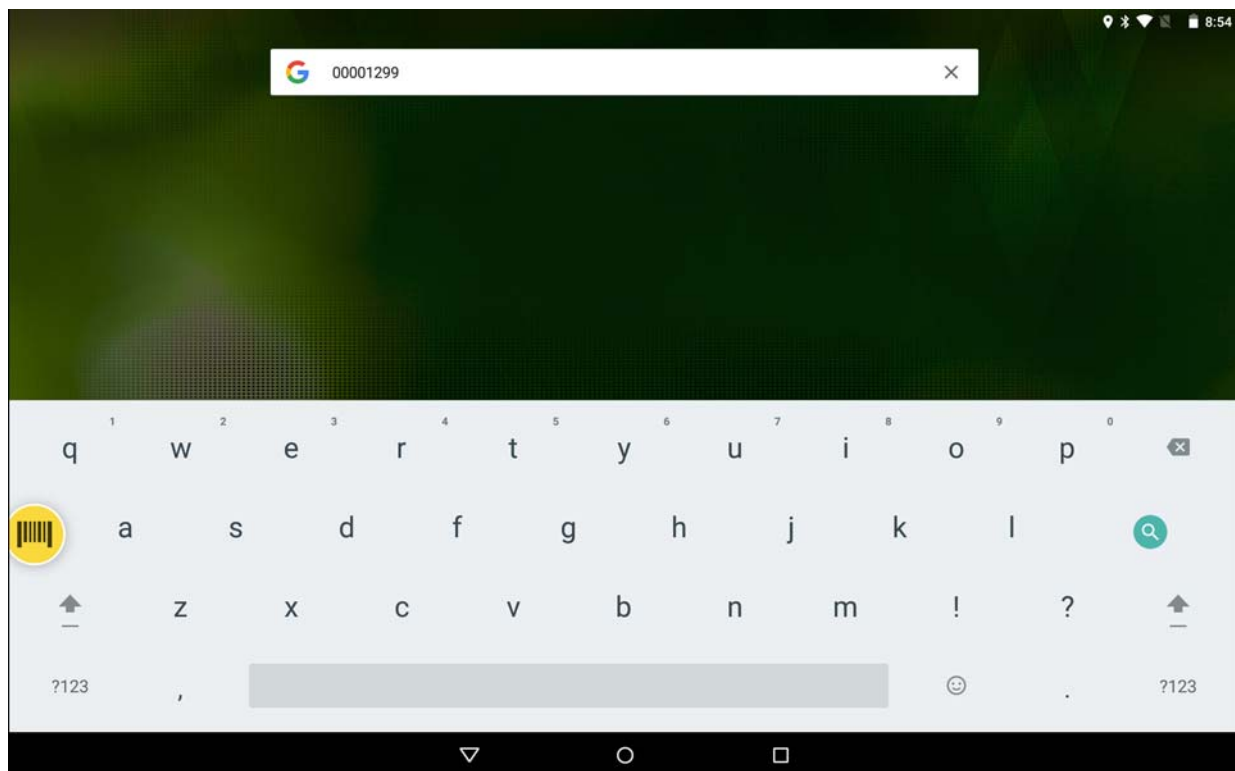


Figure 4-26 Formatted Data

DataWedge Settings

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

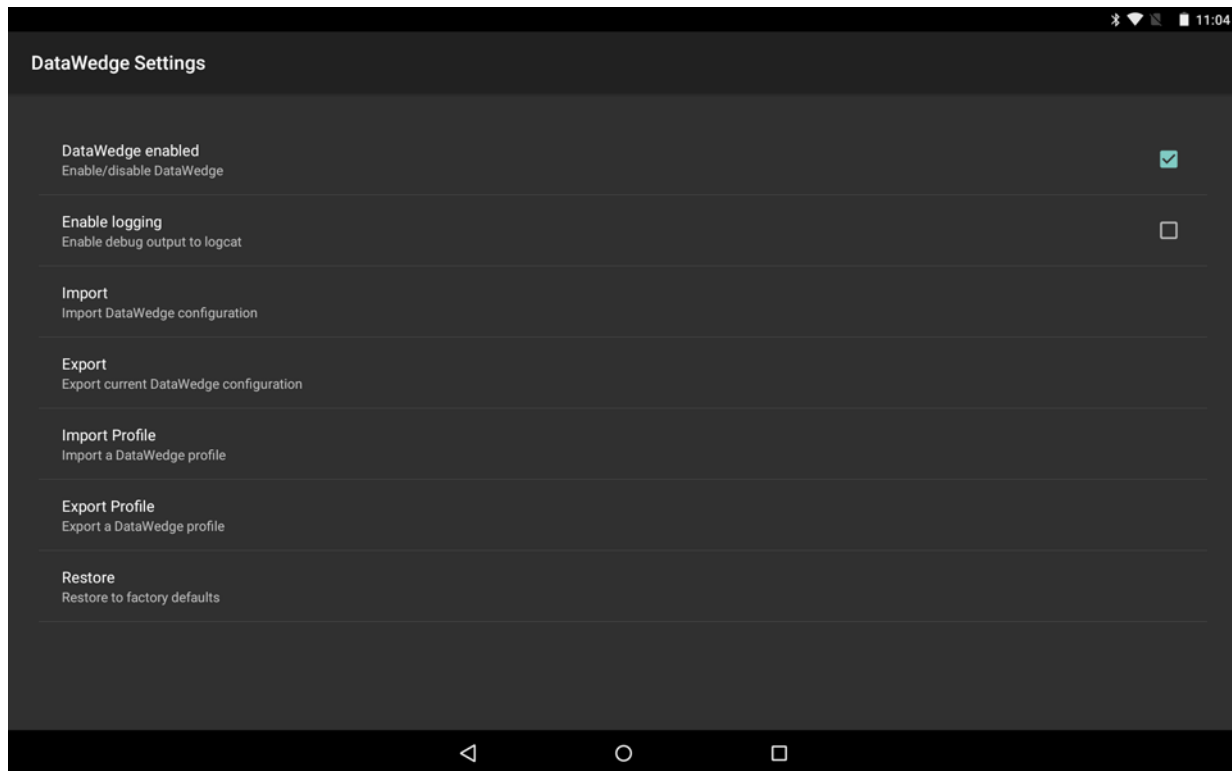








Figure 4-27 *DataWedge Settings Window*

- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option.
- **Enable logging** - Enables or disables DataWedge debug messages in logcat. To enable 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
/storage/emulated/0/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
/storage/emulated/0/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/enterprisereset* for a configuration file, *datawedge.db* or a profile file, *dwprofile_x.db*. If the file is found, it imports the file to replace any existing configuration or profile.



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

Auto Import

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

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



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

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

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application

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

Capture Data and Taking a Photo in the Same Application

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

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

Soft Scan Feature

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

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

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

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

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

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

Sample

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

Scanner Input Plugin

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



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

Function Prototype

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

Parameters

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

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

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

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

Return Values

None.

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

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

Error messages will be logged for invalid actions and parameters.

Example

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

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

Comments

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



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

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

Enumerate Scanners

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

Function Prototype

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

Parameters

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

Return Values

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

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

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

Error messages will be logged for invalid actions and parameters

Example

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

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

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

Comments

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

Set Default Profile

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

Default Profile Recap

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

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

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

Usage Scenario

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

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

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

Function Prototype

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

Parameters

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

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

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

Return Values

None.

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

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

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

Example

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

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

Comments

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

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

Reset Default Profile

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

Function Prototype

```
Intent i = new Intent();

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

Parameters

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

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

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

Return Values

None.

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

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

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

Example

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

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

Comments

None.

Switch To Profile

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

Profiles Recap

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

Profile information consists of:

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

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

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



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

Usage Scenario

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

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

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

Function Prototype

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

Parameters

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

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

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

Return Values

None.

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

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

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

Example

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

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

Comments

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

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

This API function activates such Profiles.

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

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



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

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

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

DataWedge auto Profile switching works as follows:

Every second...



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

CHAPTER 5 SETTINGS

This chapter describes settings available for configuring the device.

Screen Unlock Settings

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

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **Security**.



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

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.
 - **None** - Disable screen unlock security.
 - **Slide** - Slide the lock icon to unlock the screen.
 - **Pattern** - Draw a pattern to unlock screen. See *Set Screen Unlock Using Pattern on page 5-3* for more information.
 - **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 5-2* for more information.
 - **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 5-2* 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. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **Security** > **Screen lock**.
3. Touch **PIN**.
4. Touch in the text field.
5. Enter a PIN (between 4 and 16 characters) then touch **Continue**.
6. Re-enter PIN and then touch **OK**.
7. Touch . The next time the device goes into suspend mode a PIN is required upon waking.

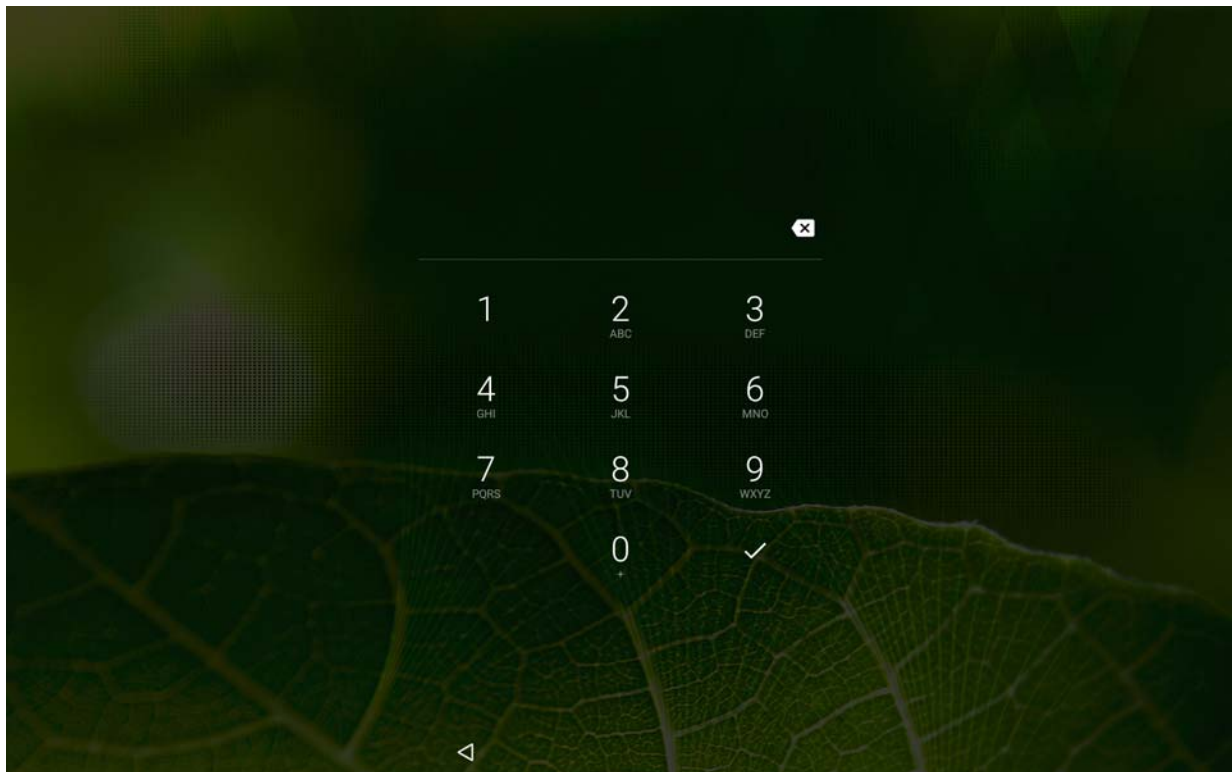





Figure 5-1 PIN Screen

Set Screen Unlock Using Password

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **Security** > **Screen lock**.
3. Touch **Password**.
4. Touch in the text field.
5. Enter a password (between 4 and 16 characters) then touch **Continue**.

6. Re-enter the password and then touch **OK**.
7. Touch . The next time the device goes into suspend mode a PIN is required upon waking.

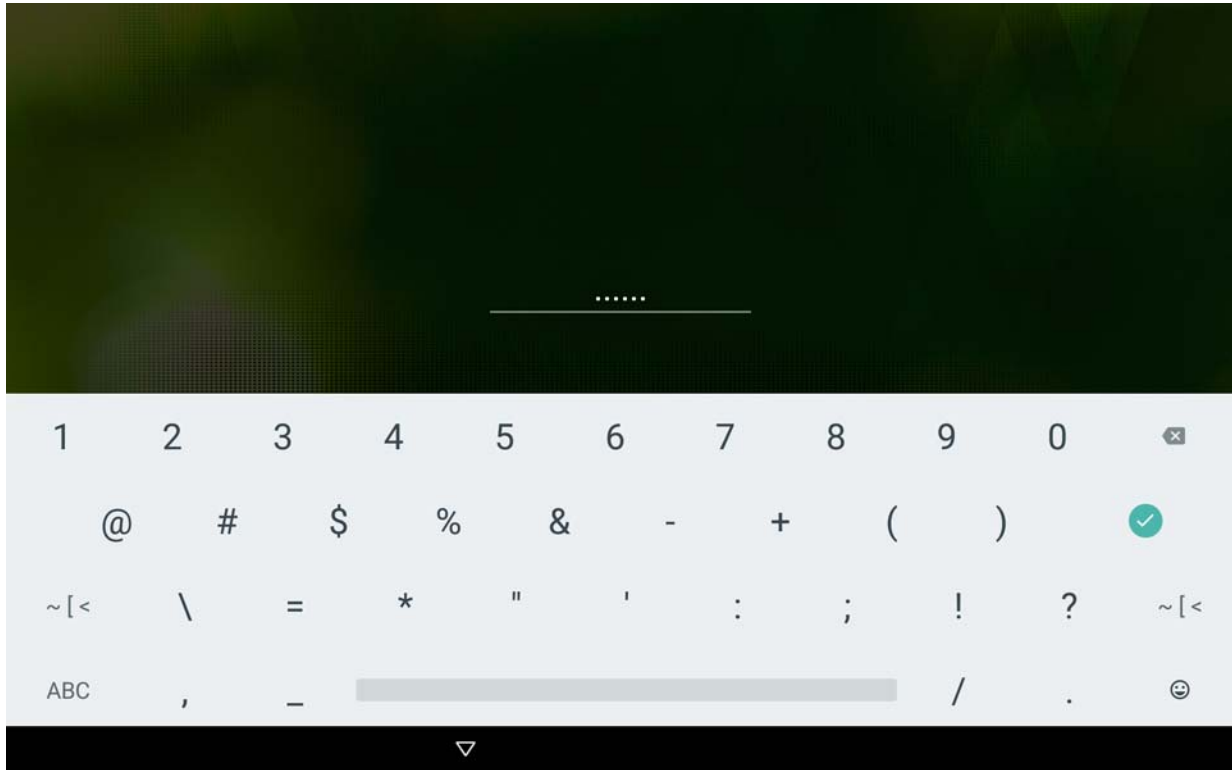




Figure 5-2 Password Screen

Set Screen Unlock Using Pattern

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **Security** > **Screen lock**.
3. Touch **Pattern**.
4. Draw a pattern connecting at least four dots.

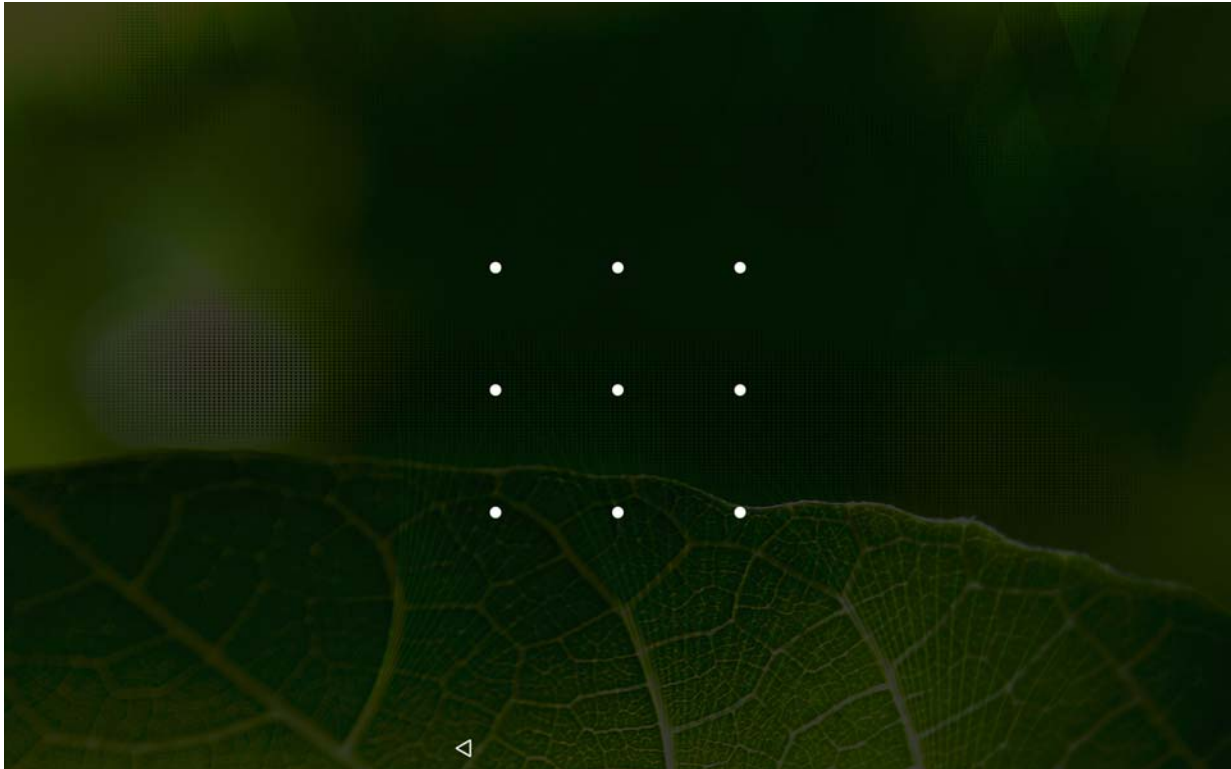



Figure 5-3 *Choose Your Pattern Screen*

5. Touch **Continue**.
6. Re-draw the pattern.
7. Touch **Confirm**.
8. On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.
9. Touch **Vibrate on touch** to enable vibration when drawing the pattern.
10. Touch . The next time the device goes into suspend mode a PIN is required upon waking.

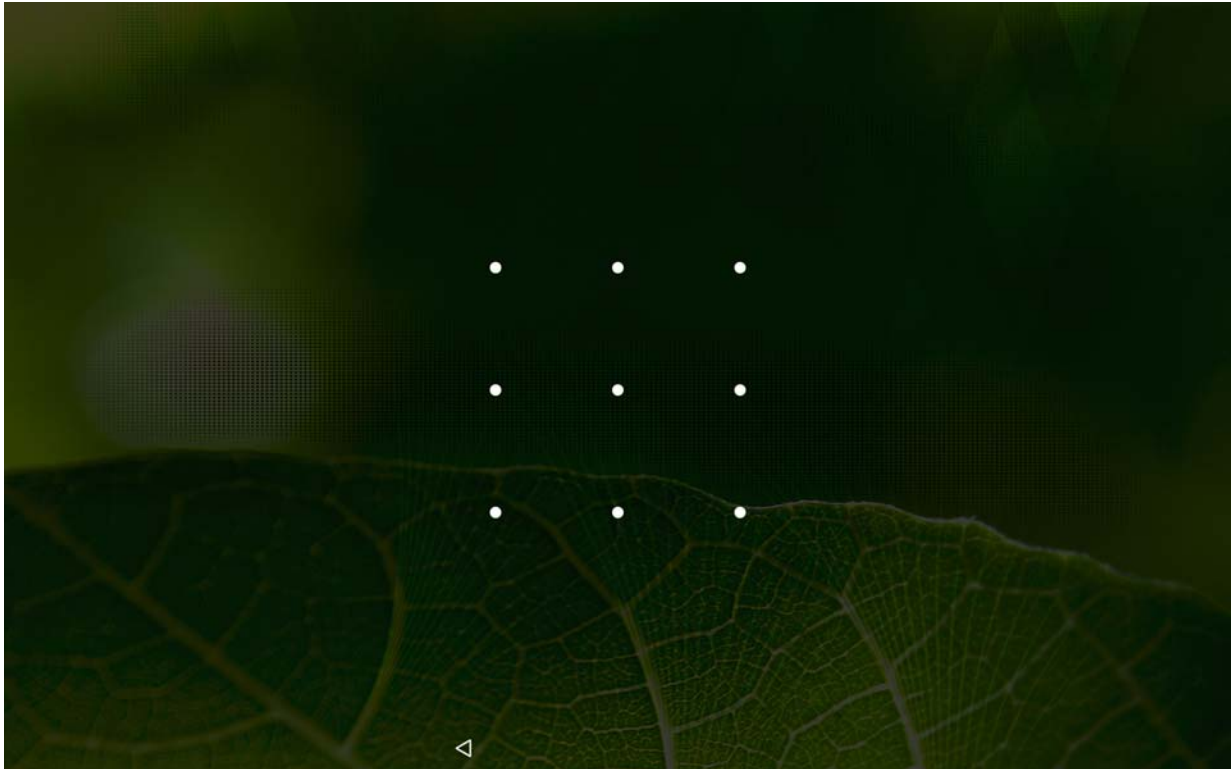




Figure 5-4 Choose Pattern Screen

Passwords

To set the device to briefly show password characters as the user types, set this option.

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **Security** > **Make passwords visible**. A check in the checkbox indicates that the option is enabled.

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 (non-GMS)
- Japanese IME (non-GMS)
- Chinese keyboard.

About Tablet

Use **About tablet** settings to view information about the ET5X.

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch  **About tablet**.
 - **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.
 - SIM status - Displays the wireless (WAN only)
 - **Network** - indicates the current network carrier.
 - **Signal strength** - indicates the radio signal strength.
 - **Cellular network type** - indicates the mobile network type.
 - **Operator info** -
 - **Service state** - indicates the state of service.
 - **Roaming** - indicates if the device is roaming outside the network.
 - **Cellular network state** - indicates the mobile network state.
 - **MDN** - displays the phone number associated with the device.
 - **IMEI** - displays the IMEI number for the device.

- **IMEI SV** - displays the IMEI SV number for the device.
- **IMEI information** - Displays the displays the IMEI number and IMEI SV number for the device. (WAN only)
- **IP address** - Displays the IP address of the device.
- **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
- **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
- **Serial number** - Displays the serial number of the device.
- **Up time** - Displays the time that the ET5X has been running since being turned on.
- **SW components** - Lists filenames and versions for various software on the ET5X.
- **Legal information** - Opens a screen to view legal information about the software included on the ET5X.
- **Model number** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Android security patch level** - Displays the current patch date.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

CHAPTER 6 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 Internal 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 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 Internal Storage.

Development Tools

Android

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



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

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

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

- android.jar
 - Java archive file containing all of the development SDK classes necessary to build an application.
- 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.

EMDK for Android

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

It also includes an exclusive Profile Manager Technology within the your IDE, providing a GUI based development tool. This allows you to write fewer lines of code resulting in reduced development time, effort and errors.

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

StageNow

StageNow is Zebra's next generation Android Staging Solution, supporting Android Lollipop, KitKat, and Jelly Bean operating systems and is built on the MX 4.3/4.4/5.x/6.0 platform. It allows simple profile creation, and easy device deployment with a simple bar code scan, tag read, or audio file play.

The StageNow Staging Solution includes the following components:

- The StageNow Workstation Tool offers a user interface that is accessed within a staging workstation (host computer). The staging administrator uses this tool to create staging profiles that configure device components, in addition to other staging actions. The Workstation Tool includes a database and server which store and save content entered in the tool.
- The StageNow Client resides on the device and provides a user interface for the staging operator to initiate staging. The operator uses a staging method, e.g., prints and scans a bar code, plays an audio file, or reads an NFC tag, to deliver staging material to the device.

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

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 6-4*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 6-4*.
- 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**, Internal storage path is **/storage/sdcard0** or **/sdcard**.

5. Touch  to view files on the 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**.
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 6-3*.

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](#).

Uninstalling an Application

To uninstall an application:

1. Touch  >  **Apps**.

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

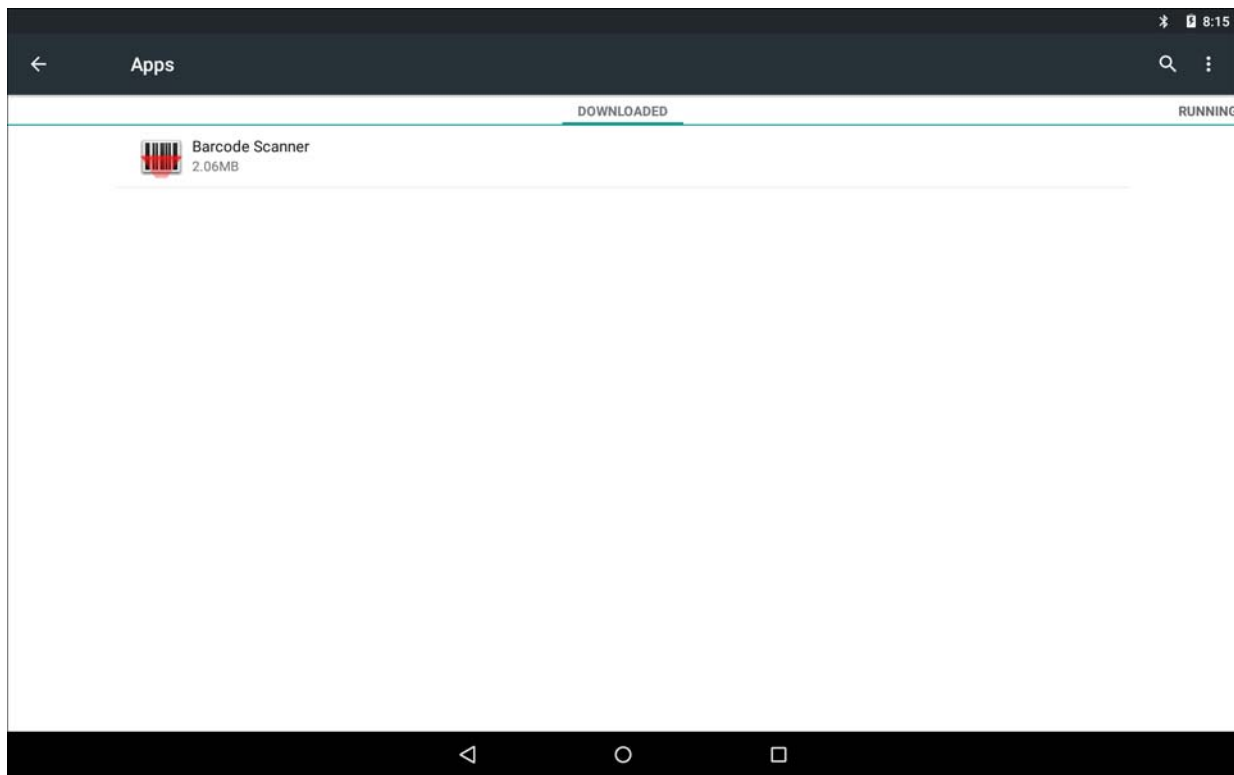


Figure 6-1 Downloaded Screen

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

System Update



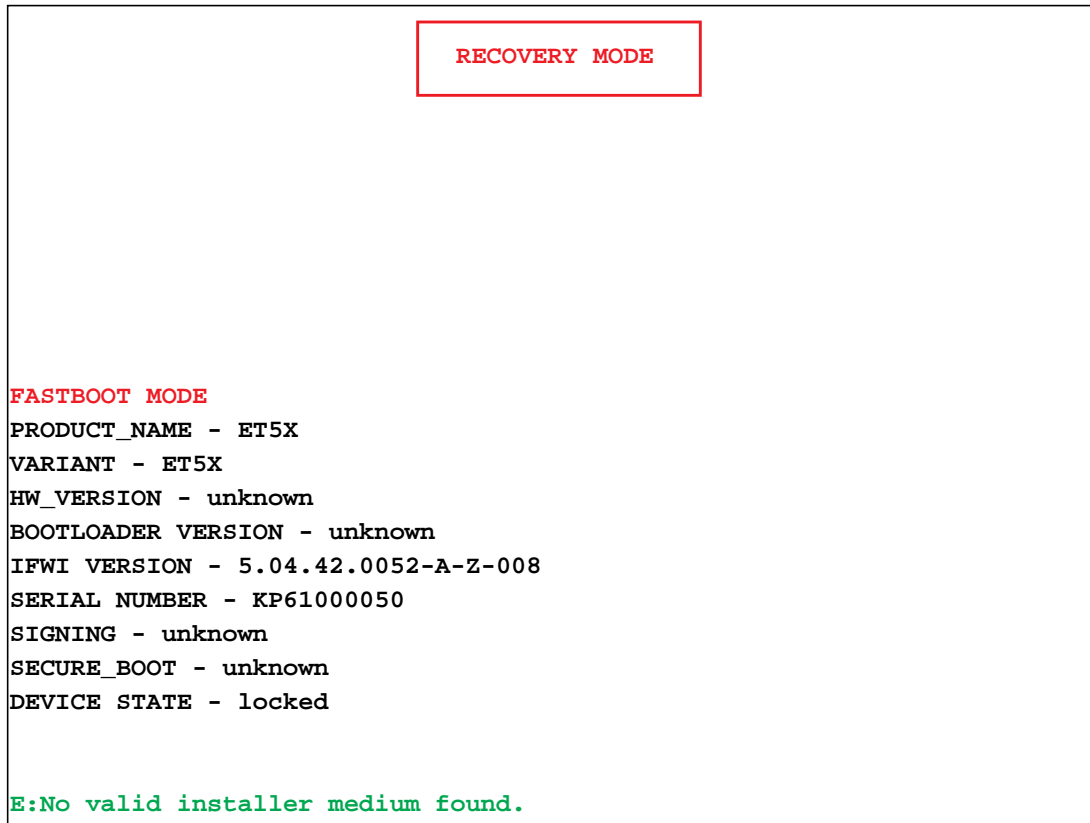
CAUTION These update procedures are only for updating an Android tablet (ET50PE, ET50PT, ET55BE, ET55BT, ET55TE, or ET55TT). Do not attempt to update a Windows Tablet (ET50NE, ET50NT, ET55AE, ET55AT, ET55RE, or ET55RT) with Android software.

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

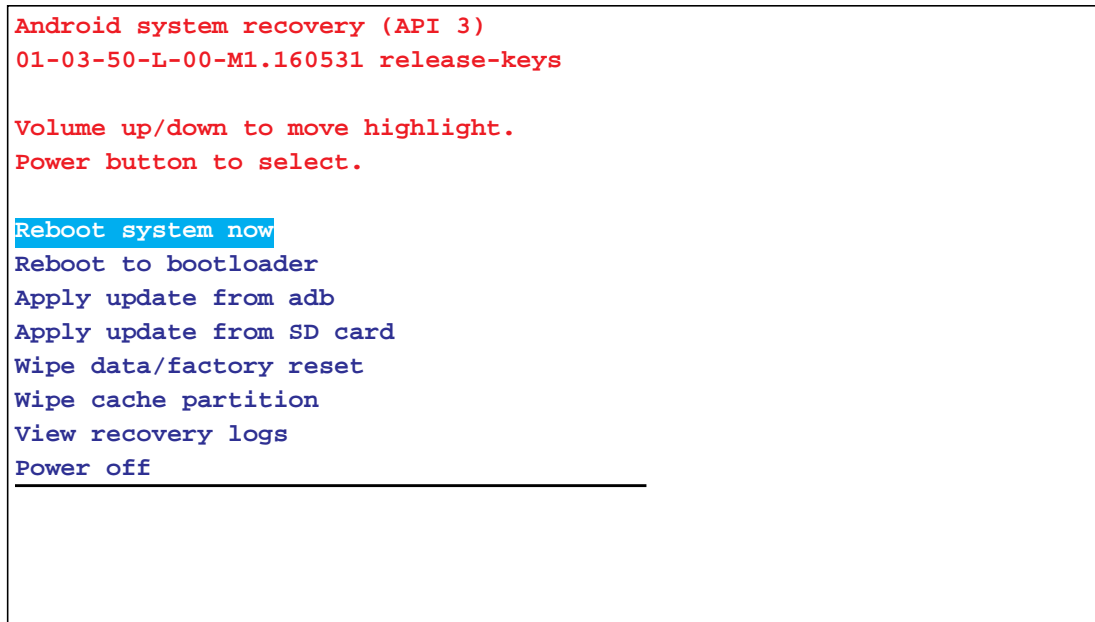
1. Download the system update package:
 - a. Go to the Zebra Support & Downloads web site, <http://www.zebra.com/support>.
 - b. Download the appropriate System Update package to a host computer.
2. Copy the System Update file to the root directory of a microSD card.
3. Press and hold the Power button until the menu appears.
4. Touch **Power off**.
5. Touch **OK**. The device turns off.
6. Open the access door.

6 - 6 ET5X Integrator Guide

7. Insert the microSD card into the SD card slot.
8. Press and release the Power button and then press and hold the Volume Down button. The Fastboot screen appears.
9. Press the Volume Up or Volume Down buttons to navigate to the Recovery Mode screen.



10. Press the Power button to enter Recovery Mode.



11. Press the Up and Down volume buttons to navigate to the **apply update from SD card** option.

```
Android system recovery (API 3)  
01-03-50-L-00-M1.160531 release-keys
```

```
Volume up/down to move highlight.  
Power button to select.
```

```
Reboot system now  
Reboot to bootloader  
Apply update from adb  
Apply update from SD card  
Wipe data/factory reset  
Wipe cache partition  
View recovery logs  
Power off
```

12. Press the Power button.

```
Android system recovery (API 3)  
01-03-50-L-00-M1.160531 release-keys
```

```
Choose a package to install:  
/sdcard
```

```
../  
ET5X-ota-yyymmdd.zip
```

13. Press the Up and Down volume buttons to navigate to System Update file (ET5X-ota-yyymmdd.zip).

14. Press the Power button. The ET5X begins the Update process.

```

-- Battery capacity is 100%. Good to execute recovery functions.

-- Install /sdcard/ET5X-ota-160622.zip ...
Finding update package ...
Opening update package ...
Verifying update package ...
Installing update ...
Patching system image unconditionally ...
Update boot image ...
Updating device specific files ...
Skip touch screen firmware update (already up-to-date) ...
script succeeded: result was [/factory]

Install from SD card complete.

```

15. Make sure the installation is success. Install from SD card complete displays on the screen.
16. Press the Volume Up or Volume Down buttons to navigate to Wipe the data/ factory reset to factory reset the device.

```

Android system recovery (API 3)
01-03-50-L-00-M1.160531 release-keys

Volume up/down to move highlight.
Power button to select.

Reboot system now
Reboot to bootloader
Apply update from adb
Apply update from SD card
Wipe data/factory reset
Wipe cache partition
View recovery logs
Power off

```

17. Press the Power button.
18. Press the Volume Up or Volume Down buttons to navigate to **Yes -- delete all user data**.

```
Android system recovery (API 3)  
01-03-50-L-00-M1.160531 release-keys
```

```
Confirm wipe of all user data?  
THIS CAN NOT BE UNDONE
```

```
No
```

```
No
```

```
No
```

```
Yes - delete all user data
```

```
No
```

```
No
```

19. Press the Power button.

20. The following messages display while deleting the user data.

```
...  
--Wiping data-  
Formatting /data...  
Formatting /cache...  
Data wipe complete.
```

21. Make sure **Data wipe complete** displays on the screen.

22. **Reboot system now** is highlighted.

```
Android system recovery (API 3)
01-03-50-L-00-M1.160531 release-keys
```

```
Volume up/down to move highlight.
Power button to select.
```

```
Reboot system now
```

```
Reboot to bootloader
Apply update from adb
Apply update from SD card
Wipe data/factory reset
Wipe cache partition
View recovery logs
Power off
```

23. Press the Power button.

24. After reboot display shows the software update progress as shown in the below screen.

```
UPDATING BIOS, DO NOT UNPLUG POWER OR RESET SYSTEM!!!
```

```
Compatibility check of update image... pass
Processing update image... done
Storing 2nd stage backup to EMMC... done
Storing 1st stage pieces to fault tolerant region... done
Destroying old IBB... done
Updating Recovery2... done
Updating 1st stage pieces... done
Updating 2nd stage... done
TXE update disabled
Purifying variables... done
```

```
Update was successful, system will soon restart
```

25. After Update was successful message appears, the device automatically reboots to home screen.

26. Press the power button and select **Power off** to power down the device.

27. Remove SD card from the SD card slot.

Storage

The device contains four types of file storage:


- Random Access Memory (RAM)
- External 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.

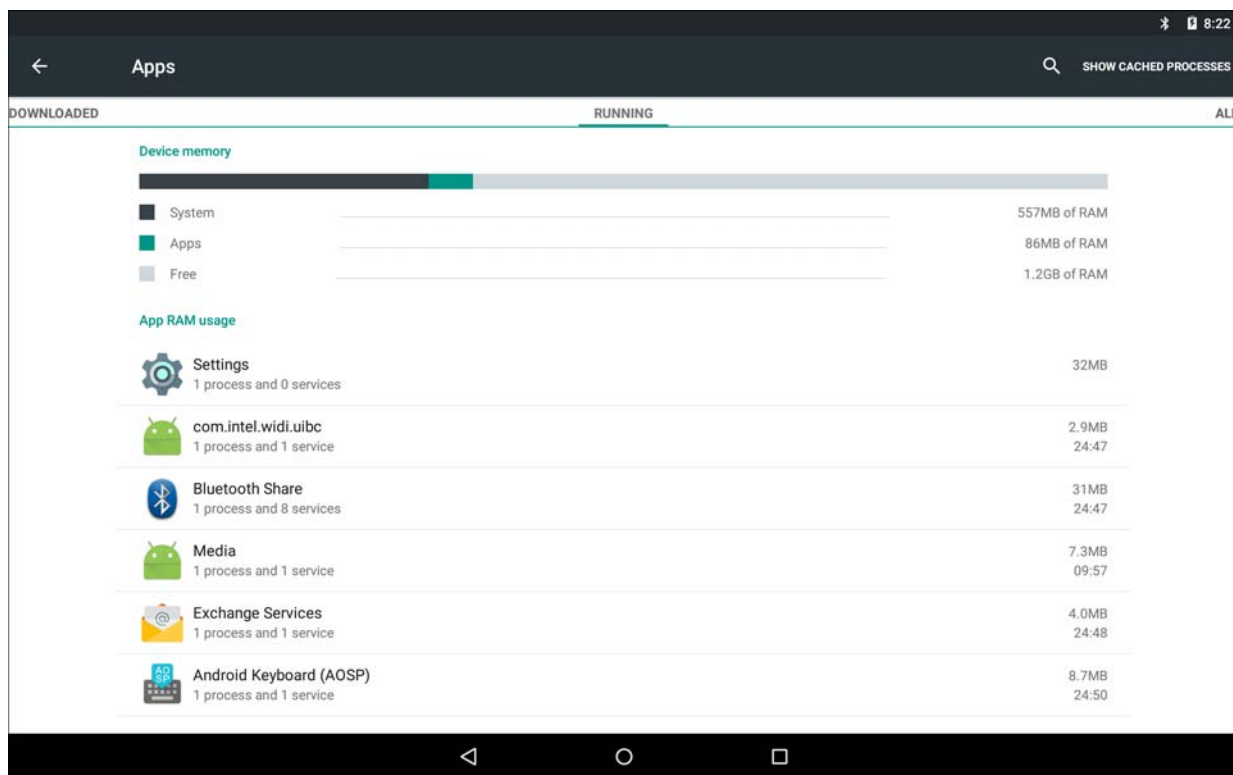




Figure 6-2 Running Screen

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

Internal Storage

The ET5X has internal storage. The internal storage content can be viewed and files copied to and from when the ET5X 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**.

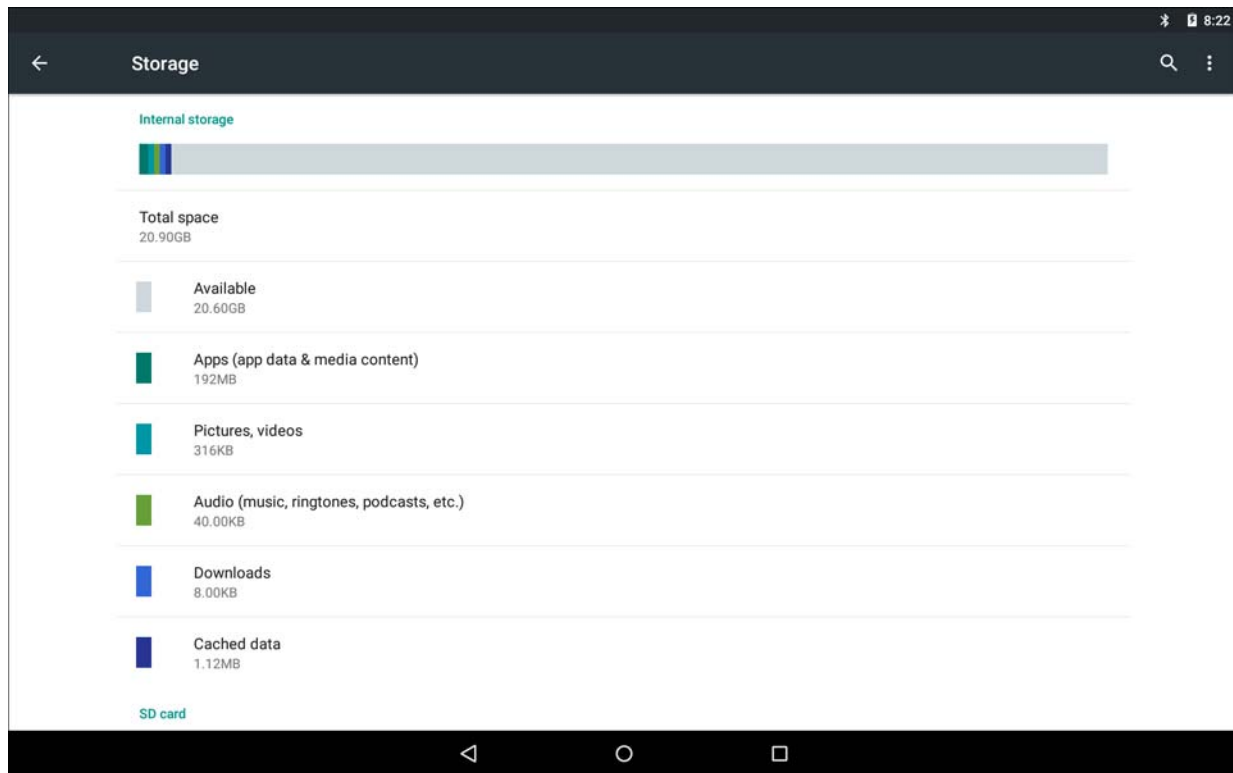




Figure 6-3 Internal Storage Screen

- **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 ET5X can have a removable microSD card or an external USB drive. The content can be viewed and files copied to and from when the ET5X is connected to a host computer.

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

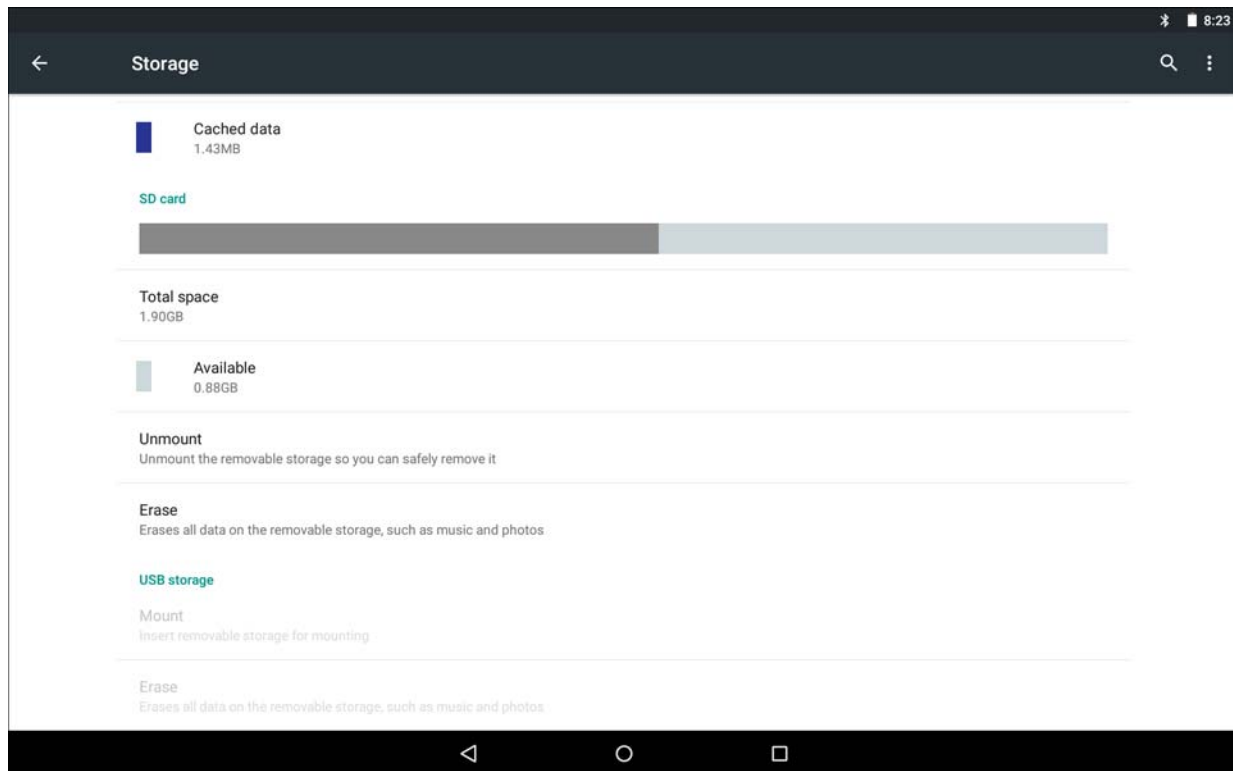




Figure 6-4 *microSD Card Storage Settings*

- **Total space** - Displays the total amount of space on the installed microSD card.
- **Available** - Displays the available space on the installed microSD card.
- **Unmount** - Unmounts the installed microSD card from the ET5X 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** - Permanently erases everything on the installed microSD card.

To view the used and available space on the USB drive, touch  >  **Storage**.

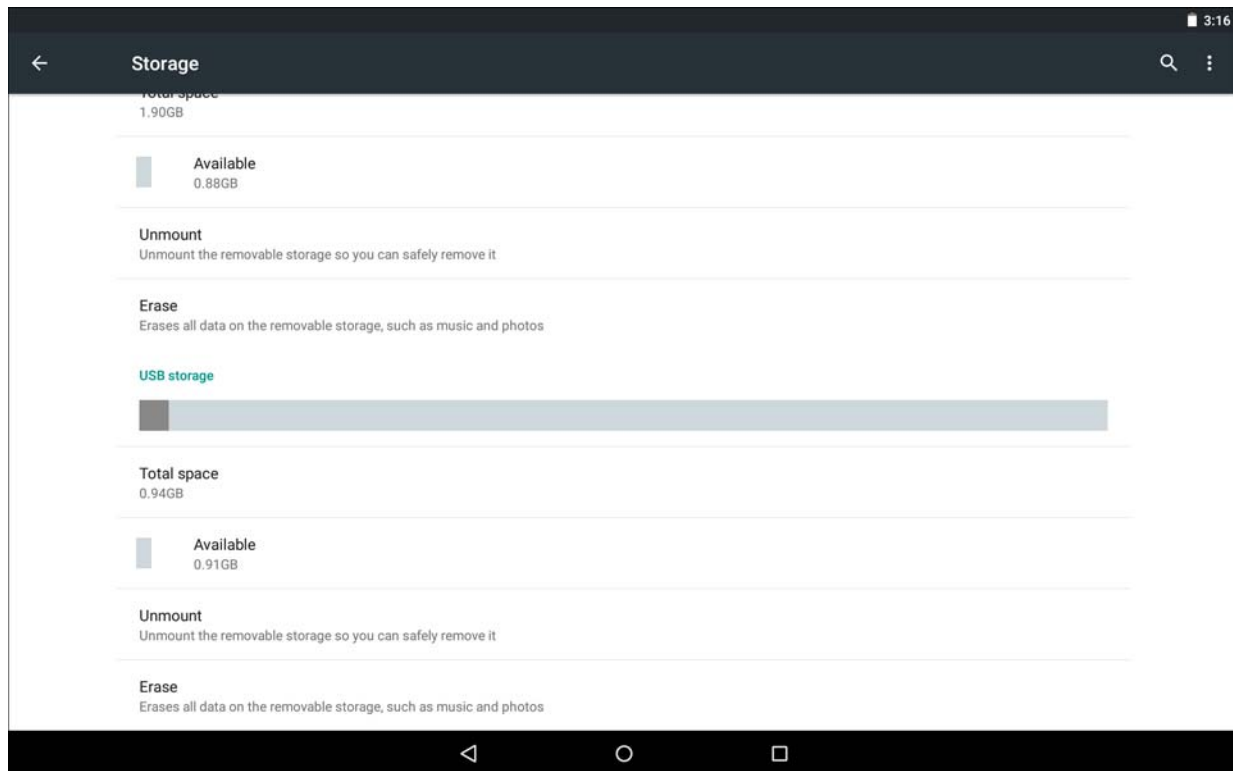


Figure 6-5 *USB Drive Storage Settings*

- **Total space** - Displays the total amount of space on the installed USB drive.
- **Available** - Displays the available space on the installed USB drive.
- **Unmount** - Unmounts the installed USB drive from the ET5X so that it can be safely removed. This setting is dimmed if there is no USB drive installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase** - Permanently erases everything on the installed USB drive.

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**.

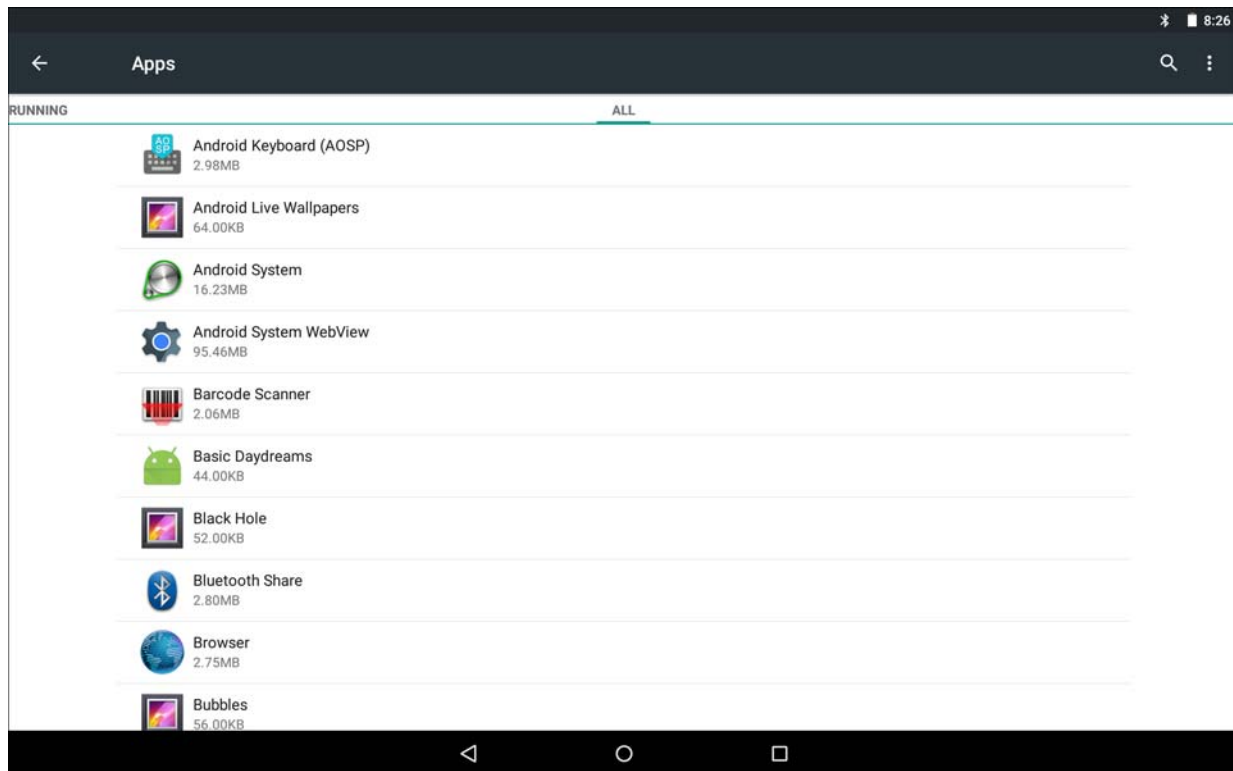


Figure 6-6 Apps Screen

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 6-4 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. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch **Apps**.
3. Swipe the screen to display the **Running** tab.

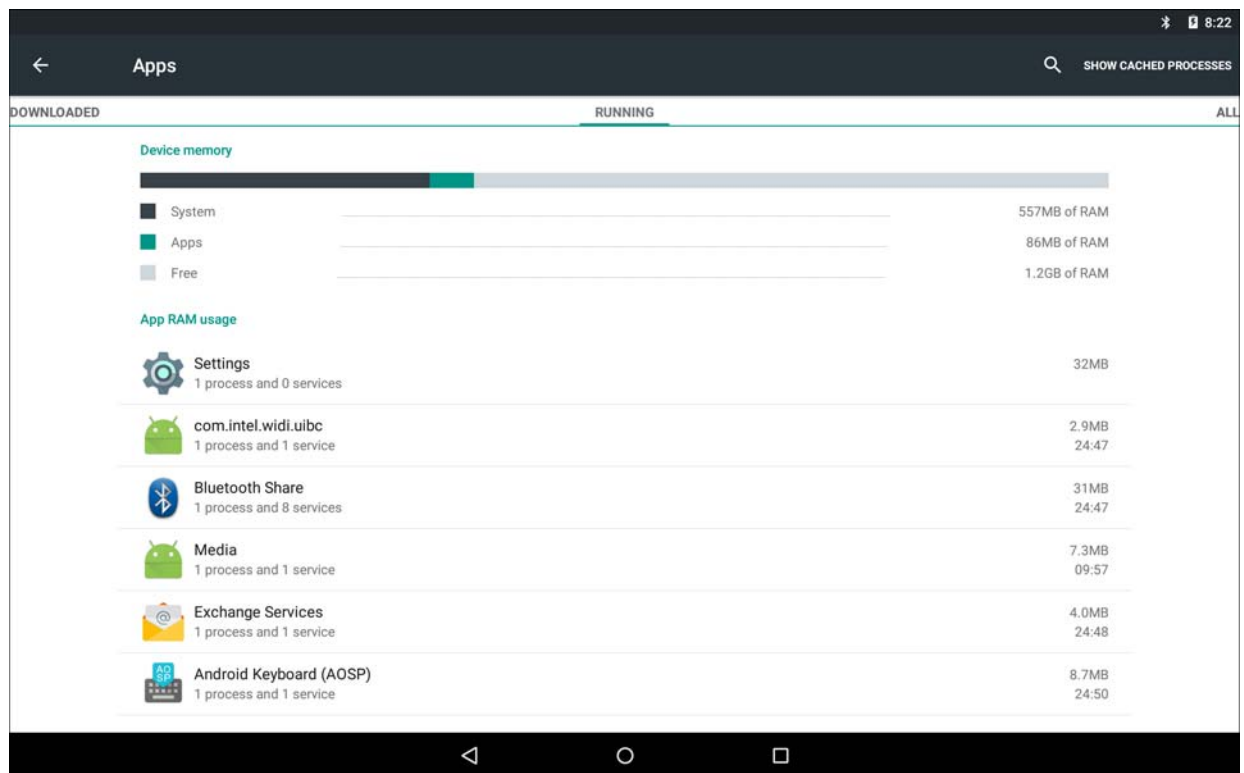


Figure 6-7 *Running Applications*

4. 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.
5. 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.

6. Touch **Stop**.

Managing Downloads

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

Touch  >  to open **Downloads** application.

- Touch an item to open it.
- Touch and hold to select an item and then touch  to delete from storage.
- Touch  > **By name**, **By date modified** or **By size** to sort list.

CHAPTER 7 MAINTENANCE AND TROUBLESHOOTING

Introduction

This chapter includes instructions on cleaning and storing the ET5X, battery maintenance and provides troubleshooting solutions for potential problems during ET5X operations.

Maintaining the ET5X

For trouble-free service, observe the following tips when using the ET5X:

- Protect the ET5X from temperature extremes.
- Do not store or use the ET5X in any location that is extremely dusty, damp, or wet.
- Use a soft lens cloth to clean the scan exit window of the ET5X. If the surface of the ET5X 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 ET5X.
- The display of the ET5X contains glass. Take care not to drop the ET5X or subject it to strong impact.

Battery Safety Guidelines

- The area in which the ET5X 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 xiii* 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 ET5X 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 xiii* 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 Zebra 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 ET5X

Housing

Using the alcohol wipes, wipe the housing.

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.

Power Connector

1. Remove the main battery from ET5X.
2. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.
3. Repeat at least three times.
4. Use the cotton tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
5. Use a dry cotton tipped applicator and repeat steps 3 through 6.
6. 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.

7. 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 Expansion Back Connectors

Use this procedure to clean the connectors on an Expansion Back:

1. Remove the Expansion Back from the ET5X.

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. 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.

5. Ensure that there is no lint left by the cotton tipped applicator, remove lint if found.
6. If grease and other dirt can be found on other areas of the Expansion Back, use lint free cloth and alcohol to remove.
7. Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before installing the Expansion Back.

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 ET5X 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

ET5X

Table 7-1 Troubleshooting the ET5X

Problem	Cause	Solution
ET5X does not turn on.	Battery not charged.	Charge the battery in the ET5X.
	Battery not installed properly.	Ensure battery is installed properly.
	System crash.	Perform a warm boot. If the ET5X still does not turn on, perform a cold boot. See <i>Resetting the ET5X</i> on page 1-6.
Battery did not charge.	Battery failed.	Replace battery. If the ET5X still does not operate, try a warm boot, then a cold boot. See <i>Resetting the ET5X</i> on page 1-6.
	ET5X removed from cradle before charging completed.	Insert the ET5X into the cradle and begin charging. The battery fully charges in approximately three 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 over Wi-Fi, no data transmitted, or transmitted data was incomplete.	Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
	You moved out of range of an access point.	Move closer to an access point.
During data communication over WAN, no data transmitted, or transmitted data was incomplete.	You are in an area of poor cellular service.	Move into an area that has better service.
	APN is not set up correctly.	See system administrator for APN setup information.
	SIM card not installed properly.	Remove and re-install the SIM card.
	Data plan not activated.	Contact your service provider and ensure that your data plan is enable.
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	Bluetooth radio is not on.	Turn on the Bluetooth radio.
	You moved out of range of another Bluetooth device.	Move within 10 meters (32.8 feet) of the other device.

Table 7-1 *Troubleshooting the ET5X (Continued)*

Problem	Cause	Solution
The multi-touch screen responds slowly or improperly.	Finger or screen is wet.	Ensure that your hands are clean and dry when touching the screen. Restart the tablet to try again.
ET5X turns itself off.	ET5X is inactive.	The ET5X turns off after a period of inactivity. If the ET5X is running on battery power.
	Battery is depleted.	Place the ET5X in a cradle to re-charge the battery.
	The ET5X's battery is low and it powers down to protect memory content.	Place the ET5X in a cradle to re-charge the battery.

Charge Only Cradle

Table 7-2 *Troubleshooting the Charge only Cradle*

Symptom	Possible Cause	Solution
ET5X battery is not charging.	ET5X was removed from cradle or cradle was unplugged from AC power.	Ensure cradle is receiving power. Ensure ET5X is seated correctly. Confirm main battery is charging. The battery fully charges in approximately three hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The ET5X is not fully seated in the cradle.	Remove and re-insert the ET5X 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).

Communication and Charging Cradles

Table 7-3 *Troubleshooting the Communication and Charging Cradles*

Symptom	Possible Cause	Solution
ET5X battery is not charging.	ET5X was removed from cradle or cradle was unplugged from AC power.	Ensure cradle is receiving power. Ensure ET5X is seated correctly. Confirm main battery is charging. The battery fully charges in approximately three hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The ET5X is not fully seated in the cradle.	Remove and re-insert the ET5X 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).
During communication, no data transmits, or transmitted data was incomplete.	ET5X removed from cradle during communications.	Replace ET5X in cradle and retransmit.
	Incorrect cable configuration.	Ensure that the correct cable configuration.
ET5X does not lock into cradle.	Access cover closed.	Open ET5X access cover and re-insert ET5X onto cradle.
	ET5X with Rugged Frame and IO Adapter does not mate with Communication and Charging Cradle.	Use Rugged Communication and Charging Cradle.

Expansion Back

Table 7-4 *Troubleshooting the Expansion Back*

Symptom	Possible Cause	Solution
Aiming laser does not display when pressing trigger.	On 8" tablet, did not remove rubber gasket during installation.	See system administrator to re-install Expansion Back.
	ET5X is in suspend mode.	Press power button to wake the tablet.
	Battery is low.	If the scanner stops emitting a laser beam upon a trigger press, check the battery level. When the battery is low, the scanner shuts off before the ET5X low battery condition notification. Note: If the scanner is still not reading symbols, contact system administrator.

Table 7-4 *Troubleshooting the Expansion Back (Continued)*

Symptom	Possible Cause	Solution
Laser comes on, but scanner does not decode the bar code.	ET5X is not programmed for the bar code.	Ensure the ET5X is programmed to read the type of bar code being scanned.
	Unreadable bar code.	Check the symbol to ensure it is not defaced. Try scanning another bar code of the same type.
	Distance between exit window and bar code is incorrect.	Move the ET5X within proper scanning range.
	Scanning application is not loaded.	Load a scanning application. See the system administrator.

APPENDIX A SPECIFICATIONS

Technical Specifications

The following tables summarize the ET5X's intended operating environment and general technical hardware specifications.

ET5X

The following table summarizes the ET5X's intended operating environment.

Table A-1 Technical Specifications

Item	Description
Physical and Environmental Characteristics	
Dimensions	8" Configuration: 228 mm W x 150 mm H x 12.5 mm D (9.0 in. L x 5.9 in. W x 0.5 in. H) 10" Configuration: (269 mm W x 181 mm H x 12.5 mm D) 10.6 in. L x 7.1 in. W x 0.5 in. H
Weight	8" Configuration: 555 g (1.2 lbs) 10" Configuration: 750 g (1.55 lbs)
Display	8" Configuration: 8.3 in (diagonal) 1920 x 1200 WUVGA with backlight 10" Configuration: 10.1 in (diagonal) 1920 x 1200 WUVGA with backlight
Touch panel	Capacitive 10 point multi-touch
Keypad Options	Virtual, Bluetooth or USB

Table A-1 Technical Specifications (Continued)

Item	Description
Expansion	Integrated connector to easily add accessories
Connectivity	Docking connector: USB 3.0, HDMI, charging; rugged connector for use with rugged dock Interfaces: full-size USB 2.0 connector, audio jack 3.5mm, microUSB (for communication with host computer)
Notification	LED flash; bar code decode; camera LED indicator
Audio	Stereo speakers and dual microphones (one front and one rear-facing)
Battery	8" Configuration: 5,900 mAh rechargeable Smart Li-Ion; user replaceable 10" Configuration: 8,700 mAh rechargeable Smart Li-Ion; user replaceable
Performance Characteristics	
CPU	Intel quad core 1.33GHz (Turbo Frequency = 1.86GHz) Frequency supports 64 bit OS
Operating System	Android Open Source Project (AOSP) version 5.1.1 or Google Mobile Services (GMS) version 5.1.1.
Memory	2 GB LPDDR3 RAM; 32 GB eMMC Flash; User accessible microSDXC card slot (standard supports up to 2 TB)
Data Capture	
Front Camera	2 MP 1080p full HD optimized for video and low lighting conditions.
Rear Camera	Image capture: 8MP auto-focus camera with user controllable LED flash, illumination; captures photographs and video.
Video	1080p (Full HD, 1920 x 1080), Frame rate = 30fps
Scanning	Optional SE4750 8" Expansion Back Optional SE4750 10" Expansion Back
User Environment	
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 60°C (-4°F to 140°F)
Battery Charging Temperature	0°C to +40°C (32°F to 104°F)
Humidity	10% to 90% RH (non condensing)
Drop Specification	Standard: 1 m (3.28 ft.) drop to concrete without rugged frame. With optional rugged frame: 1.8 m (5.9 ft.) to concrete per MIL STD 810G. With optional Expansion Back: Per MIL STD 810G across operating temperatures.

Table A-1 Technical Specifications (Continued)

Item	Description
Vibration	Operational: random vibration 10-1000 Hz 1.9g RMS, 1 hour duration per axis. Non-operational: random vibration 10-1000Hz, 4.1 g RMS
Environmental Sealing	IP65
ESD	+/-8kVdc air discharge +/-4kVdc direct discharge +/-4kVdc indirect discharge
WWAN Wireless Data Communications	
	Global LTE with HSPA+ North America multi-carrier LTE with both Verizon (EVDO) and AT&T (HSPA+) 3G fallback
WLAN Wireless Data Communications	
WLAN radio	2x2 MIMO; IEEE 802.11a/b/g/n/ac/d/h/i/r.
Data Rate	2.4 GHz: 802.11b/g/n - up to 144 Mb per second 5 GHz: 802.11a/n/ac - up to 866.7 Mb per second
Operating Channels	Chan 1 - 13 (2412 - 2472 MHz), Chan 36 - 165 (5180 - 5825 MHz) Channel Bandwidth: 20, 40, 80 MHz Actual operating channels/frequencies depend on regulatory rules and certification agency.
Antenna	Dual band antennas for 2x2 MIMO
WLAN Security	WEP (40 or 104 bit); WPA/WPA2 Personal (TKIP and AES); WPA/WPA2 Enterprise (TKIP and AES) - EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0-MSCHAPv2, PEAPv1-EAP-GTC, EAP Fast and LEAP.
WPAN Wireless Data Communications	
Bluetooth	Class 2, Bluetooth v4.0 (Bluetooth® Smart)
Near Field Communication	P2P: ISO 18092 • Reader/Writer: ISO 14443 – A-B, MIFARE, FeliCa®, ISO 15693, NFC Forum Tag Types 1 to 4 • Card emulation: ISO 14443 – A-B-B', MIFARE, FeliCa RF • Distance up to 3 cm
Sensors	
Gyroscope	Maintains orientation based on principles of conservation of angular momentum
Motion Sensor	3-axis accelerometer that enables motion-sensing applications for dynamic screen orientation and power management.
Ambient Light Sensor	Automatically adjusts display brightness, keypad and display backlight.
Electronic Compass	Independent — does not depend on GPS

Table A-1 *Technical Specifications (Continued)*

Item	Description
Peripherals and Accessories	
Cradles	Charge Only Cradle Communication and Charging Cradles Rugged Communication Cradle 4-Slot Charge Only Cradle Charging Adapter 4-Slot Battery Charger
Printers	Supports extensive line of Zebra approved printers
Rugged Frame	Provides additional protection for the tablet.

SE4750 Expansion Back Decode Range

SE4750 SR Decode Ranges

Table A-2 *SE4750 SR Decode Distances*

Bar Code Type	Near Distance (in, typical)	Far Distance (in, typical)
3 mil Code 39	2.8	6.2
5 mil Code 128	2.3	8.7
5 mil PDF417	3.0	8.1
6.67mil PDF417	2.2	10.6
10 mil Data Matrix	2.4	10.6
100% UPCA	1.6*	23.0
15 mil Code 128	2.4*	25.2
20.0 mil Code 39	1.6*	36.3

* 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.

SE4750 MR Decode Ranges

Table A-3 SE4750 MR Decode Distances

Bar Code Type	Near Distance (in, typical)	Far Distance (in, typical)
5 mil Code 128	7.4	16.0
5 mil PDF417	8.1	13.1
7.5 mil Data Matrix	8.3	12.8
10 mil Data Matrix	7.0	17.0
13 mil UPCA	2.3*	38.0
15 mil Code 128	4.0*	40.0
20 mil Code 39	2.1*	54.0
100 mil Code 39	11.0	172.0
160 mil Data Matrix	11.5	138.0

* 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.

Accessory Specifications

Charge Only Cradle

Table A-4 Charge Only Cradle Technical Specifications

Feature	Description
Dimensions	Height: 7.9 cm (3.1 in.) Width: 14.2 cm (5.6 in.) Depth: 11.9 cm (4.7 in.)
Weight	550 g (19.4 oz)
Input Voltage	12 VDC
Power Consumption	60 watts
Operating Temperature	0°C to 40°C (32°F to 104°F)
Humidity	10% to 90% non-condensing
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Communication and Charging Cradle

Table A-5 Communication and Charging Cradle Technical Specifications

Feature	Description
Dimensions	Height: 7.9 cm (3.1 in.) Width: 14.2 cm (5.6 in.) Depth: 11.9 cm (4.7 in.)
Weight	550 g (19.4 oz)
Input Voltage	12 VDC
Power Consumption	60 watts
Operating Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 90% non-condensing
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Rugged Communication and Charging Cradle

Table A-6 *Rugged Communication and Charging Cradle Technical Specifications*

Feature	Description
Dimensions	Height: 7.9 cm (3.1 in.) Width: 14.2 cm (5.6 in.) Depth: 11.9 cm (4.7 in.)
Weight	550 g (19.4 oz)
Input Voltage	12 VDC
Power Consumption	60 watts
Operating Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 90% non-condensing
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Expansion Backs

Table A-7 *8" Expansion Back Technical Specifications*

Feature	Description
Dimensions	Height: 137 mm (5.4 in.) Width: 157.5 mm (6.2 in.) Depth: 54 mm (2.1 in.)
Weight	246 g (8.7 oz)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 60°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Drop	1.2 m (4 ft) drop to plywood over concrete per MIL-STD 810G across operating temperatures with rugged frame.
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Table A-8 8" SE4750 Expansion Back Technical Specifications

Feature	Description
Dimensions	Height: 137 mm (5.4 in.) Width: 157.5 mm (6.2 in.) Depth: 54 mm (2.1 in.)
Weight	273 g (9.6 oz)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 60°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Drop	1.2 m (4 ft) drop to plywood over concrete per MIL-STD 810G across operating temperatures with rugged frame.
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Table A-9 10" Expansion Back Technical Specifications

Feature	Description
Dimensions	Height: 157.7 mm (6.2 in.) Width: 184 mm (7.2 in.) Depth: 54 mm (2.1 in.)
Weight	307 g (10.8 oz)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 60°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Drop	1.2 m (4 ft) drop to plywood over concrete per MIL-STD 810G across operating temperatures with rugged frame.
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

Table A-10 10" SE4750 Expansion Back Technical Specifications

Feature	Description
Dimensions	Height: 157.7 mm (6.2 in.) Width: 184 mm (7.2 in.) Depth: 54 mm (2.1 in.)
Weight	336.5 g (11.9 oz)

Table A-10 10" SE4750 Expansion Back Technical Specifications (Continued)

Feature	Description
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 60°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Drop	1.2 m (4 ft) drop to plywood over concrete per MIL-STD 810G across operating temperatures with rugged frame.
Electrostatic Discharge (ESD)	+/- 8 kV air +/- 4 kV contact

INDEX

Numerics

A

accessories

- four slot charge only cradle . . . 2-7, 2-11, 2-15, 2-21
- single slot serial/USB cradle 2-4
- specifications A-6

B

- battery charging temperature A-2
- bullets xiii

C

- cleaning 7-1
- configuration 1-1
- configurations xi
- conventions
 - notational xii
- CPU A-2
- cradles
 - four slot charge only 2-7, 2-11, 2-15, 2-21
 - single slot 2-4

D

- data capture xi
- decode distances A-4, A-5
- dimensions A-1
- display xi, A-1
- drop specification A-2

F

- four slot charge only cradle 2-7, 2-11, 2-15, 2-21

G

- getting started 1-1

H

- humidity A-2

I

- information, service xiii

L

- lithium-ion battery 1-1

M

- main battery
 - installing 1-1
- maintenance 7-1
- memory xi, A-2

O

- operating environment, tablet A-1
- operating system xi, A-2
- operating temperature A-2

P

- parts of the tablet
 - front view 1-1

R

- radios xi

related documentsxiii

related softwarexiii

S

single slot serial/USB cradle 2-4

specifications A-1

starting the tablet 1-1

storage temperature A-2

T

tablet configuration 1-1

technical specifications

 accessories A-6

technical specifications, tablet A-1

troubleshooting 7-5

U

unpacking 1-1

W

weight A-1

WLAN 802.11a/b/g/nxi, xii

WPAN Bluetoothxi, xii



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

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.

© 2016 Symbol Technologies LLC, a subsidiary of Zebra Technologies Corporation. All rights reserved.