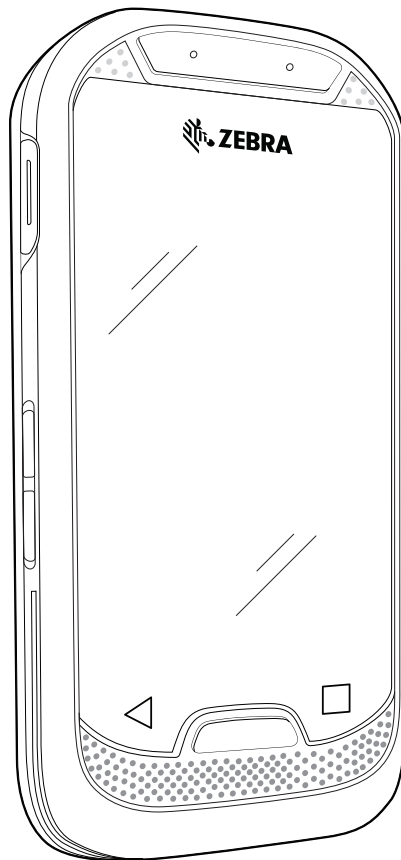


# EC30

## Enterprise Companion



## Integrator Guide for Android™ 8.1.0 Oreo



## Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to [zebra.com/copyright](https://zebra.com/copyright).

WARRANTY: For complete warranty information, go to [zebra.com/warranty](https://zebra.com/warranty).

END USER LICENSE AGREEMENT: For complete EULA information, go to [zebra.com/eula](https://zebra.com/eula).

## Terms of Use

- Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

- Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

- Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

- Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

## Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	7/2019	Initial release.
-02 Rev A	11/2019	Added information to Troubleshooting.
-03 Rev A	7/2021	Added steps for manually entering Android recovery mode.

# Table of Contents

Copyright .....	2
Terms of Use .....	2
Revision History .....	2
<b>About This Guide .....</b>	<b>10</b>
Introduction .....	10
Documentation Set .....	10
Configurations .....	10
Software Versions .....	10
Chapter Descriptions .....	11
Notational Conventions .....	11
Related Documents .....	12
Service Information .....	12
<b>Getting Started .....</b>	<b>13</b>
Introduction .....	13
Setup .....	13
Charging the Device .....	13
Charging Temperature .....	14
Charging Indicators .....	14
Resetting the Device .....	14
Performing a Soft Reset .....	14
Performing a Hard Reset .....	15
<b>Accessories .....</b>	<b>16</b>
Introduction .....	16
Accessories .....	16
2-Slot Charge Only Cradle .....	19
Setup .....	20

## Table of Contents

Charging the Device .....	21
Charging Status .....	21
Charging Temperature .....	21
10-Slot Charge Only Cradle .....	22
Setup .....	22
Charging the Device .....	23
Charging Status .....	23
Charging Temperature .....	23
10-Slot Locking Charge Only Cradle .....	24
Setup .....	24
Charging the Device .....	25
Manual Release Using a Release Key .....	25
Charging Status .....	26
Charging Temperature .....	26
10-Slot Cradle Rack Installation .....	26
Rack Mount Installation .....	29
Wall Installation .....	31
Bottom Tray Assembly .....	32
Bracket Wall Mounting .....	32
Rack Mount Plate Installation .....	34
<b>Settings.....</b>	<b>38</b>
Introduction .....	38
WLAN Configuration .....	38
Configuring a Secure Wi-Fi Network .....	38
Manually Adding a Wi-Fi Network .....	40
Configuring for a Proxy Server .....	40
Configuring the Device to Use a Static IP Address .....	41
Wi-Fi Preferences .....	42
Additional Wi-Fi Settings .....	43
Wi-Fi Direct .....	43
WPS Push Button .....	44
WPS Pin Entry .....	45
Setting Screen Lock .....	45
Setting Screen Lock Using PIN .....	46
Setting Screen Unlock Using Password .....	46
Setting Screen Unlock Using Pattern .....	47
Showing Passwords .....	48
Remapping a Button .....	48
Accounts .....	50
Language Usage .....	50

## Table of Contents

Changing the Language Setting .....	50
Adding Words to the Dictionary .....	50
Keyboard Settings .....	50
PTT Express Configuration .....	51
RxLogger .....	51
RxLogger Configuration .....	51
RxLogger Settings .....	52
ANR Module .....	52
Kernel Module .....	52
Logcat Module .....	53
LTS Module .....	54
Ramoops Module .....	54
Resource Module .....	54
Snapshot Module .....	55
TCPDump Module .....	55
Tombstone Module .....	56
Configuration File .....	56
Enabling Logging .....	56
Disabling Logging .....	56
Extracting Log Files .....	56
RxLogger Utility .....	57
App View .....	57
Backup .....	57
Archive Data .....	58
Overlay View .....	58
Initiating the Main Chat Head .....	58
Removing the Main Chat Head .....	58
Viewing Logs .....	58
Removing a Sub Chat Head Icon .....	59
Backing Up In Overlay View .....	59
About .....	60
<b>USB Communication .....</b>	<b>61</b>
Introduction .....	61
Transferring Files with a Host Computer via USB .....	61
Transferring Files .....	61
Transferring Photos .....	62
Disconnect from the Host Computer .....	62
<b>DataWedge .....</b>	<b>63</b>
Introduction .....	63
Basic Scanning .....	63

Profiles .....	64
Profile0 .....	64
Plug-ins .....	64
Input Plug-ins .....	65
Process Plug-ins .....	65
Output Plug-ins .....	65
Profiles Screen .....	65
Profile Context Menu .....	66
Options Menu .....	67
Disabling DataWedge .....	67
Creating a New Profile .....	67
Profile Configuration .....	68
Associating Applications .....	68
Data Capture Plus .....	70
Barcode Input .....	72
Enabled .....	72
Scanner Selection .....	72
Hardware Trigger .....	72
Auto Switch to Default on Event .....	73
Configure Scanner Settings .....	73
Decoders .....	73
Decoder Params .....	75
UPC EAN Params .....	82
Reader Params .....	84
Scan Params .....	87
UDI Params .....	88
Basic Multibarcodes params .....	88
Keep enabled on suspend .....	88
Voice Input .....	88
Intent Output .....	90
Intent Overview .....	91
IP Output .....	92
Usage .....	93
Using IP Output with IPWedge .....	94
Using IP Output without IPWedge .....	95
Generating Advanced Data Formatting Rules .....	96
Configuring ADF Plug-in .....	96
Creating a Rule .....	96
Defining a Rule .....	97
Defining Criteria .....	97
Defining an Action .....	98
Deleting a Rule .....	99
Order Rules List .....	99
Deleting an Action .....	100

ADF Example .....	100
DataWedge Settings .....	104
Importing a Configuration File .....	104
Exporting a Configuration File .....	105
Importing a Profile File .....	105
Exporting a Profile .....	105
Restoring DataWedge .....	105
Configuration and Profile File Management .....	106
Enterprise Folder .....	106
Auto Import .....	106
Programming Notes .....	106
Overriding Trigger Key in an Application .....	106
Capture Data and Taking a Photo in the Same Application .....	106
Disable DataWedge on Device .....	107
DataWedge APIs .....	107
Reporting .....	107
Soft Scan Trigger .....	107
Function Prototype .....	107
Parameters .....	107
Scanner Input Plugin .....	108
Function Prototype .....	108
Parameters .....	108
Return Values .....	108
Example .....	109
Comments .....	109
Enumerate Scanners .....	109
Function Prototype .....	109
Parameters .....	110
Return Values .....	110
Example .....	111
Comments .....	111
Set Default Profile .....	112
Default Profile Recap .....	112
Usage Scenario .....	112
Function Prototype .....	112
Parameters .....	112
Return Values .....	112
Example .....	113
Comments .....	113
Reset Default Profile .....	113
Function Prototype .....	114
Parameters .....	114
Return Values .....	114
Example .....	114

Comments .....	114
Switch To Profile .....	115
Profiles Recap .....	115
Usage Scenario .....	115
Function Prototype .....	115
Parameters .....	115
Return Values .....	116
Example .....	116
Comments .....	116
Notes .....	117
<b>Application Deployment.....</b>	<b>118</b>
Introduction .....	118
Security .....	118
Secure Certificates .....	118
Installing a Secure Certificate .....	118
Configuring Credential Storage Settings .....	119
Development Tools .....	119
Development Workstation .....	119
Target Device .....	120
EMDK for Android .....	120
StageNow .....	120
ADB USB Setup .....	120
Enabling USB Debugging .....	121
Entering Android Recovery Manually .....	121
Application Installation .....	122
Installing Applications Using the USB Connection .....	122
Installing Applications Using the Android Debug Bridge .....	123
Uninstalling an Application .....	124
Performing a System Update .....	124
Downloading the System Update Package .....	124
Using ADB .....	125
Verify System Update Installation .....	126
Performing an Enterprise Reset .....	126
Downloading the Enterprise Reset Package .....	126
Using ADB .....	126
Performing a Factory Reset .....	127
Downloading the Factory Reset Package .....	127
Using ADB .....	127
Storage .....	128
Random Access Memory .....	128
Internal Storage .....	129



## Table of Contents

Enterprise Folder .....	130
App Management .....	130
Viewing App Details .....	131
Managing Downloads .....	132
<b>Maintenance and Troubleshooting .....</b>	<b>133</b>
Introduction .....	133
Maintaining the Device .....	133
Battery Safety Guidelines .....	133
Cleaning Instructions .....	134
Approved Cleanser Active Ingredients .....	134
Harmful Ingredients .....	134
Device Cleaning Instructions .....	135
Special Cleaning Notes .....	135
Cleaning Materials Required .....	135
Cleaning Frequency .....	135
Cleaning the Device .....	135
Housing .....	135
Display .....	135
Exit Window .....	136
Cleaning Cradle Connectors .....	136
Troubleshooting .....	136
EC30 .....	136
2-Slot Charge Only Cradle .....	138
10-Slot Charge Only Cradle .....	139
10-Slot SmartLock Charge Only Cradle .....	140
<b>Technical Specifications .....</b>	<b>141</b>
EC30 .....	141
Decode Distances .....	143
I/O Connector Pin-Outs .....	144
2-Slot Charge Only Cradle Technical Specifications .....	144
10-Slot Charge Only Cradle Technical Specifications .....	145
10-Slot SmartLock Charge Only Cradle Technical Specifications .....	146

# About This Guide

## Introduction

This guide provides information about using the EC30 Enterprise Companion and accessories.



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

## Documentation Set

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

- EC30 Enterprise Companion Quick Start Guide - describes how to get the device up and running.
- EC30 Enterprise Companion User Guide for Android 8.1 Oreo - describes how to use the device.
- EC30 Enterprise Companion Integrator Guide for Android 8.1 Oreo - describes how to set up the device and accessories.

## Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
EC30	WLAN: 802.11 a/b/g/n/ac/d/h /i/k/r/w WPAN: Bluetooth v5.0 Low Energy	3.0" Full Wide Video Graphics Array (854 x 480)	4 GB RAM / 32 GB Flash	2D imager (SE-2100)	Android-based, Google™ Mobile Services (GMS) 8.1. Android-based AOSP 8.1.

## Software Versions

To determine the current software versions:

1. Swipe down from the Status bar to open the Quick Settings bar.
2. Touch > **System**.

3. Touch **About phone**.
4. Scroll to view the following information:
  - **Model**
  - **Android version**
  - **Android security patch version**
  - **Kernel version**
  - **Build number**.

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

- **Serial number**

## Chapter Descriptions

Topics covered in this guide are as follows:

- [Getting Started](#) provides information on getting the device up and running for the first time.
- [Accessories](#) describes the available accessories and how to use them with the device.
- [USB Communication](#) describes how to connect the device to a host computer using USB.
- [DataWedge](#) describes how to use and configure the DataWedge application.
- [Settings](#) provides the settings for configuring the device.
- [USB Communication](#) provides information for transferring files between the device and a host computer.
- [Application Deployment](#) provides information for developing and managing applications.
- [Maintenance and Troubleshooting](#) includes instructions on cleaning and storing the device, and provides troubleshooting solutions for potential problems during device operation.
- [Technical Specifications](#) provides the technical specifications for the device.

## Notational Conventions

The following conventions are used in this document:

- **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 (for example, those that describe step-by-step procedures) appear as numbered lists.

## Related Documents

- EC30 Enterprise Companion Quick Start Guide, p/n MN-003607-xx.
- EC30 Enterprise Companion Regulatory Guide, p/n MN-003604-xx.
- EC30 Enterprise Companion Accessory Regulatory Guide, p/n MN-003609-xx.
- EC30 Enterprise Companion User Guide for Android 8.1.0 Oreo, p/n MN-003653-xx.
- RS507 Hands-free Imager Product Reference Guide, p/n 72E-12082-xx.
- DS36X8 Product Reference Guide, p/n MN-002689-xx.
- RS6000 User Guide, MN-002704-xx.

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

## Service Information

If you have a problem with your equipment, contact Customer Support for your region. Contact information is available at: [www.zebra.com/support](http://www.zebra.com/support).

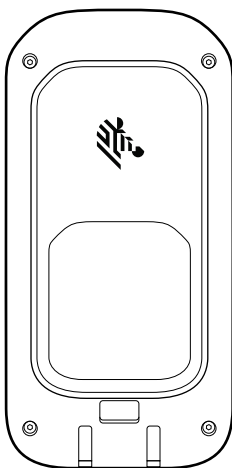
When contacting support, please have the following information available:

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

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

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

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



# Getting Started

## Introduction

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

## Setup

To start using the device for the first time charge the device to at least 30% capacity.



**NOTE:** When the device is shipped from the factory, it is placed into Ship Mode, where the device enters its lowest possible power state. The device can exit Ship Mode by docking it in a powered cradle or attaching a powered USB cable.

## Charging the Device



**IMPORTANT:** Do not store the device for extended periods of time as the battery may drain completely and become unrecoverable.

Use one of the following accessories to charge the EC30.

Table 1 Charging Accessories

Description	Part Number
<b>Cradles</b>	
2-Slot Charge Only Cradle	CRD-EC30-2SCHG1-01
10-Slot Charge Only Cradle	CRD-EC30-10SC1-01
10-Slot Charge Only Locking Cradle	CRD-EC30-10SLC1-01
<b>Charge and Communication Cables</b>	
USB-C Charging Cable 1.5 m (4.92 ft)	CBL-TC2X-USBC-01
USB-C Charging Cable 1 m (3.28 ft)	CBL-TC5X-USBC2A-01



**NOTE:** Ensure that you follow the guidelines for battery safety described in the EC30 Integrator Guide.

To charge the battery:

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

## Charging Temperature

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

## Charging Indicators

*Table 2 Charging LED Status Indicators*

State	Indication
Off	Device is not charging. Device is not inserted correctly in the cradle or connected to a power source. Charger or cradle is not powered.
Slow Blinking Amber (1 blink every 4 seconds)	Device is charging.
Slow Blinking Red (1 blink every 4 seconds)	Device is charging but the battery is at end of useful life.
Solid Green	Charging complete.
Solid Red	Charging complete but the battery is at end of useful life.
Fast Blinking Amber (2 blinks/second)	Charging error, for example: <ul style="list-style-type: none"> <li>• Temperature is too low or too high.</li> <li>• Charging has gone on too long without completion (typically eight hours).</li> </ul>
Fast Blinking Red (2 blinks/second)	Charging error but the battery is at end of useful life., for example: <ul style="list-style-type: none"> <li>• Temperature is too low or too high.</li> <li>• Charging has gone on too long without completion (typically eight hours).</li> </ul>

## Resetting the Device

The reset functions include the following:

- Soft reset
- Hard reset
- Enterprise reset
- 

## Performing a Soft Reset

Perform a soft reset if applications stop working.

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

2. Touch **Restart**.

The device reboots.

## Performing a Hard Reset

Perform a hard reset if the device stops responding.

1. Simultaneously press the Power and Volume Up buttons for at least five seconds.
2. When the screen turns off, release the buttons.

The device reboots.

# Accessories

## Introduction

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

## Accessories

This table lists the accessories available for the device.

**Table 3** *Accessories*

Accessory	Part Number	Description
<b>Cradles</b>		
2-Slot Charge Only Cradle	CRD-EC30-2SCHG1-01	Provides device charging. Use with power supply, p/n PWR-BGA12V50W0WW.
10-Slot Charge Only Cradle	CRD-EC30-10SC1-01	Charges up to 10 devices. Use with power supply, p/n PWR-BGA12V108W0WW and DC line cord, p/n CBL-DC-381A1-01.
10-Slot Charge Only Locking Cradle	CRD-EC30-10SLC1-01	Charges up to 10 devices. Use with power supply, p/n PWR-BGA12V108W0WW and DC line cord, p/n CBL-DC-381A1-01.
Cradle Mount	BRKT-SCRD-SMRK-01	Mounts the 10-Slot Charge Only Cradle and 10-Slot Charge Only Locking Cradle to a rack.
Cradle Mount Plate	BRKT-EC30-10SC1-01	Mounts the 10-Slot Charge Only Cradle and 10-Slot Charge Only Locking Cradle to a rack with the displays facing up.
<b>Charge and Communication Cables</b>		
USB-C Charging Cable	CBL-TC2X-USBC-01	Provides device charging and USB communication with a host computer.
USB-C Charging Cable	CBL-TC5X-USBC2A-01	Provides device charging and USB communication with a host computer.
<b>Audio Accessories</b>		
Bluetooth Headset	HS3100-OTH	Rugged Bluetooth Headset. Includes HS3100 Boom Module and HSX100 OTH Headband Module.



**Table 3** Accessories (Continued)

Accessory	Part Number	Description
3.5 mm Headset	HDST-35MM-PTT1-01	Use for PTT and VoIP calls.
3.5 mm Headset	HDST-35MM-PTVP-01	Use headset for PTT and VoIP calls.
3.5 mm Quick Disconnect Adapter Cable	CBL-TC51-HDST35-01	Adapter provides connection to the 3.5 mm Headset.
<b>Carrying Solutions</b>		
Basic Lanyard	SG-EC30-BLYD1-01	EC30 basic lanyard with adjustable neck strap and adapter (1-pack).
Basic Lanyard	SG-EC30-BLYD1-10	EC30 basic lanyard with adjustable neck strap and adapter (10-pack).
Retractable Lanyard	SG-EC30-RLYD1-01	EC30 retractable lanyard with magnetic recoil, adjustable neck strap, and adapter (1-pack).
Retractable Lanyard	SG-EC30-RLYD1-10	EC30 retractable lanyard with magnetic recoil, adjustable neck strap, and adapter (10-pack).
Soft Holster	SG-EC30-HLSTR1-01	EC30 soft holster.
Rigid Holster	SG-EC30-RHLSTR1-01	EC30 rigid holster with rotating belt clip.
Garment Clip	SG-EC30-CLIP1-01	EC30 vest/garment clip with coiled tether and adapter.
Belt Clip	SG-EC30-RCB1-01	EC30 retractor with magnetic recoil, carabiner, and adapter.
Arm Mount Adapter	SG-EC30-ARM1-01	EC30 arm mount adapter (standard strap size).
Arm Mount Adapter	SG-EC30-ARML1-01	EC30 arm mount adapter (long strap size).
Screen Protector	SG-EC30-SCRNP1-05	Provides additional protection for the screen (5-pack).
<b>Power Supplies</b>		
Power Supply	PWR-BGA12V50W0WW	Provides power to the 2-Slot cradle. Requires DC Line Cord, p/n CBL-DC-388A1-01 and country specific three wire grounded AC line cord sold separately.
Power Supply	PWR-BGA12V108W0WW	Provides power to the 10-Slot Charge Only cradle and the 10-Slot Locking Cradle. Requires DC Line Cord, p/n CBL-DC-381A1-01 and country specific three wire grounded AC line cord sold separately.
Power Supply	PWR-WUA5V12W0US	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with US plug.

**Table 3** *Accessories (Continued)*

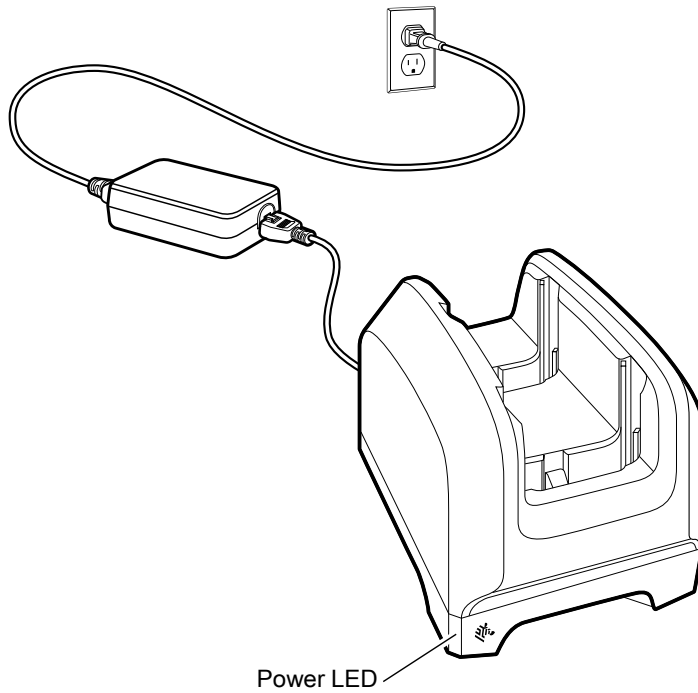
Accessory	Part Number	Description
Power Supply	PWR-WUA5V12W0GB	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with Great Britain plug.
Power Supply	PWR-WUA5V12W0EU	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with Europe plug.
Power Supply	PWR-WUA5V12W0AU	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with Australia plug.
Power Supply	PWR-WUA5V12W0CN	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with China plug.
Power Supply	PWR-WUA5V12W0BR	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with Brazil plug.
Power Supply	PWR-WUA5V12W0KR	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with Korea plug.
Power Supply	PWR-WUA5V12W0IN	Provides power to the EC30. Requires USB-C Charging Cable. Power Supply-100-240 VAC, 5 V, 2.5 A with India plug.
DC Line Cord	CBL-DC-388A1-01	Provides power from the power supply to the 2-Slot cradle.
DC Line Cord	CBL-DC-381A1-01	Provides power from the power supply to the 10-Slot Charge Only Cradle and 10-Slot Locking Cradle.

## 2-Slot Charge Only Cradle

The 2-Slot Charge Only Cradle:

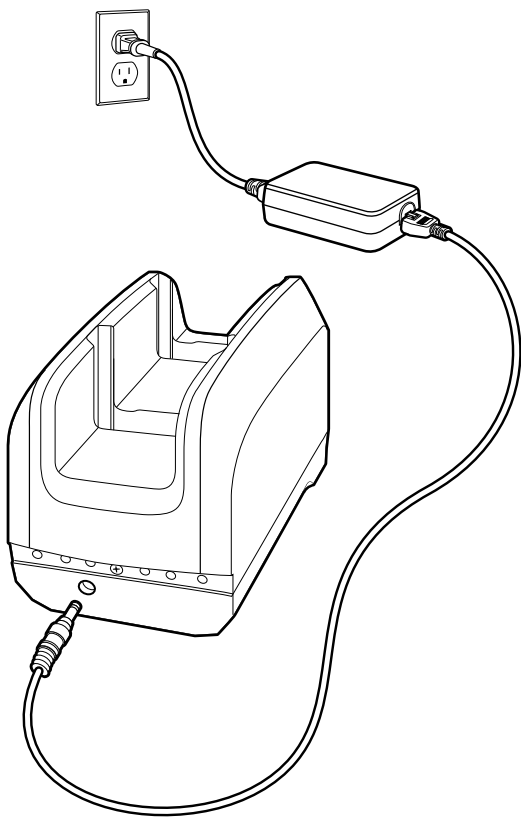
- Provides 5 VDC power for operating the device.
- Simultaneously charges up to two devices.

**Figure 1** 2-Slot Charge Only Cradle



## Setup

**Figure 2** 2-Slot Charge Only Cradle

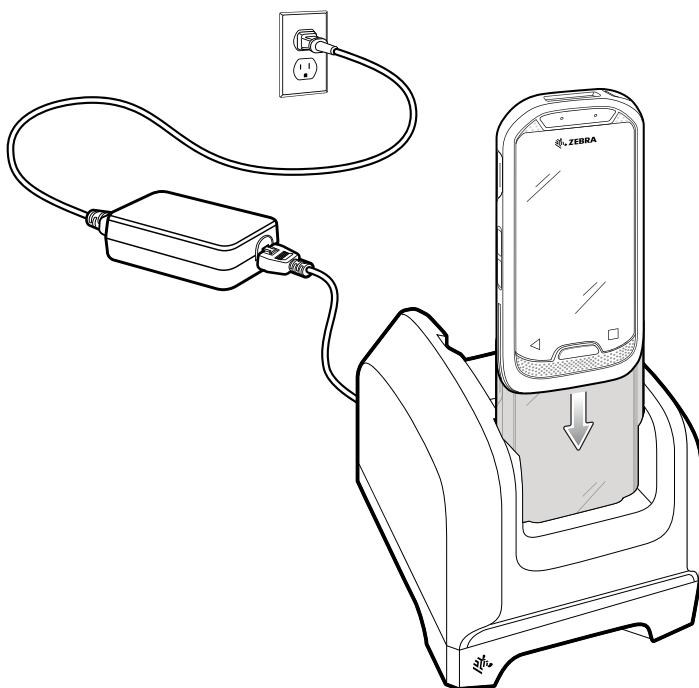


## Charging the Device

To charge a device:

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

**Figure 3** Battery Charging



2. Ensure the device is seated properly.

## Charging Status

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

The 1,200 mAh (typical) / 1,100 mAh (minimum) battery charges from fully depleted to 90% in approximately 2.5 hours, and from fully depleted to 100% in approximately three hours.

## Charging Temperature

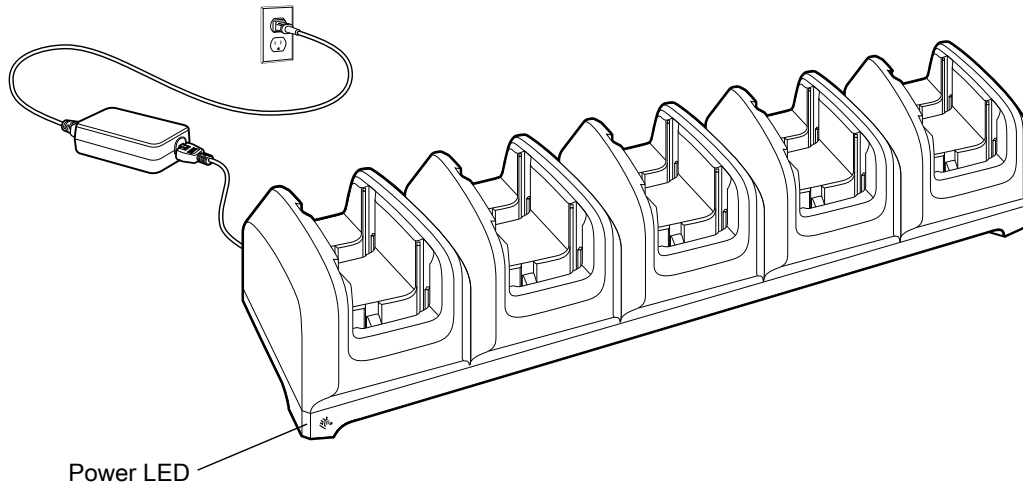
Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (for example, approximately +37 °C (+98 °F)) the device or cradle may for small periods of time alternately enable and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

## 10-Slot Charge Only Cradle

The 10-Slot Charge Only Cradle:

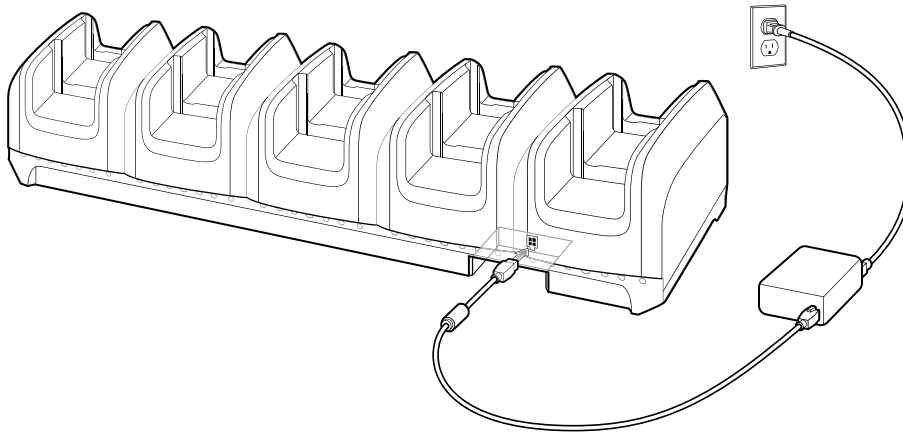
- Provides 5 VDC power for operating the device.
- Simultaneously charges up to ten devices.

**Figure 4** 10-Slot Charge Only Cradle



## Setup

**Figure 5** 10-Slot Charge Only Cradle

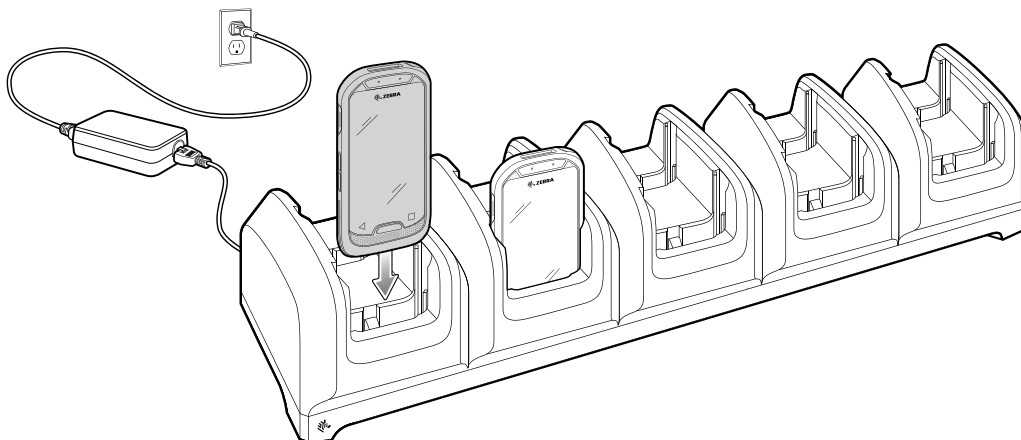


## Charging the Device

To charge a device:

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

**Figure 6** Device Battery Charging



2. Ensure the device is seated properly.

## Charging Status

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

The 1,200 mAh (typical) / 1,100 mAh (minimum) battery charges from fully depleted to 90% in approximately 2.5 hours and from fully depleted to 100% in approximately three hours.

## Charging Temperature

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

## 10-Slot Locking Charge Only Cradle

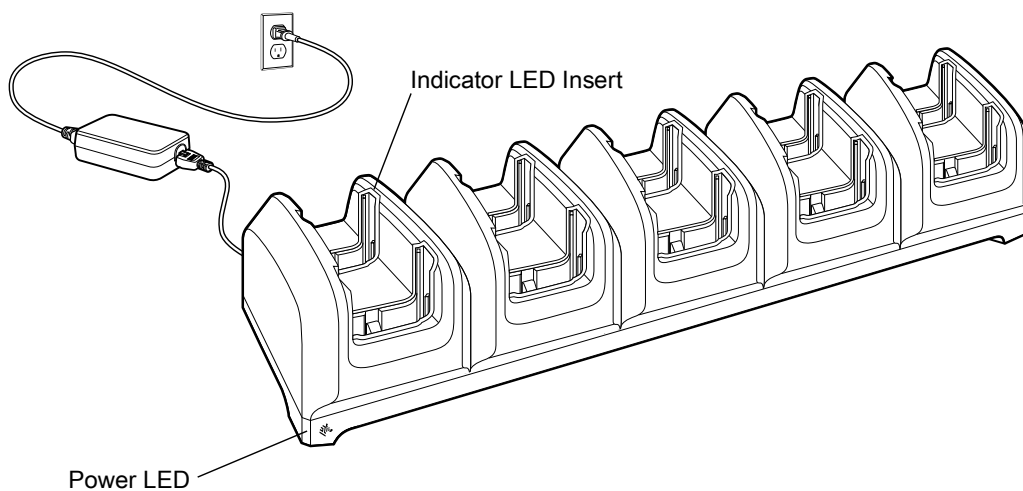


**NOTE:** Controlling the locking cradle is done through a software API. For more information, go to [techdocs.zebra.com](https://techdocs.zebra.com).

The 10-Slot Locking Charge Only Cradle:

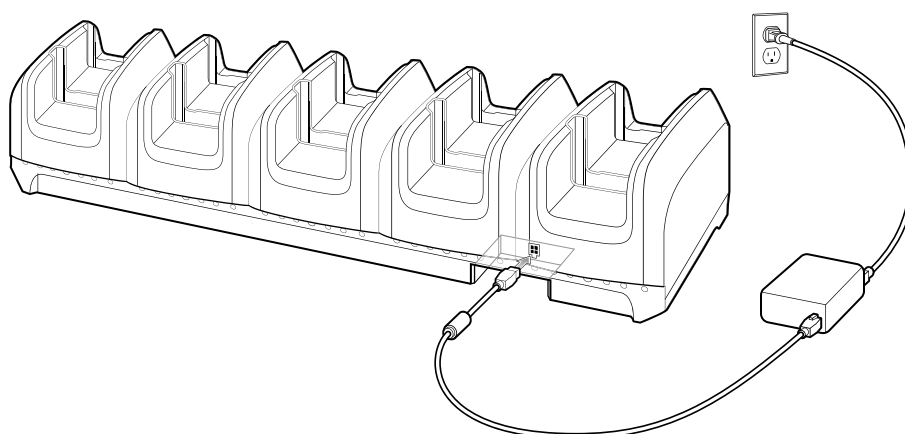
- Provides 5 VDC for operating the cradle.
- Simultaneously charges up to ten devices.
- Each slot contains an Indicator LED Insert with RGB LEDs.

**Figure 7** 10-Slot Locking Charge Only Cradle



## Setup

**Figure 8** 10-Slot Locking Charge Only Cradle



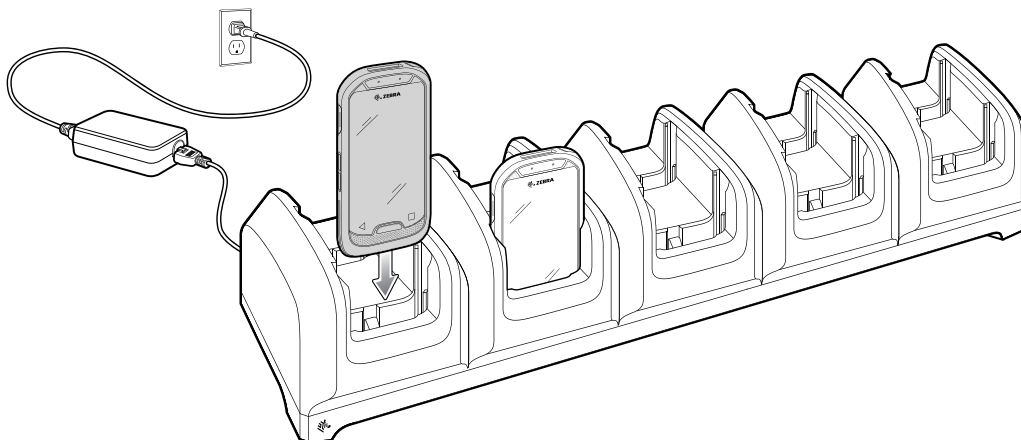


## Charging the Device

To charge a device:

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

**Figure 9** Device Battery Charging



2. Ensure the device is seated properly.

## Manual Release Using a Release Key

The EC30 10-Slot Locking Charge Only Cradle contains a locking mechanism that locks the EC30 inside the cradle when docked. If the EC30 fails to unlock during normal operation, use a release key (KT-MC18-CKEY-20) to unlock the EC30.

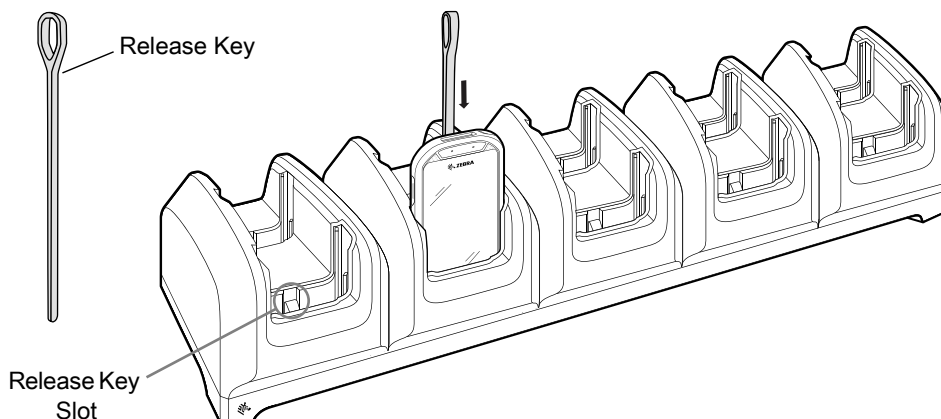


**CAUTION:** Do not use any device to unlock the cradle other than the tools described below. Failure to comply could result in damage to the cradle and void the warranty.

To release a locked device:

1. Insert the release key straight into the slot as shown below.
2. While pressing the release key all the way into the slot, remove the device from the cradle.

**Figure 10** Manual Release of the EC30



## Charging Status

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

The 1,200 mAh (typical) / 1,100 mAh (minimum) battery charges from fully depleted to 90% in approximately 2.5 hours and from fully depleted to 100% in approximately three hours.

## Charging Temperature

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

## 10-Slot Cradle Rack Installation

Use the Rack/Wall Mount Bracket to mount a 10-slot cradle on a rack. When installing on a rack, first assemble the bracket and cradles/chargers and then install the assembly on the rack.

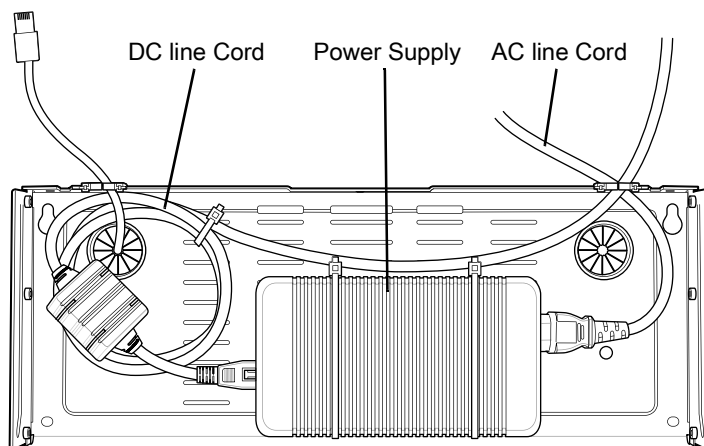
1. Place the power supply in bottom tray.
2. Connect AC line cord to power supply.
3. Connect DC line cord to power supply.
4. Secure power supply and cables to bottom tray with tie wraps.



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

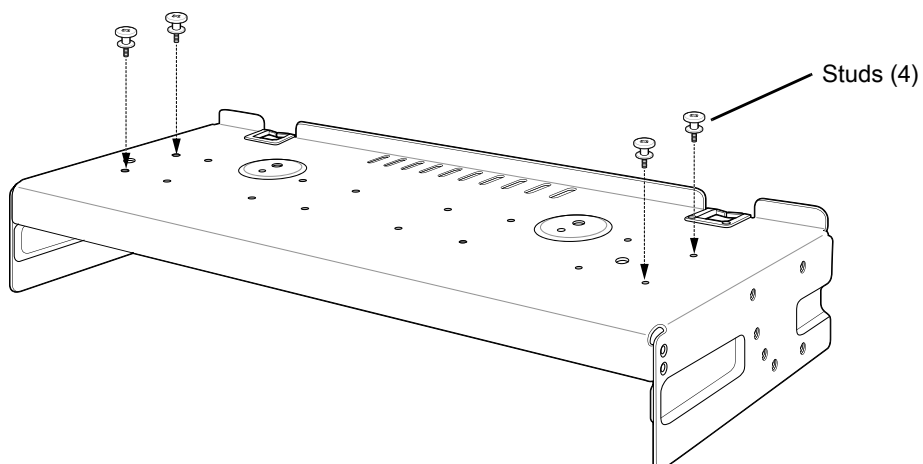
5. Route cables through cable slots.

**Figure 11** Power Supply in Bottom Tray



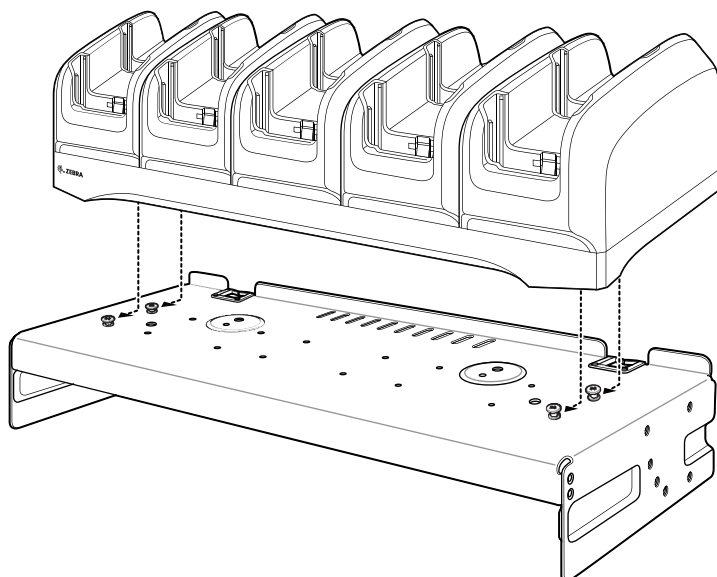
- Secure four M2.5 studs to the top tray as shown.

**Figure 12** Install Studs



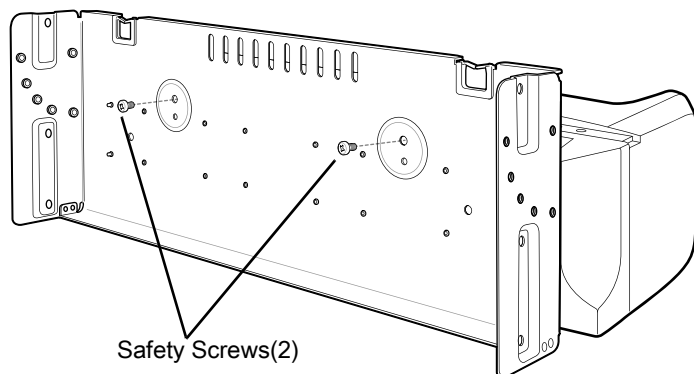
- Align and install 10-Slot cradle onto studs of the top tray.

**Figure 13** Align Cradle on Studs



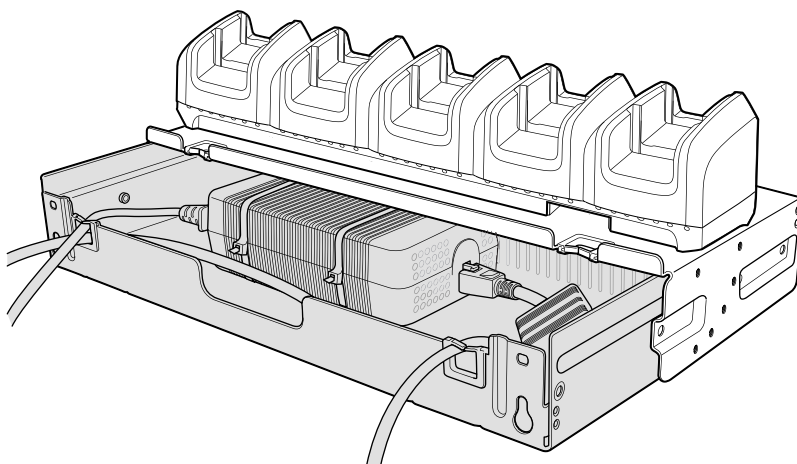
- Secure cradle to the top tray with two M2.5 safety screws.

**Figure 14** Secure Cradle



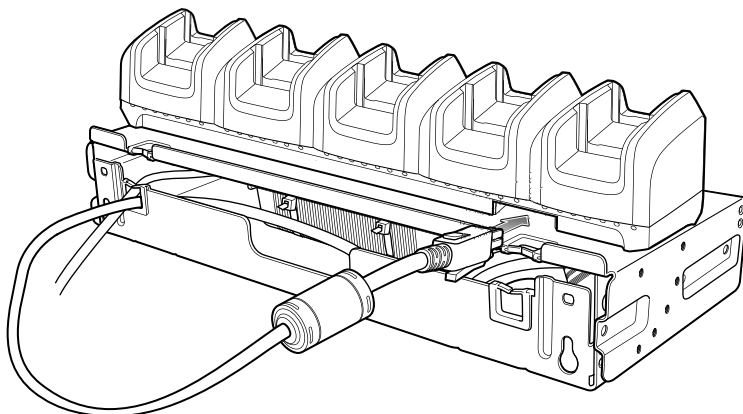
- Slide the top tray onto the bottom tray.

**Figure 15** Slide Top Tray onto Bottom Tray



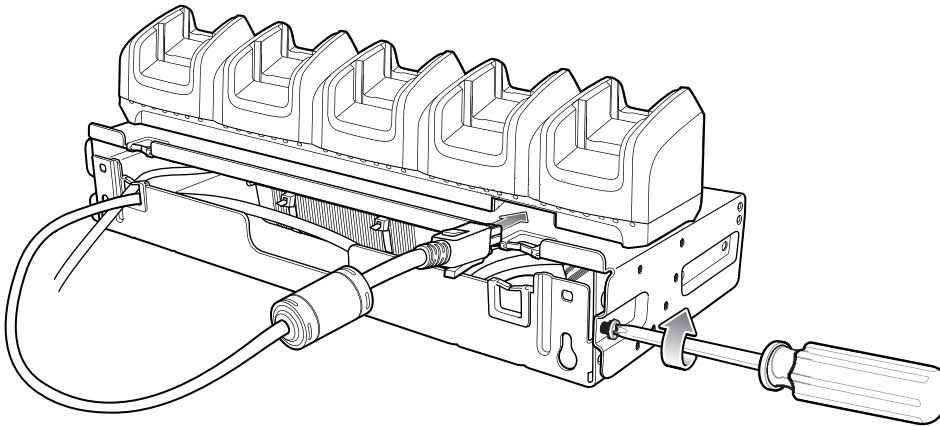
- Connect cables to the cradle.

**Figure 16** Connect Cables



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

**Figure 17** Secure Top and Bottom Tray



See [Rack Mount Installation on page 29](#) for installing the bracket assembly onto a rack.

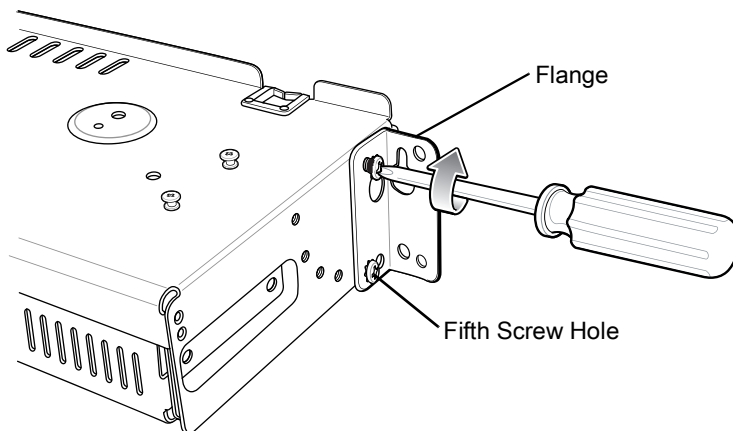
## Rack Mount Installation



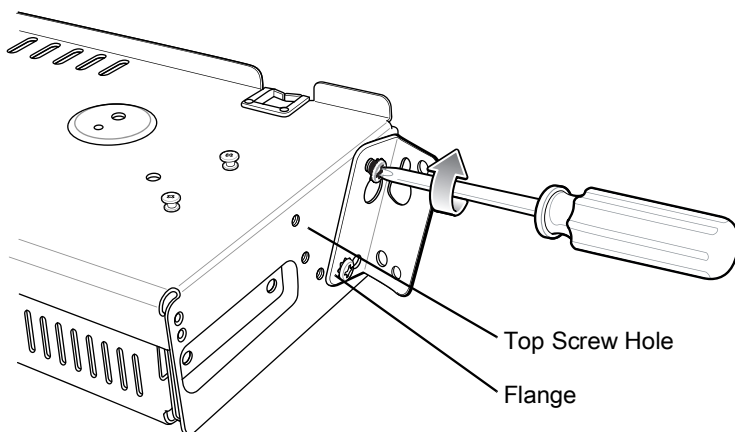
**NOTE:** Use screws provided with rack system. Refer to rack user documentation for instructions.

1. Secure mounting brackets to both sides of the top tray with four M5 screws (two on each side).

**Figure 18** Flange Horizontal Position



**Figure 19** Flange 25° Position



**CAUTION:** Install mounting bracket with 10-Slot cradle at a maximum height of four feet from the ground.

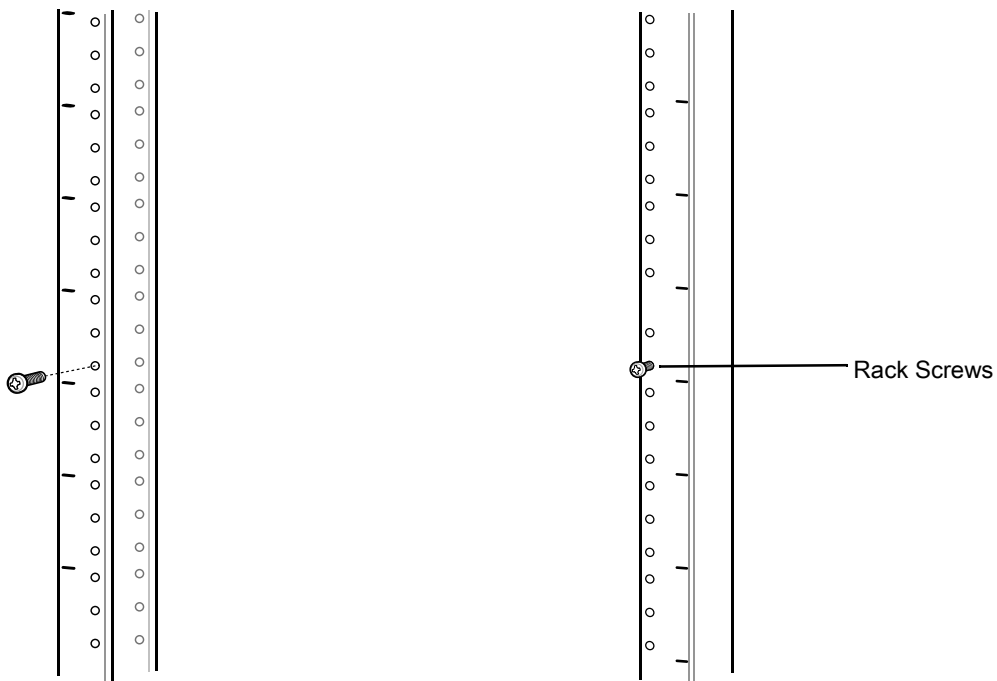


**NOTE:** Distance between two horizontal mounted brackets should be at least 14.5" apart (from top of one flange to the top of the next flange).

Distance between two 25° mounted brackets should be at least 12" apart (from top of one flange to the top of the next flange).

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

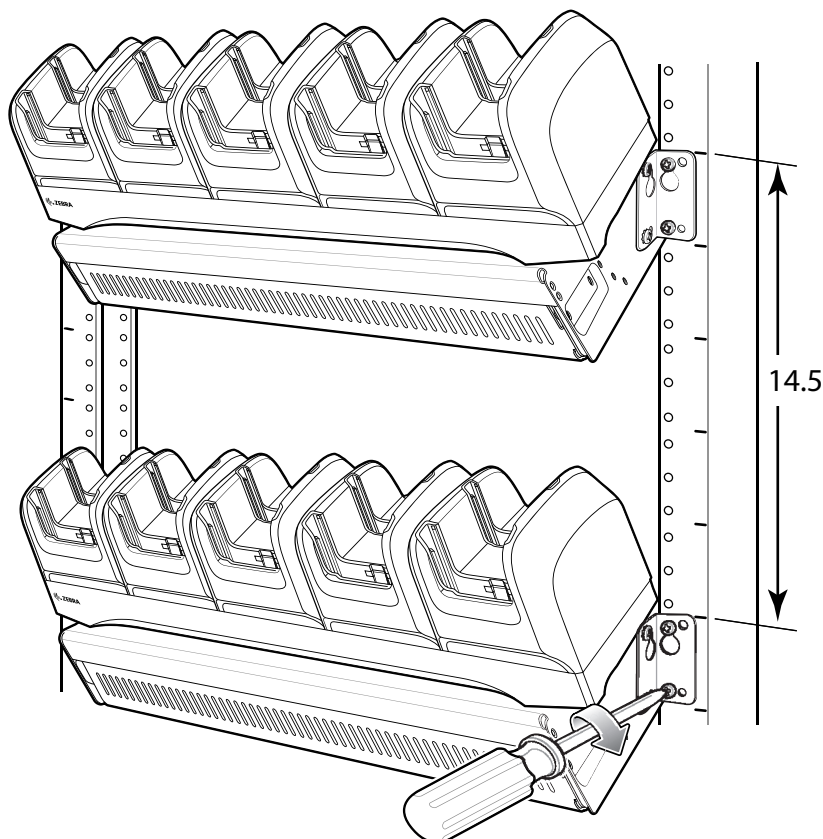
**Figure 20** Install Rack System Screws



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

- Place the brackets on the screws.

**Figure 21** Secure Bracket to Rack (Horizontal Position Shown)



- Secure the top screws.
- Install bottom screws and tighten screws.
- Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

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

## Wall Installation

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

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

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



**CAUTION:** Install mounting bracket with 10-Slot cradle at a maximum height of four feet from the ground.

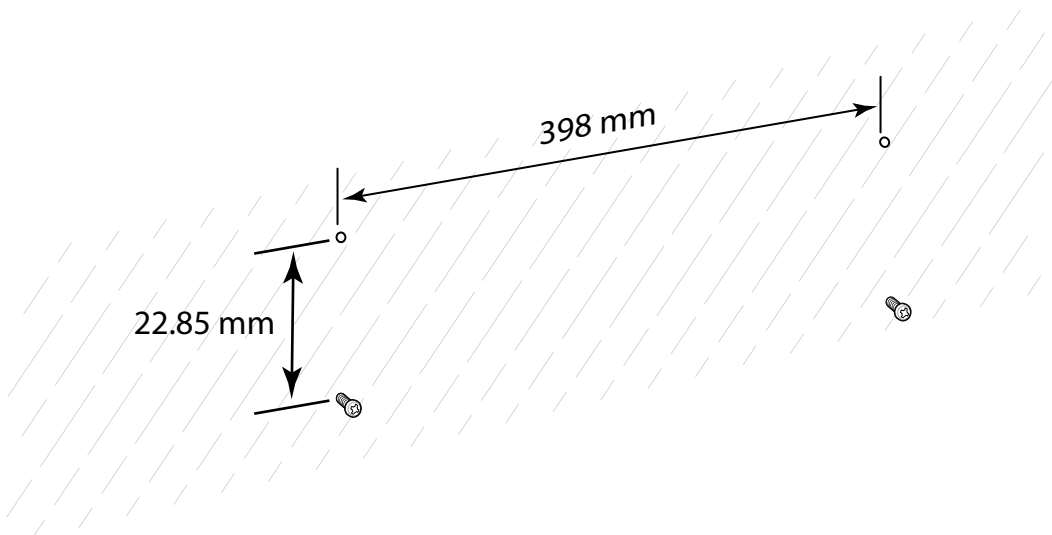
## Bottom Tray Assembly

See steps 1 through 5 on [page 26](#) for instructions.

## Bracket Wall Mounting

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

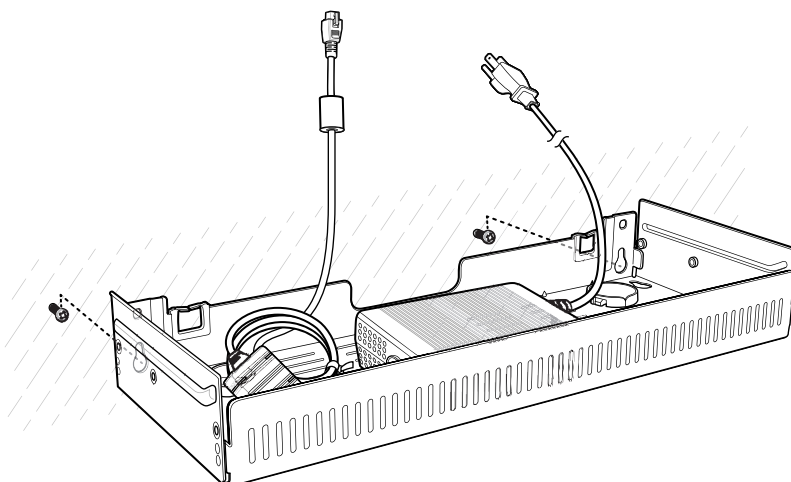
**Figure 22** Horizontal Mounting Template



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



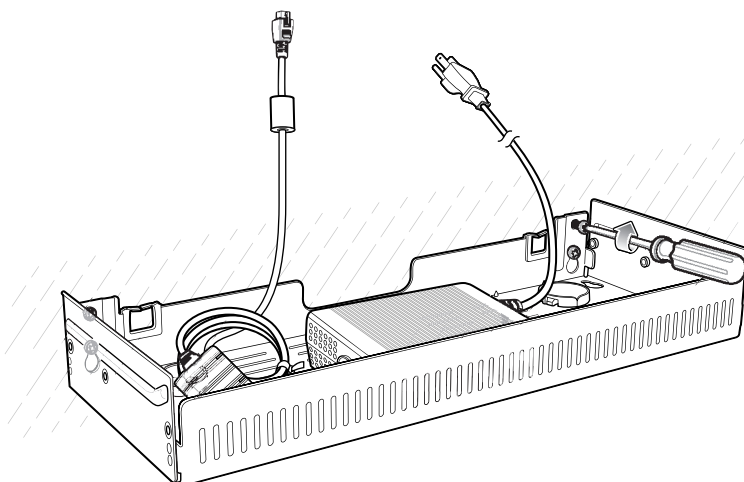
**Figure 23** Horizontal Installation



5. Install two top screws.

6. Tighten all screws.

**Figure 24** Horizontal Installation - Tighten Screws



7. Assembly the cradle onto the bracket. See steps 7 through 11 on [page 27](#).

8. Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

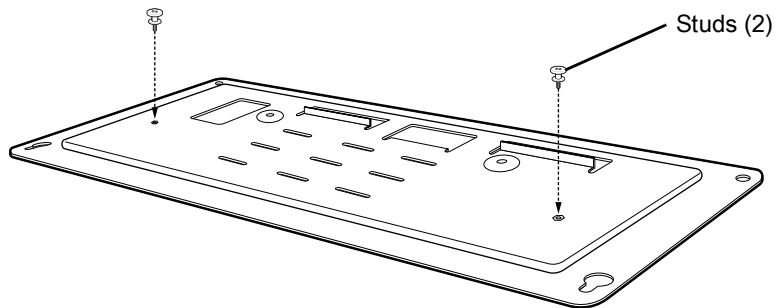
- Use tie wraps to secure cables to the bracket and rails.
- Coil cables wherever possible.
- Route power cables along the rails.
- Route inter-cradle cables to the side rails and then from the rails to the bracket.

## Rack Mount Plate Installation

Use the Rack/Wall Mount Plate to mount a 10-slot cradle on a rack. When installing on a rack, first assemble the plate and cradle, and then install the assembly on the rack.

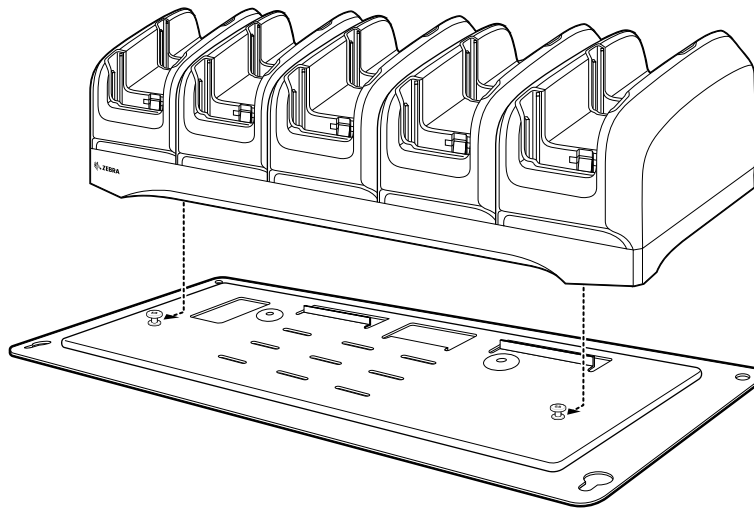
1. Secure two M2.5 studs to the top tray as shown.

**Figure 25** Install Studs



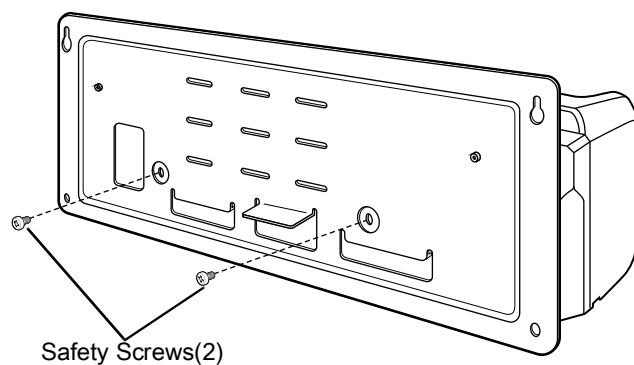
2. Align and install 10-Slot cradle onto studs of plate.

**Figure 26** Align Cradle on Studs



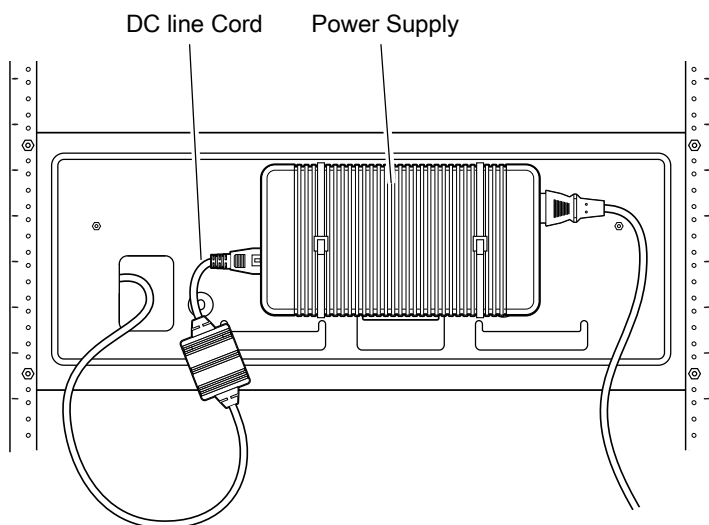
3. Secure cradle to the top tray with two M2.5 safety screws.

**Figure 27** Secure Cradle



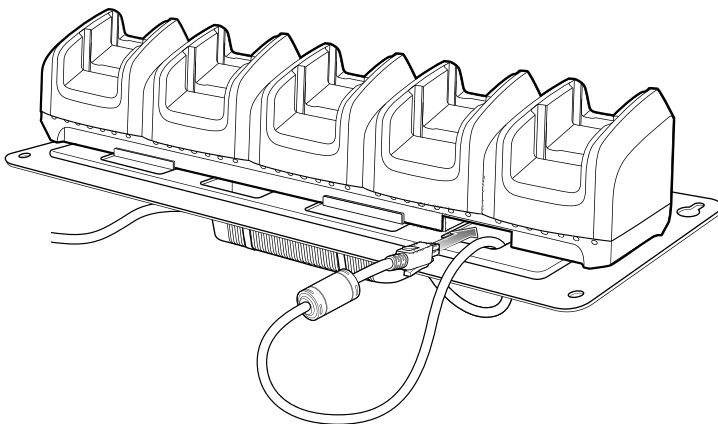
4. Place the power supply on the tray shelf.
5. Connect AC line cord to power supply.
6. Connect DC line cord to power supply.
7. Secure power supply and cables to tray with tie wraps.
8. Route DC line cord through cable slot.

**Figure 28** Power Supply on Tray Shelf



9. Connect cable to cradle.

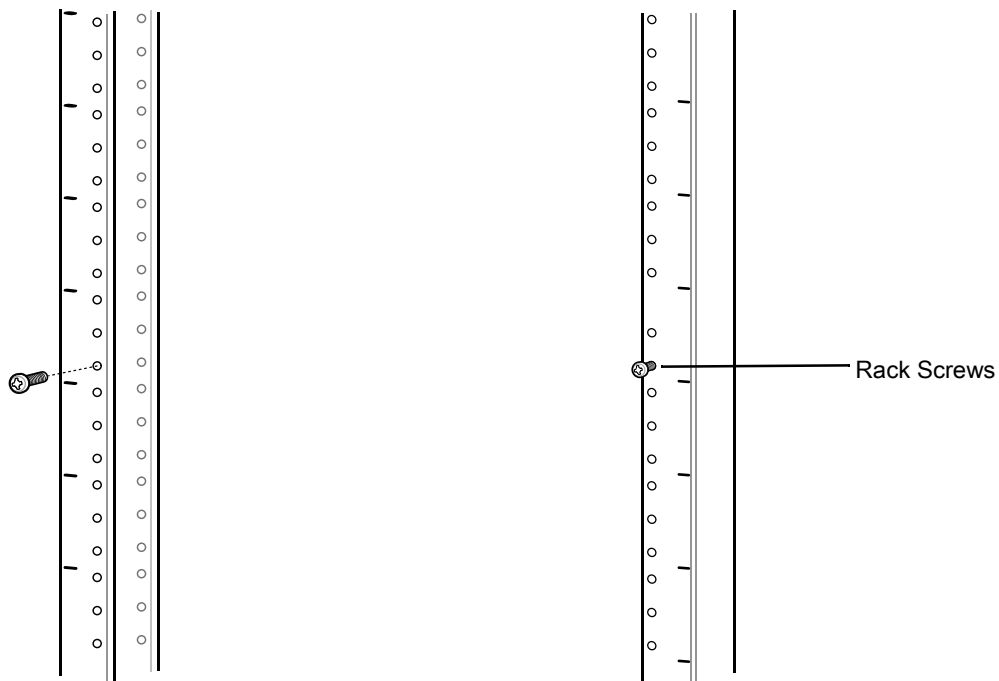
**Figure 29** Connect Cable



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

10. Install two screws for top of the mounting plate. The screw heads should protrude half way from the rail.

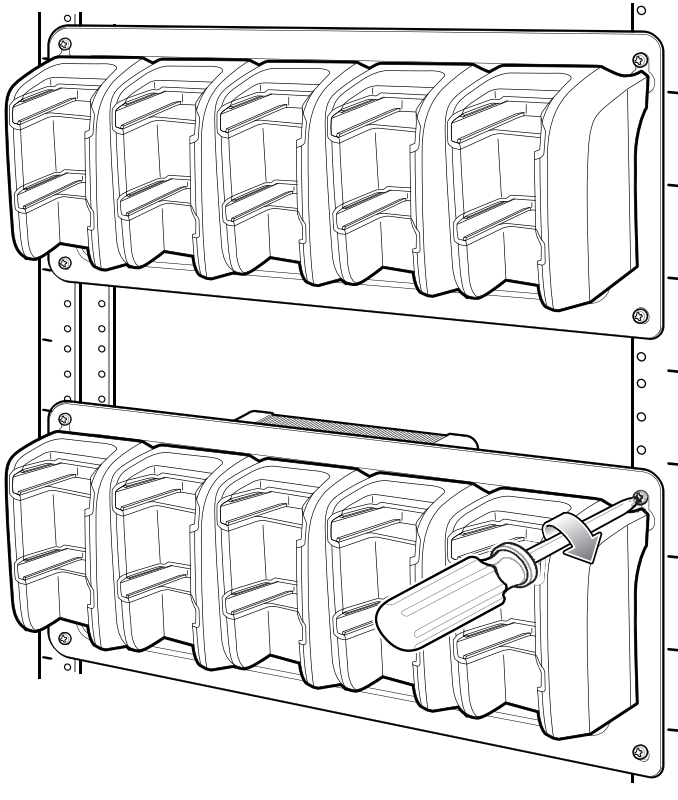
**Figure 30** Install Rack System Screws



11. Align the mounting plate's top mounting key holes with the screws.

12. Hang the bracket on the screws.

**Figure 31** Secure Plate to Rack



13. Install two bottom screws.

14. Tighten all screws.

15. Route cables and connect to power source.



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

While installing the brackets, power supplies and cables:

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

# Settings

## Introduction


This chapter describes settings available for configuring the device.

## WLAN Configuration

This section provides information on configuring Wi-Fi settings.

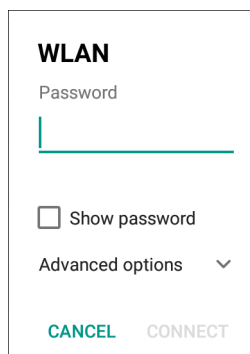
### Configuring a Secure Wi-Fi Network

To set up a Wi-Fi network:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Network & Internet > Wi-Fi**.
3. Slide the switch to the **ON** position.
4. The device searches for WLANs in the area and lists them on the screen.
5. Scroll through the list and select the desired WLAN network.

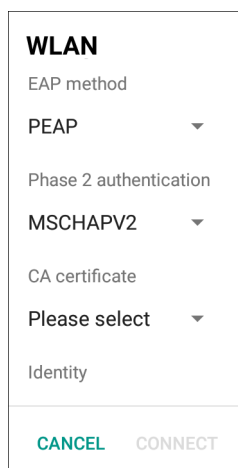
6. Touch the desired network. If the network security is **Open**, the device automatically connects to the network. For all other network security a dialog box appears.

**Figure 32** WLAN WEP Network Security Dialog Box



The dialog box is titled "WLAN". It contains a "Password" label followed by a text input field with a green underline. Below the input field is a checkbox labeled "Show password". Underneath the checkbox is a label "Advanced options" with a downward-pointing chevron. At the bottom of the dialog are two buttons: "CANCEL" in teal and "CONNECT" in gray.

**Figure 33** WLAN 802.11 EAP Network Security Dialog Box



The dialog box is titled "WLAN". It contains several fields: "EAP method" with a dropdown menu showing "PEAP"; "Phase 2 authentication" with a dropdown menu showing "MSCHAPV2"; "CA certificate" with a dropdown menu showing "Please select"; and "Identity" with a text input field. At the bottom of the dialog are two buttons: "CANCEL" in teal and "CONNECT" in gray.

7. If the network security is **WEP** or **WPA/WPS2 PSK**, enter the required password and then touch **Connect**.
8. If the network security is 802.1x EAP:
- Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **TTLS**, or **LEAP**.
  - Touch the **Phase 2 authentication** drop-down list and select an authentication method.
  - If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
  - If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the Location & security settings.
  - If required, in the **Identity** text box, enter the username credentials.
  - If desired, in the **Anonymous identity** text box, enter an anonymous identity username.
  - If required, in the **Password** text box, enter the password for then given identity.




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

9. Touch **Connect**.

10. Touch .


## Manually Adding a Wi-Fi Network

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

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Network & Internet > Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Scroll to the bottom of the list and select **Add network**.
5. In the **Network name** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, set the type of security to:
  - **None**
  - **WEP**
  - **WPA/WPA2 PSK**
  - **802.1x EAP**.
7. If the network security is **None**, touch **Save**.
8. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password, and then touch **Save**.
9. If the network security is **802.1x EAP**:
  - Touch the **EAP method** drop-down list and select **PEAP, TLS, or TTLS, PWD, or LEAP**.
  - Touch the **Phase 2 authentication** drop-down list and select an authentication method.
  - If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
  - If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the **Security** settings.
  - If required, in the **Identity** text box, enter the username credentials.
  - If desired, in the **Anonymous** identity text box, enter an anonymous identity username.
  - If required, in the **Password** text box, enter the password for the given identity.



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

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


## Configuring for a Proxy Server

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

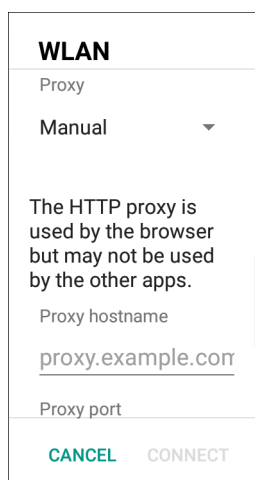


It is important for enterprise customers to be able to set up secure computing environments within their companies, making proxy configuration essential. Proxy configuration acts as a security barrier ensuring that the proxy server monitors all traffic between the Internet and the intranet. This is normally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

To configure the device for a proxy server:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Network & Internet > Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. Touch **Advanced options**.
6. Touch **Proxy** and select **Manual**.

**Figure 34** Proxy Settings



**WLAN**

Proxy

Manual ▼


The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

proxy.example.com

Proxy port


CANCEL CONNECT

7. In the **Proxy hostname** text box, enter the address of the proxy server.
8. In the **Proxy port** text box, enter the port number for the proxy server.
9. In the **Bypass proxy for** text box, enter addresses for web sites that are not required to go through the proxy server. Use a comma “,” between addresses. Do not use spaces or carriage returns between addresses.
10. Touch **Connect**.
11. Touch .

## Configuring the Device to Use a Static IP Address

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

To configure the device to connect to a network using a static IP address:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Network & Internet > Wi-Fi**.

3. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. Touch **Advanced options**.
6. Touch **IP settings** and select **Static**.

**Figure 35** Static IP Settings

**WLAN**

IP settings

Static ▼

IP address

192.168.1.128

Gateway

192.168.1.1

Network prefix length

CANCEL CONNECT

7. In the **IP address** text box, enter an IP address for the device.
8. If required, in the **Gateway** text box, enter a gateway address for the device.
9. If required, in the **Network prefix length** text box, enter the prefix length.
10. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
11. If required, in the **DNS 2** text box, enter a DNS address.
12. Touch **Connect**.
13. Touch ☐.

## Wi-Fi Preferences

Use the **Wi-Fi preferences** to configure advanced Wi-Fi settings. From the Wi-Fi screen scroll down to the bottom of the screen and touch **Wi-Fi preferences**.

- **Open network notification** - When enabled, notifies the user when an open network is available.
- **Advanced - Touch to expand options.**
  - **Additional settings** - See Additional Settings.
  - **Install Certificates** - Touch to install certificates.
  - **Network rating provider** - Disabled (AOSP devices). To help determine what constitutes a good Wi-Fi network, Android supports external Network rating providers that provide information about the quality of

open Wi-Fi networks. Select one of the providers listed or **None**. If none are available or selected, the Connect to open networks feature is disabled.

- **Wi-Fi Direct** - Displays a list of devices available for a direct Wi-Fi connection.
- **WPS Push Button** - Touch to connect to a network using Wi-Fi Protected Setup (WPS) push button method.
- **WPS Pin Entry** - Touch to connect to a network using Wi-Fi Protected Setup (WPS) pin entry method.
- **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **IP address** - Displays the IP address of the device when connecting to Wi-Fi networks.

## Additional Wi-Fi Settings



**NOTE:** Additional Wi-Fi settings are for the device, not for a specific wireless network.

Use the **Additional Settings** to configure additional Wi-Fi settings. To view the additional Wi-Fi settings, scroll to the bottom of the **Wi-Fi** screen and touch **Wi-Fi Preferences > Advanced > Additional settings**.

- **Regulatory**
  - **Country Selection** - Displays the acquired country code if 802.11d is enabled, else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Set the frequency band to: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
  - **Available channels (2.4 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
  - **Available channels (5 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
- **Logging**
  - **Advanced Logging** – Touch to enable advanced logging or change the log directory.
  - **Wireless logs** - Use to capture Wi-Fi log files.
    - **Fusion Logger** - Touch to open the **Fusion Logger** application. This application maintains a history of high level WLAN events which helps to understand the status of connectivity.
    - **Fusion Status** - Touch to display live status of WLAN state. Also provides information about the device and connected profile.
- **About**
  - **Version** - Displays the current Fusion information.

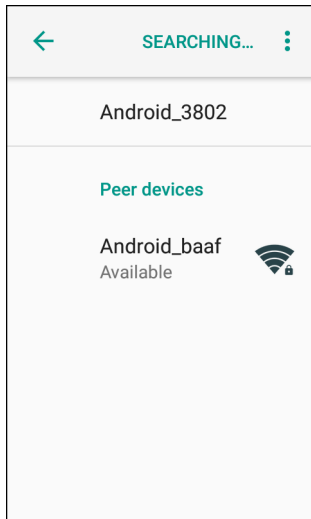
## Wi-Fi Direct

Wi-Fi Direct devices can connect to each other without having to go through an access point. Wi-Fi Direct devices establish their own ad-hoc network when required, letting you see which devices are available and choose which one you want to connect to.

1. Swipe down from the status bar and then touch .

2. Touch **Wi-Fi > Wi-Fi preferences > Advanced > Wi-Fi Direct**. The device begins searching for another Wi-Fi Direct device.

**Figure 36** Wi-Fi Direct Screen



3. Under **Peer devices**, touch the other device name.
4. On the other device, select **Accept**.
5. **Connected** appears on the device. On both devices, in their respective Wi-Fi Direct screens, the other device name appears in the list.

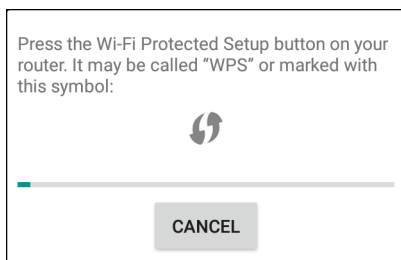
## WPS Push Button

Wi-Fi Protected Setup (WPS) is a feature allowing devices to easily connect to Wi-Fi access points without typing a long password.

To use a wireless router WPS button:

1. On the device, swipe down from the status bar and then touch **⚙**.
2. Touch **Wi-Fi > Wi-Fi preferences > Advanced > WPS Push Button**. A dialog box displays.

**Figure 37** WPS Setup Dialog Box




3. On the wireless router, locate the WPS button. The device connects to the wireless router.

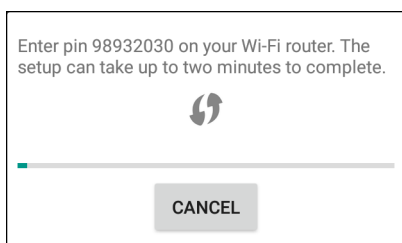
## WPS Pin Entry

Wi-Fi Protected Setup (WPS) is a feature allowing devices to easily connect to Wi-Fi access points without typing a long password.

To use a PIN to connect to a wireless router:

1. Log in to the router.
2. Go to the Add WPS Client screen. Refer to the wireless router user documentation specific information.
3. On the device, swipe down from the status bar, and then touch .
4. Touch **Wi-Fi > Wi-Fi preferences > Advanced > WPS Pin Entry**. A dialog box displays with an Pin number.


**Figure 38** Pin Entry Dialog Box



5. On the router, enter the Pin number. The device connects to the wireless router.

## Setting Screen Lock

Use the **Device security** settings to set preferences for locking the screen.

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Security & location**.



**NOTE:** Options vary depending upon the policy of some apps, such as email.

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

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


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

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

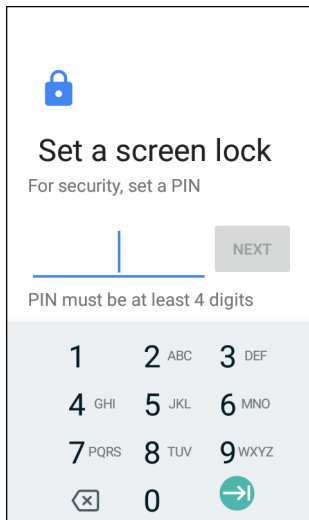
Slide the screen up to unlock. If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.


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

## Setting Screen Lock Using PIN


1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. To require a PIN upon device start up select **Yes**, or select **No** not to require a PIN.

**Figure 39** PIN Screen



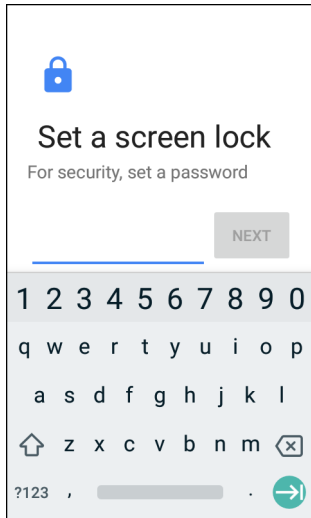
6. Touch in the text field.
7. Enter a PIN (4 numbers), and then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch . The next time the device goes into suspend mode a PIN is required upon waking.

## Setting Screen Unlock Using Password

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Password**.


5. To require a password upon device start up select **Yes**, or select **No** not to require a password.
6. Touch in the text field.
7. Enter a password (between 4 and 16 characters), and then touch **Next**.

**Figure 40** Password Screen



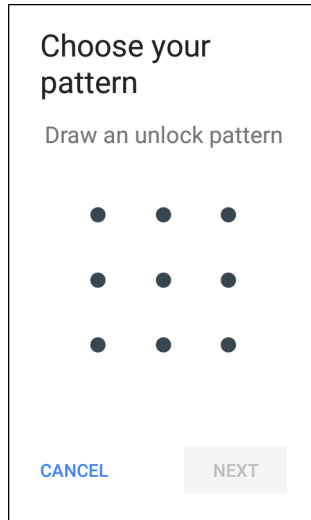
8. Re-enter the password and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch ☐. The next time the device goes into suspend mode a password is required upon waking.

## Setting Screen Unlock Using Pattern

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Pattern**.

5. To require a pattern upon device start up select **Yes**, or select **No** not to require a pattern.


**Figure 41** Choose Your Pattern Screen



6. Draw a pattern connecting at least four dots.
7. Touch **Continue**.
8. Re-draw the pattern.
9. Touch **Confirm**.
10. Select the type of notifications that appear when the screen is locked, and then touch **Done**.
11. Touch ☐. The next time the device goes into suspend mode a pattern is required upon waking.

## Showing Passwords

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


1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Slide the **Show passwords** switch to the ON position.

## Remapping a Button

Buttons on the device can be programmed to perform different functions or as shortcuts to installed apps.



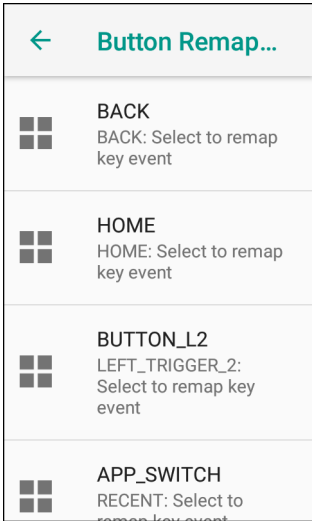
**NOTE:** It is not recommended to remap the scan button.

1. Swipe down from the Status bar to open the Quick Access panel and then touch .



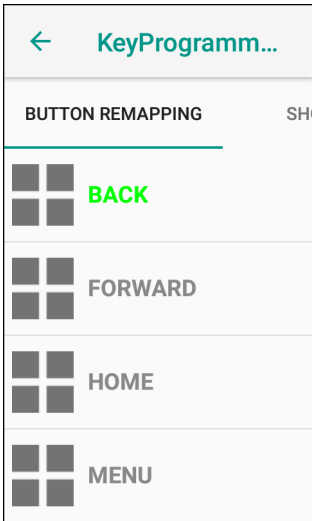
- 2. Touch **Key Programmer**. A list of programmable buttons displays.

Figure 42 Button Remap Program Screen



- 3. Select the button to remap.

Figure 43 KeyProgrammer Screen



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



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

- 6. Touch ○.

## Accounts



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

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



## Language Usage

Use the **Language & input** settings to change the device's language, including words added to the dictionary.

### Changing the Language Setting

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > Languages & input**.
3. Touch **Languages**. A list of available languages displays.
4. If the desired language is not listed, touch **Add a language** and select a language from the list.
5. Touch and hold  to the right of the desired language, then drag it to the top of the list.
6. The operating system text changes to the selected language.

### Adding Words to the Dictionary

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > Languages & input > Advanced > Personal dictionary**.
3. If prompted, select the language where this word or phrase is stored.
4. Touch **+** to add a new word or phrase to the dictionary.
5. Enter the word or phrase.
6. In the **Shortcut** text box, enter a shortcut for the word or phrase.
7. Touch .

## Keyboard Settings

Use the **Languages & input** settings to configure the on-screen keyboards. The device contains the following keyboard settings:

- Android Keyboard - Non-GMS devices only.
- Gboard - GMS devices only.
- Enterprise Keyboard - Not pre-installed on the device. Contact Zebra Support for more information.

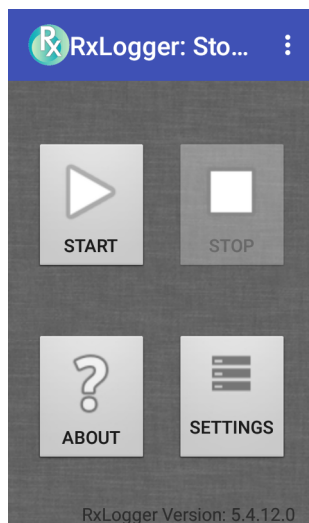
## PTT Express Configuration

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

## RxLogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics, allows for the creation of custom plug-ins, and diagnoses device and application issues. RxLogger logs the following information: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging, cellular logging, TCP dumps, Bluetooth logging, GPS logging, logcat, FTP push/pull, ANR dumps, etc. All generated logs and files are saved onto flash storage on the device (internal or external).

**Figure 44** RxLogger



## RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plug-ins already built-in. The included plug-ins are described below.

To open the configuration screen, from the RxLogger home screen touch **Settings**.

**Figure 45** RxLogger Configuration Screen

SAVE	CANCEL
RxLogger Settings	
ANRModule	
KernelModule	
LogcatModule	
LTSMModule	
RamoopsModule	
ResourceModule	

## RxLogger Settings

The RxLogger Settings module provides additional RxLogger settings.

- **Enable notifications** - Select to allow RxLogger notifications in the Status bar and Notification panel.
- **Enable debug logs** - Select to enable debug logs.

### ANR Module

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

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the default log path to store the ANR log files.
- **Collect Historic ANRs** - Collects ANR trace files from the system.

### Kernel Module

The Kernel Module captures kmsg from the system.

- **Enable Module** - Enables logging for this kernel module.
- **Log path** - Specifies the high level log path for storage of all kernel logs. This setting applies globally to all kernel buffers.
- **Kernel Log filename** - Specifies the base log filename for this kernel buffer. The current file count is appended to this name.
- **Max Kernel log file size** - Specifies the maximum size, in megabytes, of an individual log file.
- **Kernel Log interval** - Sets the interval, in seconds, on which to flush the log buffer to the file.
- **Kernel Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Enable System Timestamp in Kernel Log** - Enables system timestamps in kernel logs.
- **System Timestamp Interval** - Sets the interval, in seconds, between system timestamps.

- **Enable Logcat Integration override** - Enables logcat integration overrides.

## Logcat Module

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

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.
- **Enable main logcat** - Enables logging for this logcat buffer.
  - **Main Log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Main Log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Main Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Main log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Main log filter** - Custom logcat filter to run on the main buffer.
- **Enable event logcat** - Enables event logging for this logcat buffer.
  - **Event log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Event log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Event log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Event log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Event log filter** - Custom logcat filter to run on the event buffer.
- **Enable radio logcat** - Enables logging for this logcat buffer.
  - **Radio log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Radio log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Radio log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Radio log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Radio log filter** - Custom logcat filter to run on the radio buffer.
- **Enable system logcat** - Enables logging for this logcat buffer.
  - **System log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **System log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **System log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **System log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **System log filter** - Custom logcat filter to run on the system buffer.

- **Enable crash logcat** - Enables logging for this crash logcat buffer.
  - **Crash log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Crash log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Crash log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Crash log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Crash log filter** - Custom logcat filter to run on the crash buffer.
- **Enable combined logcat** - Enables logging for this logcat buffer.
  - **Enable main buffer** - Enable or disable the addition of the main buffer into the combined logcat file.
  - **Enable event buffer** - Enable or disable the addition of the event buffer into the combined logcat file.
  - **Enable radio buffer** - Enable or disable the addition of the radio buffer into the combined logcat file.
  - **Enable system buffer** - Enable or disable the addition of the system buffer into the combined logcat file.
  - **Enable crash buffer** - Enable or disable the addition of the crash buffer into the combined logcat file.
  - **Combine log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Combined log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Combined log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Combined log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Combined log filter** - Custom logcat filter to run on the combined buffer.

### LTS Module

The LTS (Long Term Storage) Module captures data over a long duration of time without losing any data. Whenever a file is done being written, LTS saves it as a GZ file in an organized path for later use.

- **Enable Module** - Enables logging for this module.
- **Storage Directory** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.

### Ramoops Module

The Ramoops Module captures the last kmsg from the device.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the high level log path for storage of all ramoops logs. This setting applies globally to all Ramoops buffers.
- **Base filename** - Specifies the base log filename for this kernel buffer. The current file count is appended to this name.
- **Ramoops file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the log size option.

### Resource Module

The Resource Module captures device information and system statistics at specified intervals. The data is used to determine the health of the device over a period of time.

- **Enable Module** - Enables logging for this module.

- **Log Path** - Specifies the high level log path for storage of all resource logs. This setting applies globally to all resource buffers.
- **Resource Log interval** - Sets the interval, in seconds, on which to flush the log buffer to the file.
- **Resource Log file size** - Specifies the maximum size, in megabytes, of an individual log file.
- **Resource Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Power** - Enables or disables the collection of Battery statistics.
- **System Resource** - Enables or disables the collection of System Resource information.
- **Network** - Enables or disables the collection of Network status.
- **Bluetooth** - Enables or disables the collection of Bluetooth information.
- **Light** - Enables or disables the collection of ambient light level.
- **Heater** - Not supported.

### Snapshot Module

The Snapshot Module collects detailed device statistics at an interval to see detailed device information.

- **Enable Module** - Enables logging for this module.
- **Log Path** - Specifies the base path to use to store the snapshot files
- **Log filename** - Specifies the base filename for all the snapshot files. The current file count is appended to this name.
- **Log Interval (sec)** - Specifies the interval, in seconds, on which to invoke a detailed snapshot.
- **Snapshot file count** - The maximum number of Snapshot files to keep at any one time.
- **Top** - Enables or disables the running of the **top** command for data collection.
- **CPU Info** - Enables detailed per process CPU logging in the snapshot.
- **Memory Info** - Enables logging of detailed per process memory usage in the snapshot.
- **Battery Info** - Enables logging of detailed power information including battery life, on time, charging, and wake locks.
- **Wake Locks** - Enables or disables the collection of the sys/fs wake\_lock information.
- **Time in State** - Enables or disables the collection of the sys/fs cpufreq for each core.
- **Processes** - Enables dumping the complete process list in the snapshot.
- **Threads** - Enables dumping all processes and their threads in the snapshot.
- **Properties** - Enables dumping of all system properties on the device. This includes build/version information as well as state information.
- **Interfaces** - Enables or disables the running of the **netcfg** command for data collection.
- **IP Routing Table** - Enables or disables the collection of the net route for data collection.
- **Connectivity** - Enables or disables the running of the **dumpsys connectivity** command for data collection.
- **Wifi** - Enables or disables the running of the **dumpsys wifi** command for data collection.
- **File systems** - Enables dumping of the available volumes on the file system and the free storage space for each.
- **Usage stats** - Enables dumping of detailed usage information for each package on the device. This includes the number of starts and duration of each run.

### TCPDump Module

The TCPDump Module captures TCP data that happens over the device's networks.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the location to store the TCPDump output log files.
- **Base filename** - Specifies the base filename to use when storing the TCPDump files. The index number of the current log file is appended to the filename.
- **Tcpdump file size (MB)** - Specifies the maximum file size, in megabytes, for each log file created.
- **Tcpdump file count** - Specifies the number of log files to cycle through when storing the network traces.

## Tombstone Module

The Tombstone Module collects tombstone (Linux Native Crashes) logs from the device.



- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the location to store the Tombstone output log files.
- **Collect Historic tombstones** - Collects new and existing tombstone files.

## Configuration File

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



## Enabling Logging

To enable logging:

1. Swipe the screen up and select .
2. Touch **Start**.
3. Touch .

## Disabling Logging

To disable logging:

1. Swipe the screen up and select .
2. Touch **Stop**.
3. Touch .

## Extracting Log Files

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



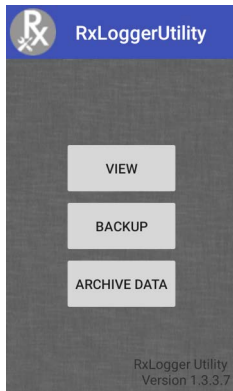
## RxLogger Utility

RxLogger Utility is a data monitoring application for viewing logs in the device while RxLogger is running. Logs and RxLogger Utility features are accessed in the App View or the Overlay View.

### App View

In App View, the user views logs in the RxLogger Utility.

**Figure 46** App View

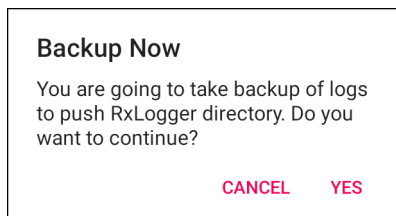


### Backup

RxLogger Utility allows the user to make a zip file of the **RxLogger** folder in the device, which by default contains all the RxLogger logs stored in the device.

To save the backup data, touch **BACKUP** > **Yes**.

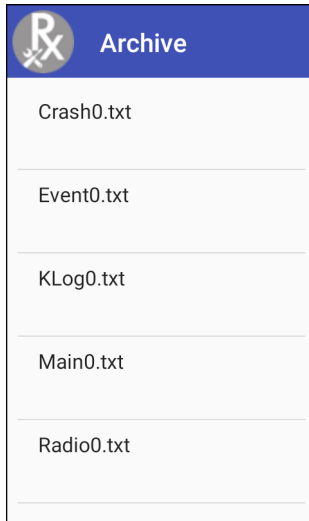
**Figure 47** Backup Message



## Archive Data

View all the RxLogger logs stored in the default **RxLogger** directory. Logs viewed in the Archive window are not live.

**Figure 48** Archive



To view the log files, touch **ARCHIVE DATA** and then touch a log file.

## Overlay View

Use Overlay View to display RxLogger information while using other apps or on the home screen. Overlay View is accessed using the Main Chat Head.

### Initiating the Main Chat Head

To initiate the Main Chat Head:

1. Open **RxLogger**.
2. Touch **⋮** > **Toggle Chat Head**. The Main Chat Head icon appears on the screen.
3. Touch and drag the Main Chat head icon to move it around the screen.

### Removing the Main Chat Head

To remove the Main Chat Head icon:

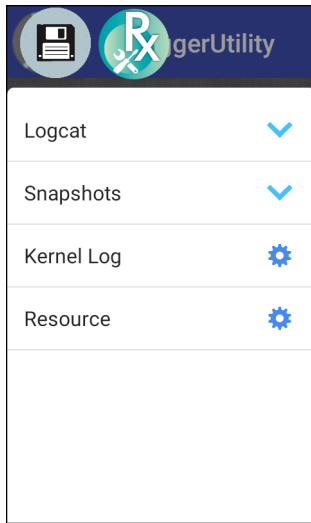
1. Touch and drag the icon. A circle with an X appears.
2. Move the icon over the circle and then release.

## Viewing Logs

To view logs:

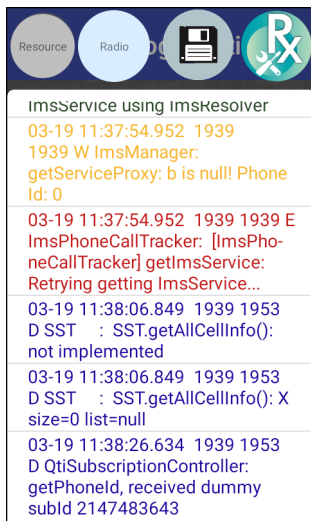
1. Touch the Main Chat Head icon. The Overlay View screen appears.

**Figure 49** Overlay View Screen



2. Touch a log to open it. The user can open many logs with each displaying a new sub Chat Head.
3. If necessary, scroll left or right to view additional Sub Chat Head icons.
4. Touch a Sub Chat Head to display the log contents.

**Figure 50** Log File




## Removing a Sub Chat Head Icon

To remove a sub chat Head icon, press and hold the icon until it disappears.


## Backing Up In Overlay View

RxLogger Utility allows the user to make a zip file of the **RxLogger** folder in the device, which by default contains all the RxLogger logs stored in the device.

The Backup icon is always available in Overlay View.

1. Touch . The Backup dialog box appears.
2. Touch **Yes** to create the back up.

## About

Use About phone settings to view information about the device. Swipe down from the Status bar to open the Quick Access panel and then touch  > **System** > **About phone**.

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

# USB Communication

## Introduction

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

## Transferring Files with a Host Computer via USB

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

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

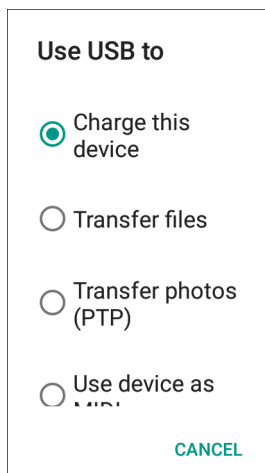
## Transferring Files



**NOTE:** Use Transfer files to copy files between the device (internal memory) and the host computer.

1. Connect a USB cable between the device and a host computer.
2. Pull down the Notification panel and touch **USB charging this device**.  
By default, **Charge this device** is selected.

**Figure 51** Use USB to Dialog Box



3. Touch **Transfer files**.

4. On the host computer, open a file explorer application.
5. Locate the **device** as a portable device.
6. Open the **Internal storage** folder.
7. Copy files to and from the device or delete files as required.

### Transferring Photos

To transfer photos using Photo Transfer Protocol:



**NOTE:** Use Photo Transfer Protocol (PTP) to copy photos from the internal memory to the host computer.

1. Connect USB cable to the device or place the device into a USB cradle. See [Accessories](#) for setup information.
2. Pull down the Notification panel and touch **USB charging this device**.
3. Touch **Transfer photos (PTP)**.
4. On the host computer, open a file explorer application.
5. Open the **Internal storage** folder.
6. Copy or delete photos as required.

### Disconnect from the Host Computer

To disconnect the device from the host computer:



**CAUTION:** Carefully follow the host computer's instructions to disconnect USB devices correctly to avoid losing information.

1. On the host computer, unmount the device.
2. Remove the USB cable from the device.

# DataWedge

## Introduction

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

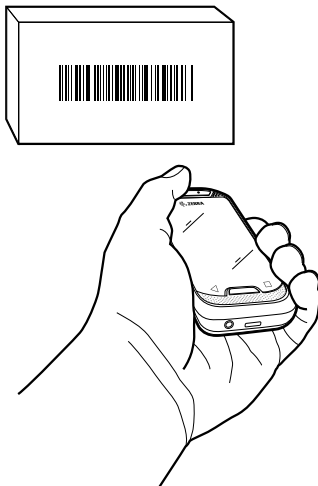
## Basic Scanning

To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the imager, decode the barcode data, and display the barcode content.

To scan with the internal imager:

1. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
2. Point the exit window on the top of the device at a barcode.
3. Press and hold the scan button. The white aiming pattern turns on to assist in aiming.

**Figure 52** Imager Scanning



4. Ensure the barcode is within the area formed by aiming pattern.

By default, the Data Capture LED lights green and a beep sounds to indicate the barcode was decoded successfully. The barcode content data displays in the text field.

## Profiles

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

Profile information consists of:

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

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

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

- Visible profiles:
  - **Profile0** - created automatically the first time DataWedge runs. Generic profile used when there are no user created profiles associated with an application.
  - **Launcher** - enables scanning when the Launcher is in foreground.
  - **DWDEMO** - provides support for the DWDEMO application.
  - **GpioCradleDemoProfile** - provides support for the Cradle Demo 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 the 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 barcode 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 barcode scanner contained in, or attached to the device. **DataWedge** contains base plug-ins for these input devices.

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

## Process Plug-ins

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


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

## Output Plug-ins

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

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

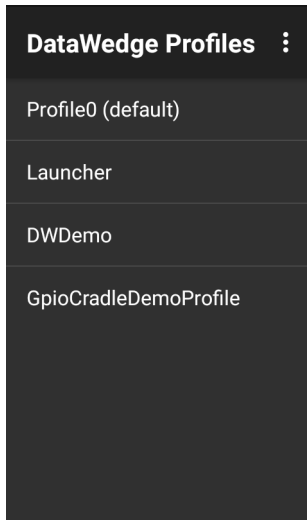
## Profiles Screen

To launch DataWedge, swipe up from the bottom of the screen and touch . By default, the following profiles appear:

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

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

**Figure 53** DataWedge Profiles Screen



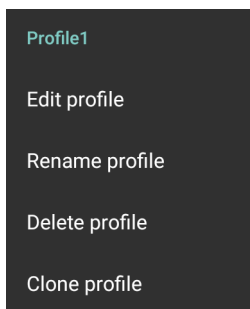
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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 54** Profile Context Menu

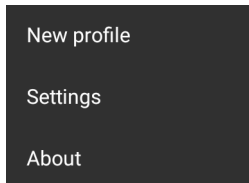


The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

## Options Menu


Touch  to open the options menu.

**Figure 55** DataWedge Options Menu



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


## Disabling DataWedge

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

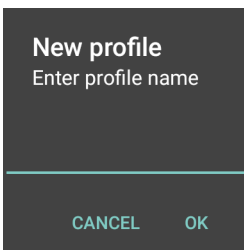
The blue check disappears from the checkbox indicating that DataWedge is disabled.

## Creating a New Profile

To create a new profile:

1. Touch .
2. Touch **New profile**.
3. 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 56** New Profile Name Dialog Box



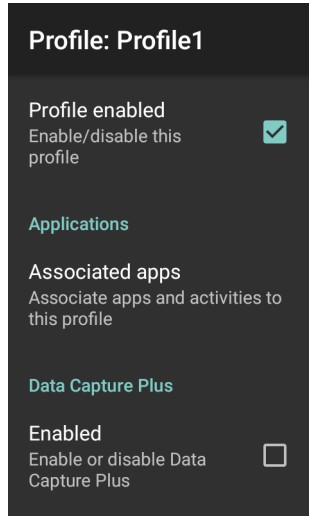
4. Touch **OK**.

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 57** Profile Configuration Screen



The configuration screen lists the following sections:

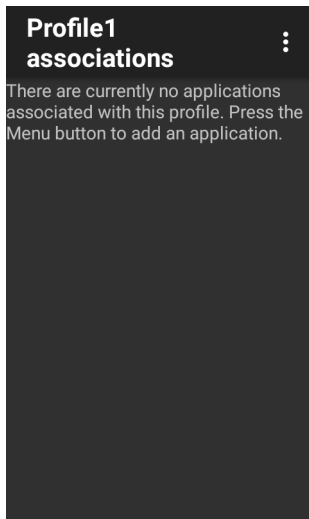
- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode Input
- Voice input
- Keystroke output
- Intent Output
- IP Output.

## 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.

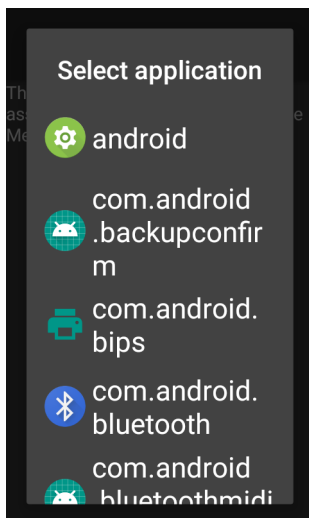
1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.

**Figure 58** Associated Apps Screen




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

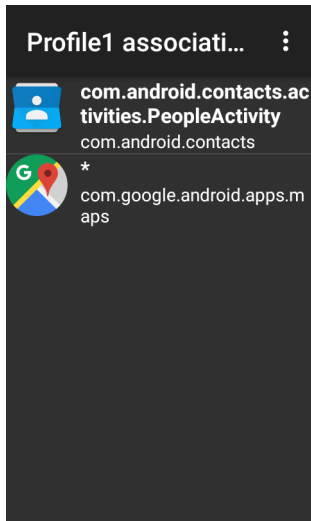
**Figure 59** Select Application Menu



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

6. Touch .

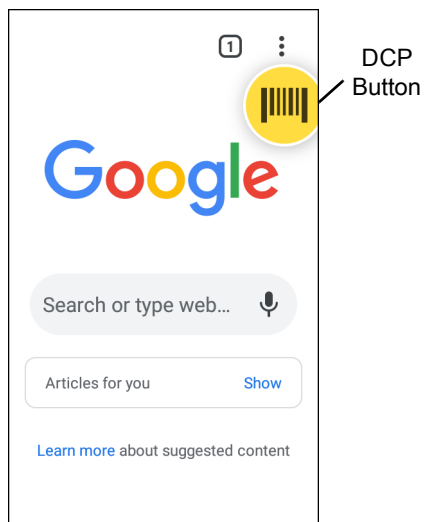
**Figure 60** Selected Application/Activity



## Data Capture Plus

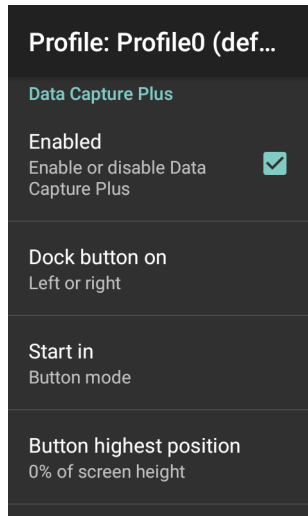
Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching a designated part of the screen. A variable screen overlay acts like a scan button.

**Figure 61** Minimized Data Capture Panel



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

**Figure 62** Data Capture Panel Settings



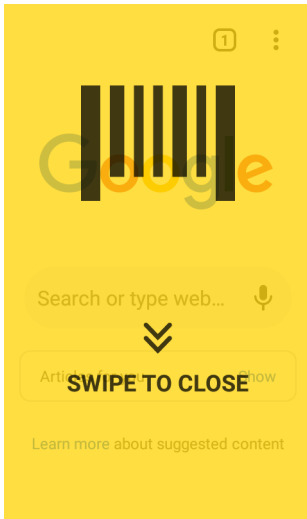
- **Enable** - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
  - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
  - **Left only** - Places the button on left edge of the screen.
  - **Right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



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

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

**Figure 63** Maximized DCP



Swipe down to return to button mode.

## Barcode Input

Use the **Barcode Input** options to configure the Barcode 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 barcode data capture when the profile is active. For Bluetooth scanners, if the device was not previously paired, a pairing barcode displays prior to automatic connection.

- **Auto (2D Barcode Imager)** - The software automatically determines the best scanning device.
- **2D Barcode Imager** - Scanning is performed using the 2D Imager.
- **Bluetooth Scanner** - Scanning is performed using the optional Bluetooth scanner.
- **RS6000 Bluetooth Scanner** - Scanning is performed using the RS6000 Bluetooth scanner.
- **DS3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.
- **LI3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.
- **DS2278 Bluetooth Scanner** - Scanning is performed using the DS2278 Bluetooth scanner.
- **DS8178 Bluetooth Scanner** - Scanning is performed using the DS8178 Bluetooth scanner.

### Hardware Trigger

Enables or disables the hardware trigger for scanning (Default - enabled). If disabled, pressing the hardware trigger will not scan a barcode. When the hardware trigger is disabled, it cannot be used for starting the scanning beam, but if scanning is started by a soft scan trigger intent, then a hardware trigger press cancels the scan.



## Auto Switch to Default on Event

This feature configures DataWedge to select an external scanner as the default scanning device immediately upon connection and revert to a built-in scanner when the external scanner is disconnected. External scanners include those connecting by Bluetooth, serial cable or snap-on module. Disabled by default. This is only available when **Scanner Selection** is set to **Auto**.

This helps reduce scanning workflow interruptions when a Bluetooth scanner is introduced and/or it becomes disconnected due to losing power or moving out of range.

- **Disabled** - No scanner switching occurs when an external scanner is connected or disconnected (default).
- **On connect** - Selects the external scanner as the default scanning device immediately upon connection.
- **On disconnect** - Reverts to a built-in scanner based on its position in an internally managed scanner list (which varies by host device). This is usually the scanner most recently used prior to the external connection (see notes below).
- **On connect/disconnect** - Selects an external scanner as the default scanning device immediately upon connection. Upon disconnection, reverts to the scanner set as the default prior to the external connection.



**NOTE:** The system selects the default scanner based on the connection state and the scanner's position in an internally managed scanner list. If the newly connected scanner is lower in the scanner list than the one currently selected as the default scanner, the newly connected scanner becomes the default scanner.

On devices with only one built-in scanner or imager, **On disconnect** reverts to that built-in scanner or imager.

## Configure Scanner Settings

Select Configure Scanner Settings to set the following:

- Select scanner to set parameters
- Decoders
- Decoder params
- UPC/EAN params
- Reader params
- Scan params
- UDI params
- Basic Multibarcodes params
- Keep enabled on suspend

## Decoders

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

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




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

**Table 4** *Supported Decoders*

Decoders	Internal Imager SE2100	RS507/RS507X	RS6000	DS3678
Australian Postal	O	O	O	O
Aztec	X	X	X	X
Canadian Postal	O	--	O	--
Chinese 2 of 5	O	O	O	O
Codabar	X	X	X	X
Code 11	O	O	O	O
Code 128	X	X	X	X
Code 39	X	X	X	X
Code 93	O	O	O	O
Composite AB	O	O	O	O
Composite C	O	O	O	O
Discrete 2 of 5	O	O	O	O
Datamatrix	X	X	X	X
Dutch Postal	O	O	O	O
DotCode	O	O	O	O
EAN13	X	X	X	X
EAN8	X	X	X	X
GS1 DataBar	X	X	X	X
GS1 DataBar Expanded	X	X	X	X
GS1 DataBar Limited	O	O	O	O
GS1 Datamatrix	O	--	O	O
GS1 QRCode	O	--	O	O
HAN XIN	O	--	O	O
Interleaved 2 of 5	O	O	O	O

**Table 4** Supported Decoders (Continued)

Decoders	Internal Imager SE2100	RS507/RS507X	RS6000	DS3678
Japanese Postal	O	O	O	O
Korean 3 of 5	O	O	O	O
MAIL MARK	X	--	X	X
Matrix 2 of 5	O	O	O	O
Maxicode	X	X	X	X
MicroPDF	O	O	O	O
MicroQR	O	O	O	O
MSI	O	O	O	O
PDF417	X	X	X	X
QR Code	X	X	X	X
Decoder Signature	O	O	O	--
TLC 39	O	O	O	O
Trioptic 39	O	O	O	O
UK Postal	O	O	O	O
UPCA	X	X	X	X
UPCE0	X	X	X	X
UPCE1	O	O	O	O
US4state	O	O	O	O
US4state FICS	O	O	O	O
US Planet	O	O	O	O
US Postnet	O	O	O	O

Touch  to return to the previous screen.

## Decoder Params

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



**NOTE:** Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

**NOTE:**

**Codabar**

- **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Length1** - Use to set decode lengths (default - 6). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Redundancy** - Sets the reader to read the barcode 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 for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 barcode.
  - **No Check Digit** - Do not verify check digit.
  - **1 Check Digit** - Barcode contains one check digit (default).
  - **2 Check Digits** - Barcode contains two check digits.

**Code128**

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 barcodes (default - disabled).
- **Ignore Code128 FNC4** - When enabled, and a Code 128 barcode 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 (default - disabled).
- **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT barcodes 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).
- **Enable Plain Code128** - Set the Plain Code128 subtype. Enables other (non-EAN or ISBT) Code 128 subtypes. 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 for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 barcodes. Select increasing levels of security for decreasing levels of barcode 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” barcodes.
  - **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 barcodes. 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 barcodes.

### Code39

- **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 barcodes (default - disabled).
- **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate barcode 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 for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 barcode to enable or disable adding the prefix character “A” to all Code 32 barcodes (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” barcodes.
  - **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 barcodes. 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 barcodes.
- **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 for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 for more information.
- **Length2** - Use to set decode lengths (default - 14). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

**DotCode**

- **Inverse** - Specify the reflectance for decoding DotCode barcodes.
  - **Disabled (0)** - Decode DotCode barcodes with normal reflectance only.
  - **Enabled (1)** - Decode DotCode barcodes with inverse reflectance only.
  - **Auto (2)** - Decodes both normal and inverse reflectance DotCode barcodes. (default - enabled).
- **Mirror** - Specify whether mirrored DotCode barcodes are decoded.
  - **Disabled (0)** - Decode non-mirrored DotCode barcodes only.
  - **Enabled (1)** - Decode mirrored DotCode barcodes only.
  - **Auto (2)** - Decodes both mirrored and non-mirrored DotCode barcodes. (default - enabled).

**Grid Matrix**

- **Inverse** - Specify the reflectance for decoding Grid Matrix barcodes.
  - **Disabled (0)** - Decode Grid Matrix barcodes with normal reflectance only.
  - **Enabled (1)** - Decode Grid Matrix barcodes with inverse reflectance only.
  - **Auto (2)** - Decodes both normal and inverse reflectance Grid Matrix barcodes. (default - enabled).
- **Mirror** - Specify whether mirrored Grid Matrix barcodes are decoded.
  - **Disabled (0)** - Decode non-mirrored Grid Matrix barcodes only.
  - **Enabled (1)** - Decode mirrored Grid Matrix barcodes only.
  - **Auto (2)** - Decodes both mirrored and non-mirrored Grid Matrix barcodes. (default - enabled).

**GS1 DataBar Limited**

- **GS1 Limited Security Level**

- **GS1 Security Level 1** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” barcodes.
- **GS1 Security Level 2** - This setting eliminates most misdecodes (default).
- **GS1 Security Level 3** - Select this option if Security level 2 fails to eliminate misdecodes.
- **GS1 Security Level 4** - If Security Level 3 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec barcodes. 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 barcodes.

**HAN XIN**

- **HAN XIN Inverse**

- **Disable** - Disables decoding of HAN XIN inverse barcodes (default).
- **Enable** - Enables decoding of HAN XIN inverse barcodes.
- **Auto** - Decodes both HAN XIN regular and inverse barcodes.

**Interleaved 2 of 5**

- **Febraban** - Enable to insert special check characters in the transmitted data stream of Interleaved 2 of 5 barcodes which are of length 14 and meet specific Febraban criteria. A check in the checkbox indicates that the option is enabled (default - disabled).
- **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 for more information.
- **Length2** - Use to set decode lengths (default - 10). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 barcodes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 barcode 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 barcodes (default - disabled).

**Matrix 2 of 5**

- **Length1** - Use to set decode lengths (default - 10). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode 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 for more information.
- **Length 2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Reduced Quiet Zone** - Enables decoding of margin-less MSI barcodes. A check in the checkbox indicates that the option is enabled (default - disabled)
- **Redundancy** - Sets the reader to read the barcode 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).

## Decoder Signature

- **Bits Per Pixel** - Use to set the bits per pixel (default - 8).
- **Format** - Use to set the format (default - JPG).
- **Height** - Use to set the height (default - 100).
- **JPEG Quality** - Use to set the JPEG quality (default - 65).
- **Width** - Use to set the width (default - 400).

## 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 None** - Transmit no preamble (default).
  - **Preamble Sys Char** - Transmit System Character only.
  - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
- **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 None** - Transmit no preamble (default).
  - **Preamble Sys Char** - Transmit System Character only.
  - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
- **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.



**NOTE:** Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar barcodes 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. (default - disabled).
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC barcodes. (default - disabled)
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **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. (default - disabled).
- **Coupon Report Mode** - Traditional coupon symbols are composed of two barcode: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded barcode. 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 barcodes: 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. (default)
- **Ean Zero Extend** - 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, for example, 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 (default - enabled).
- **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 barcodes. Select higher security levels for lower quality barcodes. 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 barcodes.
  - **Level 1** - As barcode quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed barcodes, and the misdecodes are limited to these characters, select this security level. (default).
  - **Level 2** - If the scanner is misdecoding poorly printed barcodes, 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 barcodes. 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 barcodes.
- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the barcode 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 barcode 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 barcode 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 barcode not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode 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 barcode not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode 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 barcode 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 barcode is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.

## Reader Params

Allows the configuration of parameters specific to the selected barcode reader.



**NOTE:** Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Character Set Configuration** - Used to support the GB2312 Chinese characters encoding.
  - **Character Set Selection** - Allows the user to convert the barcode data if different from default encoding type.
    - **Auto Character Set Selection (Best Effort)** - Automatic character convert option. Tries to decode data from the Preferred selection. The first correct decodable character set is used to convert the data and is sent.
    - **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.
    - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.
    - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
  - **Auto Character Set Preferred Order** - In **Auto Character Set Selection** mode, the system will try to decode the data in a preference order of character sets. The algorithm used is a best effort one. That is, there could be cases where the data can be decoded from more than one character set. The first character set from the preferred list which can decode the data successfully will be chosen to decode the data and sent to the user. Any other character set that is in the list but lower in the preferred order, would not be considered, even if the data could be successfully decoded using such character set.
 

The preferred character set and its preference order is configurable to the user through the **Auto Character Set Preferred Order** menu. Users can change the order by dragging the icon for that menu item. To delete an item, long press on an item and the **Delete** option will appear. To add a new item, tap the menu icon at top right corner and options to add UTF-8 and GB2312 will appear.

    - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
    - **GB2312** - Character set of the People's Republic of China, used for simplified Chinese characters.
  - **Auto Character Set Failure Option** - If the system cannot find a character set from the preferred list that can be used to successfully decode the data, the character set selected in **Auto Character Set Failure Option** is used to decode the data and send to the user. If **NONE** is used, Null data is returned as string data.
    - **NONE**
    - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
    - **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** - ended for Western European languages.
    - **Shift\_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
    - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.
- **Presentation mode parameters** - Sets the scene detection qualifier for presentation mode (default - none).

- **1D Quiet Zone Level** - Sets the level of aggressiveness in decoding barcodes with a reduced quiet zone (the area in front of and at the end of a barcode), 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 barcode) for decoding.
- **3** - The scanner decodes anything in terms of quiet zone or end of barcode.
- **Adaptive Scanning** - When adaptive scanning is enabled, the scan engine toggles between wide and narrow, allowing the scan engine to decode barcodes based on the distance.
  - **Disable**
  - **Enable** (default).
- **Beam Width** - Beam Width is applicable only with linear scanners.
  - **Narrow**
  - **Normal** (default)
  - **Wide**
- **Aim mode** - Turns the scanner cross-hairs on or off.
  - **On** - Cross-hair is on (default).
  - **Off** - Cross-hair is off.
- **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 (default).
  - **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.
  - **Press and Sustain** - A trigger pull activates the laser for aiming, which continues until the Beam Timer expires or a valid 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 -5000).
- **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**.
- **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.
- **Digimarc Decoding** - Enables/disables support for Digimarc, which encodes and invisibly integrates traditional barcode data onto product packaging. Supported with internal imager only. (default - Enabled).

- **Illumination Brightness** - Sets the brightness of the illumination by altering LED power. The default is 10, which is maximum LED brightness. For values from 1 to 10, LED brightness varies from lowest to highest level of brightness.
- **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.
  - **Off** - Illumination is off.
  - **On** - Illumination is on (default).
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D barcodes.
  - **Disable** - Disables decoding of inverse 1D barcodes (default).
  - **Enable** - Enables decoding of only inverse 1D barcodes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D barcodes.
- **Keep Pairing Info After Reboot**
  - **Disable** - Disables the ability to keep pairing info after reboot.
  - **Enable** - Enables the ability to keep pairing info after reboot. (default).
- **LCD Mode** - Enables or disables LCD mode. LCD mode enhances the ability of the imager to read barcodes from LCD displays such as cellphones.
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.
- **Linear Security Level** - Sets the number of times a barcode is read to confirm an accurate decode.
  - **Security Short or Codabar** - Two times read redundancy if short barcode or Codabar (default).
  - **Security All Twice** - Two times read redundancy for all barcodes.
  - **Security Long and Short** - Two times read redundancy for long barcodes, three times for short barcodes.
  - **Security All Thrice** - Three times read redundancy for all barcodes.
- **HW Engine Low Power Timeout** - Time (0 - 1,000 ms in increments of 50 ms) of inactivity before scanner enters low-power mode from (default - 250)..
- **Picklist** - Allows the imager to decode only the barcode that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple barcodes 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 barcode within the field of view can be decoded (default).
  - **Enabled** - Enables Picklist mode so that only the barcode under the projected reticle can be decoded.
- **Poor Quality Decode Effort** - Enable poor quality barcode decoding enhancement feature.
- **Power Modes** - Sets the power mode for the device.
  - **Low Power Mode** - Enables Low Power mode.
  - **Optimized Power Mode** - - Enables Optimized Power mode (default).
  - **High Power Mode** - Enables High Power mode.
  - **Always On** - Enables Always On mode.
- **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.
- **Scanning Modes** - Scanning options available on the device.
  - **Single** - Set to scan general barcodes (default).
  - **UDI** - Set to scan healthcare specific barcodes.
  - **Basic MultiBarcode** - Set to scan multiple barcodes. When this option is selected, the **Multibarcodes** can be set to read from 2 to 10 barcodes on a single scan.



## Scan Params

Allows the configuration of Code ID and decode feedback options.



**NOTE:** Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned barcode. This is useful when the reader is decoding more than one code type. Select a code ID character to insert between the prefix and the decoded symbol.
  - **Code ID Type None** - No prefix (default)
  - **Code ID Type AIM** - Insert AIM Character prefix.
  - **Code ID Type Symbol** - Insert Symbol character prefix.
- **Engine Decode LED** - Use to turn on scanner red LED when the scan beam is emitting either by scanner trigger or using soft scan button.
- **BT Disconnect On Exit** - Bluetooth connection is disconnected when data capture application is closed .
- **Connection Idle Time** - Set connection idle time. The Bluetooth connection disconnects after being idle for set time.
- **Display BT Address Barcode** - Enable or disable displaying Bluetooth Address bar code if there is no Bluetooth scanner being paired when application tries to enable the Bluetooth scanner.
- **Establish Connection Time** - The timeout which the device will try to enable or reconnect to the Bluetooth scanner when the Bluetooth scanner is not in the vicinity or not paired.
- **Audio Feedback Mode** - Select good decode audio indication.
  - **Local Audio Feedback** - Good decode audio indication on device only.
  - **Remote Audio Feedback** - Good decode audio indication.
  - **Both** - Good decode audio indication on device and scanner (default).
  - **Disable** - No good decode audio indication on either device or scanner.
- **LED Feedback Mode** - Select good decode LED indication.
  - **Local LED Feedback** - Good decode LED indication on device only.
  - **Remote LED Feedback** - Good decode LED indication on scanner.
  - **Both** - Good decode LED indication on device and scanner (default).
  - **Disable** - No good decode LED indication on either device or scanner.
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode (default optimized-beep).
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).
- **Decode Feedback LED Timer** - Set the amount of time (in milliseconds) that the green Data Capture LED stays lit after a good decode. (default - 75 msec.)
- **Beep Volume 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.

- **Ringer** - Uses Ringer audio stream to play the decode beep.
- **Music and Media** - Uses Media audio stream to play the decode beep.
- **Alarms** - Uses Alarms audio stream to play the decode beep.
- **Notifications** - Uses Notifications audio stream to play the decode beep. (default)

## UDI Params

Allows the configuration of parameters specific to healthcare barcodes.

- **Enable UDI-GSI** - Enable UDI using GS1 standards (default - enabled).
- **Enable UDI-HIBCC** - Enable UDI using HIBCC standards (default - enabled).
- **Enable UDI-ICCBBA** - Enable UDI using ICCBBA standards (default - enabled).

## Basic Multibarcodes params

Set the number of barcodes that the device can read on a single scan from 2 to 10. Must also enable **Reader Params > Scanning Modes > Basic MultiBarcode** option.

## Keep enabled on suspend

Keep Bluetooth scanner enabled after suspend (default-disabled).

## Voice Input

Zebra GMS devices have a built in Google speech recognition engine. By making use of the speech engine capabilities, DataWedge has extended automated data capturing to user applications through voice. Currently, DataWedge does not capture data for Voice Input.

Voice data capturing starts after you speak the predefined start phrase and it stops after you speak the data or speak the end phrase, if one was defined.



### IMPORTANT:

- Simultaneous use of Voice Input in DataWedge and Google Voice is not supported.
- Voice Input is not supported if the Enterprise Home Screen (EHS) is in restricted mode. However, enabling all of the privilege settings in EHS reinstates Voice Input.
- Voice Input is not supported if the device language is changed to another language, for example Chinese.

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

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.
- **Data capture start phrase** - Starts data capture with the phrase entered in this field. This field is mandatory. (Default - **start**).  
Providing numbers and other special characters as the data capture start phrase is not supported.
- **Data capture end phrase** - Ends data capture with the phrase entered in this field or keep it blank if not required. This field is not mandatory. (Default - Blank).
- **End detection timeout** - Sets the timeout value (in seconds) for data capture when the device is at the **waiting for data** state. If the value is set to 0 and the Data capture end phrase is defined, the device waits indefinitely. If the value is set to 0 and the Data capture end phrase is not defined, data is returned immediately (default - 0).
- **Tab command** - Enables the Tab command, which sends a tab key when the user speaks the command **send tab**. The commands are supported only when the device is at the **Waiting for start phrase** state.
- **Enter command** - Enables the Enter command, which sends an enter key when the user speaks the command **send enter**. The commands are supported only when the device is at the **Waiting for start phrase** state.



- **Data type** - Allows the user to configure the data type. Set the data type to limit the data capture according to the preferences specified. Available options:
  - **Any** - Scanning a barcode of ABC123, returns ABC123.
  - **Alpha** - Scanning a barcode of ABC123, returns ABC only.
  - **Numeric** - Scanning a barcode of ABC, returns 123 only.
- **Start phrase waiting tone** - Enables or disables this option. Enables audio feedback for **Waiting for start**. This option notifies the user that the device is waiting to start the speech engine if you miss the toast message and the **Waiting for start** state changes.
- **Data capture waiting tone** - Enables or disables this option. Enables audio feedback for **Waiting for data**. This option notifies the user that the device is waiting to capture data if you miss the toast message.
- **Validation window** - Enables or disables the **Validate captured data** window. Enable this option to validate the result that you speak. The window displays the data spoken and the data can be edited on the same screen if any modification is needed. This is very useful when used with the offline mode, since the results receive at this moment might not be accurate.
- **Offline speech recognition** - Enables or disables speech recognition. Enable this option to use Voice Input when you do not have access to the Internet. This option uses an offline recognition speech engine to detect the data you speak.

## Keystroke Output

DataWedge supports Keystroke Output, which collects the processed data and sends it to the foreground application as a series of keystrokes which helps data capturing to applications without writing any code.

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 barcode 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 barcode is processed. When DataWedge detects this character code in a barcode, the focus moves to the next field.
  - **Line feed** - Line feed character code in a barcode is processed. When DataWedge detects this character code in a barcode, the focus moves to the next field.
  - **Carriage return** - Carriage return character code in a barcode is processed. When DataWedge detects this character code in a barcode, the focus moves to the next field.
- **Inter character delay** - Set the delay between keystrokes (in milliseconds).
- **Delay Multibyte characters only** - If Inter character delay is set, enable Delay Multibyte characters only to delay only the multibyte characters.
- **Key event options** - Set control character options.
  - **Key event delay** - Set the amount of time (in milliseconds) to wait for control characters (default - 0).
  - **Send Characters as Events** - Enable to send ASCII characters 32-126 as events.
  - **Send Enter as string** - Enable to send the Enter character as a string.
  - **Send Tab as string** - Enable to send the Tab character as a string.
  - **Send Control Characters as Events** - Enable to send ASCII characters 1-31 (except Enter and Tab) as events.

- **Data formatting and ordering** - Allows formatting and ordering of UDI and Multibarcodes data.
  - **UDI specific** - Allows the output order of acquired UDI data to be adjusted and the optional insertion of a tab, line feed, or carriage return character between tokens.
    - **Send tokens** - Set to select the output format for UDI data. (default - disabled)
    - **Token separator** - Set to select a separator character. If no separator character is selected when Send tokens is set to Barcodes and tokens, two instances of the same data are sent. (default - none)
    - **Token order** - Set to include or exclude Tokens from the output and adjust their output order.
  - **Multibarcodes specific** - Allows the optional insertion of a tab, line feed, or carriage return between each barcode.
    - **Barcode separator** - Set to select a separator character. If no separator character is selected, the data set is sent as a single string.
- **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 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, [developer.android.com](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
- **Receiver foreground flag** - Set Broadcast intent flag in Intent delivery. (DS3678).
- **Use startForegroundService on failure** - Enable this option to use startForegroundService if startService fails.
- **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 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.action.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 barcode.
- String DATA\_STRING\_TAG = "com.symbol.datawedge.data\_string";
  - String contains the output data as a String. In the case of concatenated barcodes, the decode data is concatenated and sent out as a single string.
- String DECODE\_DATA\_TAG = "com.symbol.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 barcode symbologies that support concatenation, for example, Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per barcode). 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: [www.zebra.com/support](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).
- **Data formatting and ordering** - Allows formatting and ordering of UDI and Multibarcodes data.
  - **UDI specific** - Allows the output order of acquired UDI data to be adjusted and the optional insertion of a tab, line feed, or carriage return character between tokens.

- **Send tokens** - Set to select the output format for UDI data. (default - disabled)
- **Token separator** - Set to select a separator character. If no separator character is selected when Send tokens is set to Barcodes and tokens, two instances of the same data are sent. (default - none)
- **Token order** - Set to include or exclude Tokens from the output and adjust their output order.
- **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 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 64** IP Output Screen

Profile: Profile1

IP output

Enabled  
Enable/disable output via IP ☐

Remote Wedge  
Enable/disable Remote Wedge option ☒

Protocol  
TCP

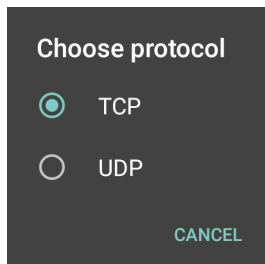
IP address  
0.0.0.0

## 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:

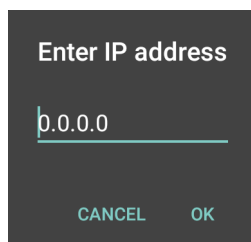
1. In **IP Output**, touch **Enabled**.  
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is enabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).

**Figure 65** Protocol Selection



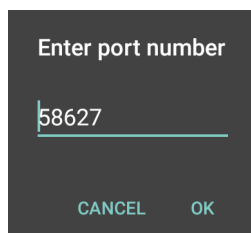
5. Touch **IP Address**.
6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

**Figure 66** IP Address Entry



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

**Figure 67** Port Number Entry



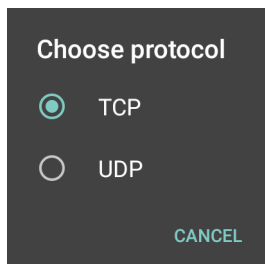
9. Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

## Using IP Output without IPWedge

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

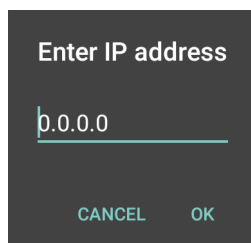
1. In **IP Output**, touch **Enabled**.  
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is disabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

**Figure 68** Protocol Selection



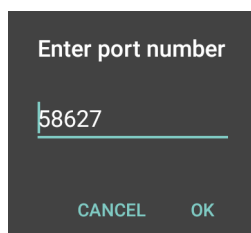
5. Touch **IP Address**.
6. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.

**Figure 69** IP Address Entry



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

**Figure 70** Port Number Entry



- 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.

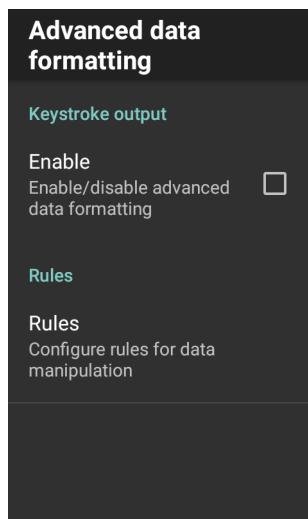
- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.
- Criteria - Criteria can be set according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

- Swipe up from the bottom of the screen and touch .
- Touch a DataWedge profile.
- In **Keystroke Output**, touch **Advanced data formatting**.

**Figure 71** Advanced Data Formatting Screen



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


## Creating a Rule



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

- Touch **Rules**.

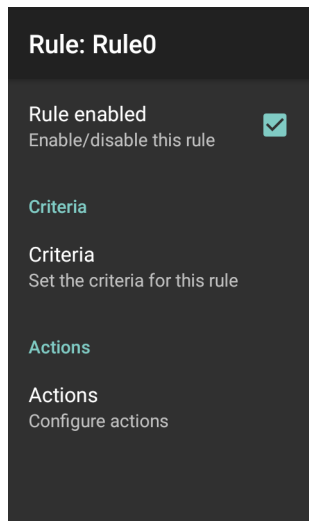


2. Touch .
3. Touch **New rule**.
4. Touch the **Enter rule name** text box.
5. In the text box, enter a name for the new rule.
6. Touch **OK**.

## Defining a Rule

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

**Figure 72** Rule List Screen

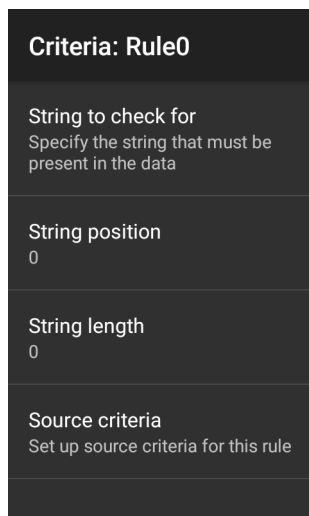


2. Touch the **Rule enabled** check box to enable the current rule.

## Defining Criteria

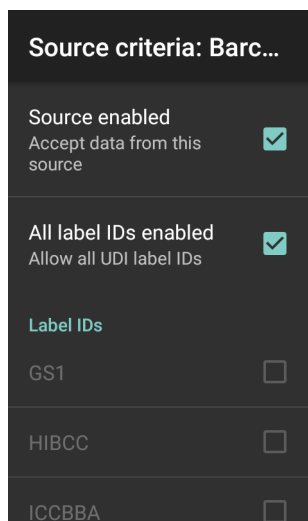
1. Touch **Criteria**.

**Figure 73** 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 barcode data with that specified length.
9. Touch the **+** or **-** to change the value.
10. Touch **OK**.
11. Touch **Source criteria** option to associate an input device to an ADF rule. The ADF rule only applies to data received from associated input devices.
12. Touch **Barcode input**. Options vary depending upon the device configuration.
13. Touch the **Source enabled** checkbox to accept data from this source.

**Figure 74** Barcode Input Screen





14. For general 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 the ADF Supported Actions table 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 rule** 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 5** 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 5** 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 <b>Crunch spaces</b> action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last <b>Remove all spaces</b> action.
	Remove leading zeros	Remove all zeros at the beginning of data.
	Stop zero removal	Stop removing zeros at the beginning of data. This disables the previous <b>Remove leading zeros</b> action.
	Pad with zeros	Left pad data with zeros to meet the specified length. Enter the number zeros to pad.
	Stop pad zeros	Stop padding with zeros. This disables the previous <b>Pad with zeros</b> action.
	Pad with spaces	Left pad data with spaces to meet the specified length. Enter the number spaces to pad.
	Stop pad spaces	Stop padding with spaces. This disables the previous <b>Pad with spaces</b> action.
	Replace string	Replaces a specified string with a new string. Enter the string to replace and the string to replace it with.
	Stop all replace string	Stop all <b>Replace string</b> actions.
Data Sending	Send next	Sends the specified number of characters from the current cursor position. Enter the number of characters to send.
	Send remaining	Sends all data that remains from the current cursor position.
	Send up to	Sends all data up to a specified string. Enter the string.
	Send pause	Pauses the specified number of milliseconds before continuing the next action. Enter the amount of time in milliseconds.
	Send string	Sends a specified string. Enter the string to send.
	Send char	Sends a specified ASCII/ Unicode character. Enter a character value. The maximum Unicode character value can be entered is U-10FFFF (= 1114111 in decimal).

## Deleting an Action

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 barcode with the following criteria:




- Code 39 barcode.

- length of 12 characters.
- contains 129 at the start position.

Modify the data as follows:

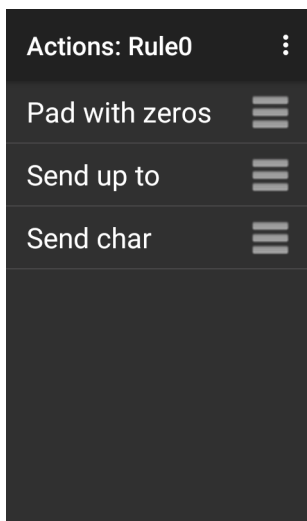
- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

To create an ADF rule for the above example:

1. Swipe up from the bottom of the screen and touch .
2. Touch **Profile0**.
3. Under **Keystroke Output**, touch **Advanced data formatting**.
4. Touch **Enable**.
5. Touch **Rule0**.
6. Touch **Criteria**.
7. Touch **String to check for**.
8. In the **Enter the string to check for** text box, enter 129 and then touch **OK**.
9. Touch **String position**.
10. Change the value to 0.
11. Touch **OK**.
12. Touch **String length**.
13. Change value to 12.
14. Touch **OK**.
15. Touch **Source criteria**.
16. Touch **Barcode input**.
17. Touch **All decoders enabled** to disable all decoders.
18. Touch **Code 39**.
19. Press  three times.
20. Touch **Actions**.
21. Touch and hold on the **Send remaining rule** until a menu appears.
22. Touch **Delete action**.
23. Touch .
24. Touch **New action**.
25. Select **Pad with zeros**.
26. Touch the **Pad with zeros** rule.

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

**Figure 75** ADF Sample Screen



46. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).

47. Aim the exit window at the barcode.

**Figure 76** Sample Barcode



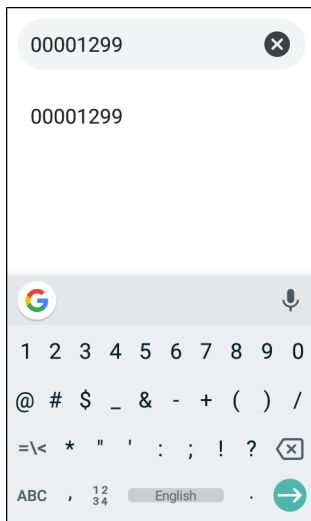
48. Press and hold the scan button.

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

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

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

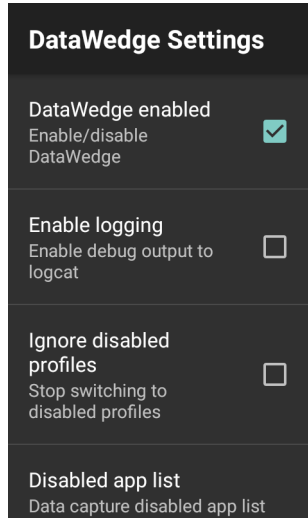
**Figure 77** Formatted Data



## DataWedge Settings

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

**Figure 78** DataWedge Settings Window



- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option (default - enabled).
- **Enable logging** - Enables or disables debug output file to logcat. To enable logging check this option (default - disabled).
- **Ignore disabled profiles** - Prevents DataWedge from switching to a Profile that is not enabled. In such instances, the Profile switch is ignored and the current Profile remains active Profile0 must be disabled to use this feature (default - disabled).
- **Disable app list** - Disables scanning functions for selected applications or activities.
- **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.
- **Reporting** - Configures reporting options.


## Importing a Configuration File

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

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




## Exporting a Configuration File

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


## Importing a Profile File



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


1. Copy the profile file to the On Device Storage **/Android/data/com.symbol.datawedge/files** folder.
2. Touch .
3. Touch **Settings**.
4. Touch **Import Profile**.
5. Touch the profile file to import.
6. 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 **Settings**.
3. Touch **Export Profile**.
4. Touch the profile to export.
5. Touch **Export**.  
The profile file (dwprofile\_x.db, where x = name of the profile) is saved to the root of the On-device Storage.

## Restoring DataWedge

To restore DataWedge to the factory default configuration:

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

## Configuration and Profile File Management

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

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

## Enterprise Folder

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



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

### Auto Import

DataWedge supports remote deployment of a configuration to a device, using tools such as commercially available third-party Mobile Device Management (MDM) systems. DataWedge monitors the `/enterprise/device/settings/datawedge/autoimport` folder for the DataWedge configuration file (`datawedge.db`) or a profile file (`dwprofile_x.db`). 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. 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.

The `/enterprise` folder cannot be seen with **Files** app or other user-level tools. Moving configuration files to and from the `/autoimport` or `/enterprisereset` folders must be done programmatically, or with a staging client app or MDM.

## Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

### Overriding Trigger Key in an Application

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


### Capture Data and Taking a Photo in the Same Application

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

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

## Disable DataWedge on Device

To disable DataWedge:

1. Swipe up from the bottom of the Home screen and touch **DataWedge**.
2. Touch  .
3. Touch **Settings**.
4. Unselect the **DataWedge enabled** check box.

## DataWedge APIs

DataWedge APIs operate primarily through Android intents - specific commands that can be used by other applications to control data capture without the need to directly access the DataWedge UI.

## Reporting

DataWedge 6.6 (and higher) can report the results of the importation of device Profiles. These HTML reports display settings differences between the originating (source) database and the target (destination) device. This allows administrators to easily identify differences and make adjustments to compensate for disparities in hardware or software capabilities from one device to another. Reports always use the destination device as the basis against which to compare incoming settings files.

## Soft Scan Trigger

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.

### Function Prototype

```
Intent i = new Intent();  
i.setAction("com.symbol.datawedge.api.ACTION");  
i.putExtra("com.symbol.datawedge.api.SOFT_SCAN_TRIGGER", "<parameter>");
```

### Parameters

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

**ACTION** [String]: "com.symbol.datawedge.api.ACTION"

**EXTRA\_DATA** [String]: "com.symbol.datawedge.api.SOFT\_SCAN\_TRIGGER"

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

- START\_SCANNING - starts scanning when triggered
- STOP\_SCANNING - stops or interrupts scanning when triggered
- TOGGLE\_SCANNING - toggles between START\_SCANNING and STOP\_SCANNING when triggered.

## 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("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SCANNER_INPUT_PLUGIN", "<parameter>");
```

## Parameters

**action:** String "com.symbol.datawedge.api.ACTION"

**extra\_data:** String "com.symbol.datawedge.api.SCANNER\_INPUT\_PLUGIN"

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

- SUSPEND\_PLUGIN - suspends the scanner so it is temporarily inactive when switching from the WAITING or SCANNING state. SCANNER\_STATUS notification broadcasts IDLE state.
- RESUME\_PLUGIN - resumes the scanner when changing from the SUSPEND\_PLUGIN suspended state. SCANNER\_STATUS notification broadcasts WAITING and SCANNING states, rotating between each depending on whether scanning is taking place. In the WAITING state it is expecting an action from the user such as a trigger press. In the SCANNING state it is actively performing a scan resulting from an action such as a trigger press.
- "ENABLE\_PLUGIN" - enables the plug-in the scanner becomes active.
- "DISABLE\_PLUGIN" - disables the plug-in the scanner becomes inactive.

## 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, for example:

```
$ 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.sendBroadcast(i);
}
```

## Comments

This intent API allows the scanner plug-in for the current Profile to be enabled or disabled. For example, activity A launches and uses the intent API 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 intent API to switch back to ProfileA, then use the intent API 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("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.ENUMERATE_SCANNERS", "");
```

## Parameters

**ACTION** [String]: "com.symbol.datawedge.api.ENUMERATE\_SCANNERS"

## Return Values

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

Error and debug messages are 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. For example:

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

Error messages are logged for invalid actions and parameters.

## Example

```
//
// Call before sending the enumeration query
//
public void registerReciever(){
    IntentFilter filter = new IntentFilter();
    filter.addAction("com.symbol.datawedge.api.RESULT_ACTION");//RESULT_ACTION
    filter.addCategory(Intent.CATEGORY_DEFAULT);
    registerReceiver(enumeratingBroadcastReceiver, filter);
}
//
// Send the enumeration command to DataWedge
//
public void enumerateScanners(){
    Intent i = new Intent();
    i.setAction("com.symbol.datawedge.api.ACTION");
    i.putExtra("com.symbol.datawedge.api.ENUMERATE_SCANNERS", "");
    this.sendBroadcast(i);
}

public void unRegisterReciever(){
    unregisterReceiver(enumeratingBroadcastReceiver);
}

//
// Create broadcast receiver to receive the enumeration result
//
private BroadcastReceiver enumeratingBroadcastReceiver = new BroadcastReceiver() {
    @Override
    public void onReceive(Context context, Intent intent) {
        String action = intent.getAction();
        Log.d(TAG, "Action: " + action);
        if(action.equals("com.symbol.datawedge.api.RESULT_ACTION")){
            //
            // enumerate scanners
            //
            if(intent.hasExtra("com.symbol.datawedge.api.RESULT_ENUMERATE_SCANNERS")) {
                ArrayList<Bundle> scannerList = (ArrayList<Bundle>)
intent.getSerializableExtra("com.symbol.datawedge.api.RESULT_ENUMERATE_SCANNERS");
                if((scannerList != null) && (scannerList.size() > 0)) {
                    for (Bundle bunb : scannerList){
                        String[] entry = new String[4];
                        entry[0] = bunb.getString("SCANNER_NAME");
                        entry[1] = bunb.getBoolean("SCANNER_CONNECTION_STATE")+"";
                        entry[2] = bunb.getInt("SCANNER_INDEX")+"";

                        entry[3] = bunb.getString("SCANNER_IDENTIFIER");

                        Log.d(TAG, "Scanner:" + entry[0] + " Connection:" + entry[1] + " Index:" + entry[2] + " ID:" + entry[3]);
                    }
                }
            }
        }
    }
};
```

## 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("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SET_DEFAULT_PROFILE", "<profile name>");
```

### Parameters

**ACTION** [String]: "com.symbol.datawedge.api.ACTION"

**EXTRA\_DATA** [String]: "com.symbol.datawedge.api.SET\_DEFAULT\_PROFILE"

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

### Return Values

None.

Error and debug messages are 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. For example:



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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

## Example

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

public void onResume() {
    // create the intent
    Intent i = new Intent();

    // set the action to perform
    i.setAction(setDefaultProfile);

    // add additional info (a name)
    i.putExtra(extraData, "myProfile");

    // send the intent to DataWedge
    this.sendBroadcast(i);
}
```

## Comments

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

Zebra recommends that this Profile is created to cater to all applications/activities that would otherwise default to using Profile0. This ensures that these applications/activities continue to work with a consistent configuration.

## Reset Default Profile

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

## Function Prototype

```
Intent i = new Intent();  
i.setAction("com.symbol.datawedge.api.ACTION");  
i.putExtra("com.symbol.datawedge.api.RESET_DEFAULT_PROFILE", "");
```

## Parameters

**ACTION** [String]: "com.symbol.datawedge.api.ACTION"

**EXTRA\_DATA** [String]: "com.symbol.datawedge.api.RESET\_DEFAULT\_PROFILE".

## Return Values

None.

Error and debug messages are 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. For example:

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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

## Example

```
// define action string  
String action = "com.symbol.datawedge.api.ACTION";  
String extraData = "com.symbol.datawedge.api.RESET_DEFAULT_PROFILE";  
  
public void onResume() {  
    // create the intent  
    Intent i = new Intent();  
  
    // set the action to perform  
    i.setAction(action);  
    i.putExtra(extraData, ""); // empty since a name is not required  
    this.sendBroadcast;  
}
```

## Comments

None.

## Switch To Profile

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

### Profiles Recap

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

Profile information consists of:

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

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

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



**NOTE:** Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile. 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 Code 128 bar codes to be scanned. Profile EAN13 is configured to only scan EAN13 bar codes and is left unassociated. Profile Code128 is configured to scan Code 128 and is left unassociated. When Activity A launches it uses SwitchToProfile to activate Profile EAN13. Similarly, when Activity B launches it uses switchToProfile to activate Profile Code128.

If another activity/app comes to the foreground, DataWedge auto Profile switching sets 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 uses switchToProfile to reset the Profile back to Profile B (or Profile M).

### Function Prototype

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SWITCH_TO_PROFILE", "<profile name>");
```

### Parameters

**ACTION** [String]: "com.symbol.datawedge.api.ACTION"

**EXTRA\_DATA** [String]: "com.symbol.datawedge.api.SWITCH\_TO\_PROFILE"

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

## Return Values

None.

Error and debug messages are 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. For example:

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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

## Example

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

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
    this.sendBroadcast(i);
}
```

## Comments

This API function has 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 is not 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 is active whenever activity A is in the foreground. When activity B comes to the foreground, DataWedge automatically switches to Profile B.

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



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

## Notes

Because DataWedge automatically switches Profile when the activity is paused, Zebra recommends that this API function is 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 use 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**

# Application Deployment

## Introduction

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

## Security

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



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

## Secure Certificates


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

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

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

## Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the device's internal memory. See USB Communication for information about connecting the device to a host computer and copying files.
2. Swipe down from the Status bar to open the Quick Access panel and then touch .
3. Touch **Security & location > Encryption & credentials**.
4. Touch **Install from storage**.
5. Navigate to the location of the certificate file.

6. Touch the filename of the certificate to install.
7. If prompted, enter the password for credential storage. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.
8. If prompted, enter the certificate's password and touch **OK**.
9. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.

**Figure 79** Name the Certificate Dialog Box

**Name the certificate**

Certificate name:

Credential use:  
VPN and apps


The package contains:  
one user certificate

CANCEL OK

10. Touch **OK**.

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

## Configuring Credential Storage Settings

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location > Encryption & credentials**.
  - **Trusted credentials** - Touch to display the trusted system credentials.
  - **User credentials** - Touch to display user credentials.
  - **Install from storage** - Touch to install a secure certificate from the internal storage.
  - **Clear credentials** - Deletes all secure certificates and related credentials.

## Development Tools

### Development Workstation

Android development tools are available at [developer.android.com](http://developer.android.com).


To start developing applications for the device, download Android Studio. 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 virtual machine. Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

Android Studio contains a full featured IDE as well as SDK components required to develop Android applications.

### Target Device

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

By default, the Developer Options are hidden. To un-hide the developer options, swipe down from the Status bar to open the Quick Access panel and then touch .

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

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

### EMDK for Android

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

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

For more information go to: [techdocs.zebra.com](http://techdocs.zebra.com).

### StageNow

StageNow is Zebra's next-generation Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a bar code, reading a tag, or playing an audio file.

The StageNow Staging Solution includes the following components:

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

For more information go to: [techdocs.zebra.com](http://techdocs.zebra.com).

### ADB USB Setup



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



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

### Enabling USB Debugging

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

1. Swipe down from the Status bar to open the Quick Access panel, and then touch .
2. Touch **System > About phone**.
3. Scroll down to **Build number**.
4. Tap **Build number** seven times. The message **You are now a developer!** appears.
5. Touch .
6. Touch **Developer options**.
7. Slide the **USB debugging** switch to the **ON** position.
8. Touch **OK**.
9. Connect the device to the host computer using the Rugged Charge/USB Cable.  
The **Allow USB debugging?** dialog box appears on the device.
10. On the device, touch **OK**.
11. On the host computer, navigate to the **platform-tools** folder.
12. Type **adb devices**.

The following displays:

**List of devices attached**

XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

13. Touch .

### Entering Android Recovery Manually

Many of the update methods discussed in this section require putting the device into Android Recovery mode. If you are unable to enter Android Recovery mode through adb commands, use the following steps to manually enter Android Recovery mode.

1. Press and hold the Power button until the menu appears.
2. Touch **Restart**.
3. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

## Application Installation

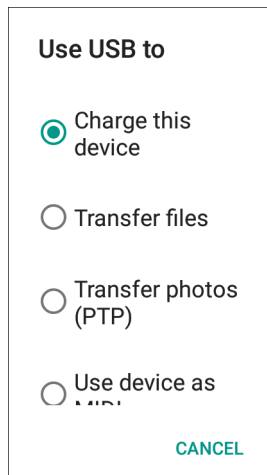
After an application is developed, install the application onto the device using one of the following methods:


- Android Debug Bridge, see Installing Applications Using the Android Debug Bridge.
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

### Installing Applications Using the USB Connection

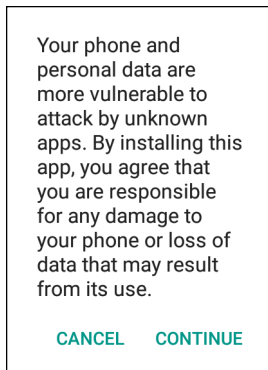
1. Connect the device to a host computer using the Rugged Charge/USB cable.
2. Pull down the Notification panel and touch **USB for Charging**.

**Figure 80** Use USB Dialog Box



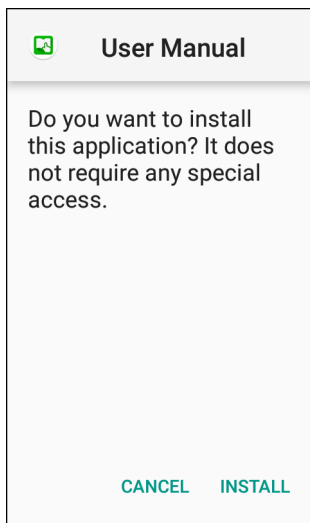
3. Touch **Transfer files**.
4. On the host computer, open a **Files** application.
5. On the host computer, copy the application .apk file from the host computer to the device.
6. Disconnect the device from the host computer.
7. Swipe the screen up and select  to view files on the Internal Storage.
8. Locate the application .apk file.
9. Touch the application file.

**Figure 81** Install App Permission Dialog Box



10. Touch **Continue** to install the app or **Cancel** to stop the installation.

**Figure 82** Accept Installation Screen




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

12. Touch **Open** to open the application or **Done** 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.


Ensure that the ADB drivers are installed on the host computer. See ADB USB Setup.

1. Connect the device to a host computer using USB. See USB Communication.
2. Swipe down from the Status bar to open the Quick Access panel and then touch .
3. Touch **System > Developer options**.
4. Slide the switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.

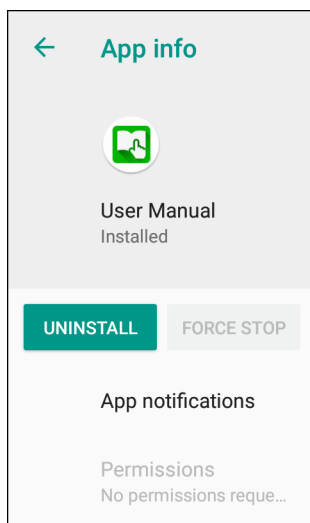
6. Touch **OK**.
7. On the host computer, open a command prompt window and use the adb command:  
`adb install <application>`  
 where: <application> = the path and filename of the apk file.
8. Disconnect the device from the host computer. See USB Communication.

## Uninstalling an Application

To uninstall an application:

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Apps & notifications**.
3. Touch **See all apps** to view all apps in the list.
4. Scroll through the list to the app.
5. Touch the app. The **App info** screen appears.

**Figure 83** App Info Screen



6. Touch **Uninstall**.
7. Touch **OK** to confirm.

## Performing a System Update

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


## Downloading the System Update Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, [www.zebra.com/support](http://www.zebra.com/support).
2. Download the appropriate System Update package to a host computer.

### Using ADB

To update the system using ADB:

1. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > 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 devices
```

The following displays:

```
List of devices attached
```

```
XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).
```



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

7. Type:

```
adb reboot recovery
```

If you are not able to enter Android Recovery mode through the adb command, go to [Entering Android Recovery Manually on page 121](#).

8. Press Enter. The System Recovery screen appears.
9. Press the Volume Up and Volume Down buttons to navigate to **Apply upgrade from ADB**.
10. Press the Power button.
11. Use the Volume Up and Volume Down buttons to navigate to **Full OTA Package** or **Diff OTA Package**.
12. Press the Power button.
13. On the host computer command prompt window type:  

```
adb sideload <file>
```


where: <file> = the path and filename of the zip file.
14. Press Enter. The System Update installs (progress appears as percentage in the Command Prompt window) and then the Recovery screen appears.
15. Press the Power button to reboot the device.



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

## Verify System Update Installation

To check that the system update installed properly:

1. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > About phone**.
3. Scroll down to **Build number**.
4. Ensure that the build number matches the new system update package file number.

## Performing an Enterprise Reset

An Enterprise Reset erases all user data in the `/data` partition, including data in the primary storage locations (`/sdcard` and emulated storage).

Before performing an Enterprise Reset, provision all necessary configuration files and restore after the reset.

Perform Enterprise Reset using ADB.


## Downloading the Enterprise Reset Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, [www.zebra.com/support](http://www.zebra.com/support).
2. Download the Enterprise Reset file to a host computer.

## Using ADB

To perform an Enterprise Reset using ADB:

1. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > 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 type:  
**adb devices.**

The following displays:

**List of devices attached**

XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

7. Type:  
**adb reboot recovery**  
If you are not able to enter Android Recovery mode through the adb command, go to [Entering Android Recovery Manually on page 121](#).
8. Press Enter. The System Recovery screen appears.
9. Press the Volume Up and Volume Down buttons to navigate to **Apply upgrade from ADB**.
10. Press the Power button.
11. Use the Volume Up and Volume Down buttons to navigate to **Full OTA Package**.
12. Press Power button.
13. On the host computer command prompt window type:  
**adb sideload <file>**  
where: <file> = the path and filename of the zip file.
14. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.
15. Press the Power button to reboot the device.

## Performing a Factory Reset

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


## Downloading the Factory Reset Package

To download the Factory Reset package:

1. Go to the Zebra Support & Downloads web site, [www.zebra.com/support](http://www.zebra.com/support).
2. Download the appropriate Factory Reset file to a host computer.

## Using ADB

To perform an Factory Reset using ADB:

1. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > 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 devices.**

The following displays:

**List of devices attached**

XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

7. Type:

**adb reboot recovery**

If you are not able to enter Android Recovery mode through the adb command, go to [Entering Android Recovery Manually on page 121](#).

8. Press Enter. The System Recovery screen appears.
9. Press the Volume Up and Volume Down buttons to navigate to **Apply upgrade from ADB**.
10. Press the Power button.
11. Use the Volume Up and Volume Down buttons to navigate to **Full OTA Package**.
12. Press Power button.
13. On the host computer command prompt window type:  
**adb sideload <file>**  
where: <file> = the path and filename of the zip file.
14. Press Enter. The Factory Reset package installs and then the Recovery screen appears.
15. Press the Power button to reboot the device.


## Storage

The device contains the following types of file storage:

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

### Random Access Memory

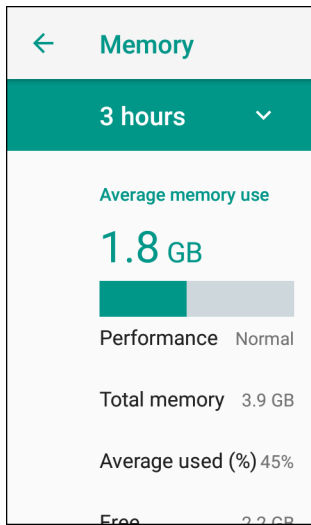
Executing programs use RAM to store data. Data stored in RAM is lost upon a reset. The operating system manages how applications use RAM. It only allows applications and component processes and services to use RAM when required. It may cache recently used processes in RAM, so they restart more quickly when opened again, but it will erase the cache if it needs the RAM for new activities.

1. To view the amount of free and used memory, swipe down from the Status bar to open the Quick Access panel and then touch .



2. Touch **System > Developer options > Memory**.

**Figure 84** Memory Screen




The screen displays the amount of used and free RAM.

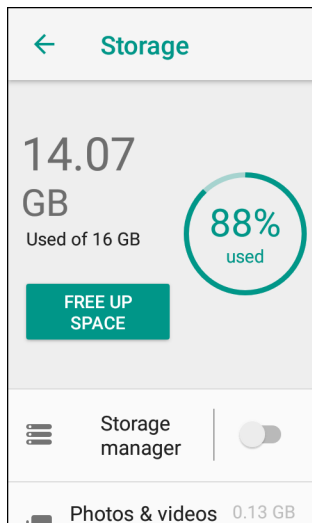
- **Performance** - Indicates memory performance.
- **Total memory** - Indicates the total amount of RAM available.
- **Average used (%)** - Indicates the average amount of memory (as a percentage) used during the period of time selected (default - 3 hours).
- **Free** - Indicates the total amount of unused RAM.
- **Memory used by apps** - Touch to view RAM usage by individual apps.

## Internal Storage

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

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

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Storage**.


**Figure 85** Storage Screen

## Enterprise Folder

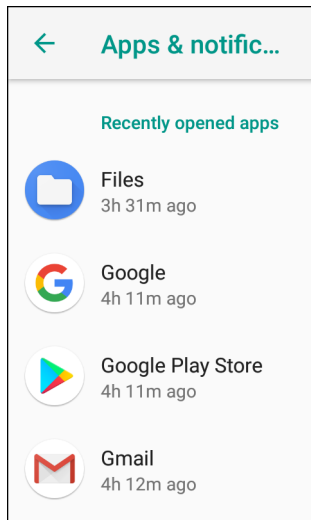
The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 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.

## App Management

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

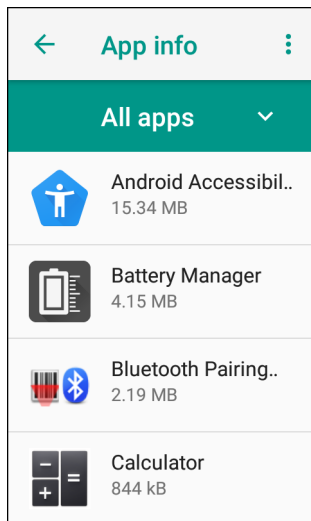
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Apps & notifications**.

**Figure 86** Apps & Notifications Screen



3. Touch **See all XX apps** to view all apps on the device.

**Figure 87** App Info Screen



4. Touch **> Show system** to include system processes in the list.
5. Touch an app, process, or service in the list to open a screen to view its details. Depending on the item, you can change its settings, permissions, notifications, and force stop or uninstall the item.

## Viewing App Details



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

- **Force stop** - stop an app.
- **Disable** - disable an app.
- **Uninstall** - remove the app and all of its data and settings from the device. See [Uninstalling an Application](#) for information about uninstalling apps.
- **Storage** - lists how much information is stored, and includes a button for clearing it.

- **Data usage** - provides information about data (Wi-Fi) consumed by an app.
- **Permissions** - lists the areas on the device that the app has access to.
- **Notifications** - set the app notification settings.
- **Open by default** - clears If you have configured an app to launch certain file types by default, you can clear that setting here.
- **Battery** - lists the amount of computing power used by the app.
- **Memory** - lists the average app memory usage.
- Advanced
  - **Draw over other apps** - allows an app to display on top of other apps.


## Managing Downloads

Files and apps downloaded using the Browser or Email are stored on the Internal storage in the Download directory. Use the Downloads app to view, open, or delete downloaded items.

1. Swipe the screen up and touch .
2. Touch  > **Downloads**.

**Figure 88** Files - Downloads Screen



3. Touch and hold an item, select items to delete and touch . The item is deleted from the device.

# Maintenance and Troubleshooting

## Introduction

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

## Maintaining the Device

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

- To avoid scratching the screen, use a Zebra approved stylus or plastic-tipped pens capacitive touch panel compatible stylus intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the device screen.
- The touch-sensitive screen of the device is glass. Do not drop the device or subject it to strong impact.
- Protect the device from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store the device in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the device. If the surface of the device screen becomes soiled, clean it with a soft cloth moistened with an approved cleanser. For a list of approved cleansers, see Approved Cleanser Active Ingredients.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.

## Battery Safety Guidelines

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Follow battery usage, storage, and charging guidelines found in this guide.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the ambient battery and charger temperatures must be between +32°F and +104°F (0°C and +40°C).
- Do not use incompatible batteries and chargers, including non-Zebra batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact the Global Customer Support Center.
- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- Do not disassemble or open, crush, bend or deform, puncture, or shred the battery.

- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with water for 15 minutes, and seek medical advice.
- If you suspect damage to your equipment or battery, contact Customer Support to arrange for inspection.

## Cleaning Instructions



**CAUTION:** Always wear eye protection.

Read warning label on alcohol product before using.

If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.



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

## Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite<sup>1</sup> (see important note below), hydrogen peroxide, ammonium chloride, or mild dish soap.



**IMPORTANT:** Use pre-moistened wipes and do not allow liquid cleaner to pool.

<sup>1</sup>When using sodium hypochlorite (bleach) based products, always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.

Due to the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidation (corrosion) when exposed to this chemical in the liquid form (including wipes). In the event that these type of disinfectants come in contact with metal on the device, prompt removal with an alcohol-dampened cloth or cotton swab after the cleaning step is critical.

## Harmful Ingredients

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

Many vinyl gloves contain phthalate additives, which are often not recommended for medical use and are known to be harmful to the housing of the device.

### Device Cleaning Instructions

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



**NOTE:** For thorough cleaning, it is recommended to first remove all accessory attachments, such as hand straps or cradle cups, from the mobile device and to clean them separately.

### Special Cleaning Notes

The device should not be handled while wearing vinyl gloves containing phthalates, or before hands are washed to remove contaminant residue after gloves are removed.

If products containing any of the harmful ingredients listed above are used prior to handling the device, such as hand sanitizer that contain ethanalamine, hands must be completely dry before handling the device to prevent damage to the device.



**IMPORTANT:** If the battery connectors are exposed to cleaning agents, thoroughly wipe off as much of the chemical as possible and clean with an alcohol wipe. It is also recommended to install the battery in the terminal prior to cleaning and disinfecting the device to help minimize buildup on the connectors.

When using cleaning/disinfectant agents on the device, it is important to follow the directions prescribed by the cleaning/disinfectant agent manufacturer.

### Cleaning Materials Required

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

### Cleaning Frequency

The cleaning frequency is at the customer's discretion due to the varied environments in which the mobile devices are used and may be cleaned as frequently as required. When dirt is visible, it is recommended to clean the mobile device to avoid build up of particles which make the device more difficult to clean later on.

### Cleaning the Device

#### Housing

Thoroughly wipe the housing, including all buttons and triggers, using an approved alcohol wipe.

#### Display

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

## Exit Window

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

## Cleaning Cradle Connectors

To clean the connectors on a cradle:

1. Remove the DC power cable from the cradle.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not leave any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton-tipped applicator.
5. Remove any lint left by the cotton-tipped applicator.
6. If grease and other dirt can be found on other areas of the cradle, use a 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 applying power to cradle.

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



**CAUTION:** After cleaning the cradle connectors with bleach-based chemicals, follow the Cleaning Cradle Connectors instructions to remove bleach from the connectors.

## Troubleshooting

### EC30


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

**Table 6** *Troubleshooting the EC30*

Problem	Cause	Solution
When pressing the power button the device does not turn on.	Battery not charged.	Charge the battery in the device.
	System crash.	Perform a reset.
When pressing the power button the device does not turn on but two LEDs blink.	Battery charge is at a level where data is maintained but battery should be re-charged.	Charge the battery in the device.



**Table 6** Troubleshooting the EC30 (Continued)

Problem	Cause	Solution
Battery did not charge.	Battery failed.	Contact system administrator.
	Device removed from cradle while battery was charging.	Insert device in cradle. See <a href="#">Charging the Device on page 13</a> .
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0°C (32°F) or above 40°C (104°F).
Cannot see characters on display.	Device not powered on.	Press the <b>Power</b> button.
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	Device disconnected from host computer during communication.	Reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software was incorrectly installed or configured.	Perform setup.
During data communication over Wi-Fi, no data transmitted, or transmitted data was incomplete.	Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
	You moved out of range of an access point.	Move closer to an access point.
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	Bluetooth radio is not on.	Turn on the Bluetooth radio.
	You moved out of range of another Bluetooth device.	Move within 10 meters (32.8 feet) of the other device.
No sound.	Volume setting is low or turned off.	Adjust the volume.
Device shuts off.	Device is inactive.	The display turns off after a period of inactivity. Set to 15 seconds for optimal battery life.
	Battery is depleted.	Contact the distributor or Zebra support.
Tapping the window buttons or icons does not activate the corresponding feature.	The device is not responding.	Reboot the device.
A message appears stating that the device memory is full.	Too many files stored on the device.	Delete unused memos and records. If necessary, save these records on the host computer.
	Too many applications installed on the device.	Remove user-installed applications on the device to recover memory. Select  > <b>Apps</b> . Select the unused application and tap <b>UNINSTALL</b> .

**Table 6** Troubleshooting the EC30 (Continued)

Problem	Cause	Solution
The device does not decode with reading bar code.	Scanning application is not loaded.	Load a scanning application on the device or enable DataWedge. See the system administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Place the device within proper scanning range.
	Device is not programmed for the bar code.	Program the device to accept the type of bar code being scanned. Refer to the EMDK or DataWedge application.
	Device is not programmed to generate a beep.	If the device does not beep on a good decode, set the application to generate a beep on good decode.
	Battery is low.	If the scanner stops emitting an LED beam upon a trigger press, check the battery level. When the battery is low, the scanner shuts off before the device low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or the Global Customer Support Center.
Device cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (32.8 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
Cannot unlock device.	User enters incorrect password.	If the user enters an incorrect password five times, the user is requested to wait for 30 seconds when using a PIN, Pattern or Password.
Some screen contents are not visible.	Some screen contents do not display correctly.	Rotate the device to enable landscape mode.

## 2-Slot Charge Only Cradle

**Table 7** Troubleshooting the 2-Slot Charge only Cradle

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

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

Symptom	Possible Cause	Action
Device battery is not charging.	Device was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure device is seated correctly. Confirm the device is charging. The battery fully charges in less than three hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, contact the distributor or Zebra support
	The device is not fully seated in the cradle.	Remove and re-insert the device into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).



## 10-Slot Charge Only Cradle

**Table 8** Troubleshooting the 10-Slot Charge Only Cradle

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

## 10-Slot SmartLock Charge Only Cradle

**Table 9** Troubleshooting the 10-Slot SmartLock Charge Only Cradle

Problem	Cause	Solution
Cradle is not locking.	Device is not inserted correctly in the cradle.	Remove the device and reinsert it correctly. Verify charging is active. Touch  > <b>System</b> > <b>About phone</b> > <b>Battery Information</b> to view battery status.
	Device has no active connection.	An icon is visible in the status bar if a connection is currently active.
Battery is not charging.	Device removed from the cradle too soon.	Replace the device in the cradle. The battery fully charges in approximately five hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Device is not inserted correctly in the cradle.	Remove the device and reinsert it correctly. Verify charging is active. Touch  > <b>System</b> > <b>About phone</b> > <b>Battery Information</b> to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

# Technical Specifications

## EC30

The following sections provide technical specification for the device.

**Table 10** EC30 Technical Specifications

Item	Description
<b>Physical Characteristics</b>	
Dimensions	Height: 114 mm (4.49 in.) Width: 57 mm (2.24 in.) Depth: 14 mm (0.55 in.)
Weight	110 g (3.88 oz)
Display	3.0" Full Wide Video Graphics Array (854 x 480); 400 Nits maximum; optically bonded to touch panel
Touch Panel	Dual mode capacitive touch with stylus or bare or gloved fingertip input; Corning Gorilla Glass 3
Backlight	Light Emitting Diode (LED)
Battery	Rechargeable Li-Ion, Power Precision+ Standard Capacity, 1200 mAh; improved battery technology for longer cycle times and real-time visibility into battery metrics for better battery management; fast USB charging (500 mA)
Connection Interface	Universal Serial Bus (USB) 2.0 High Speed (host and client)
Network Connections	WLAN, WPAN (Bluetooth)
Notification	Audible tone; multi-color LEDs
Keypad	On-screen keyboard
Voice and Audio	One microphone support with noise suppression; speaker; Bluetooth wireless headset support. Hands-free mode (PTT only); headset mode (PTT and VoIP); HD Voice.
Buttons	Dedicated push-to-talk button, volume up/down buttons, Home button, Power Button, and Scan button.
<b>Performance Characteristics</b>	
CPU	Snapdragon 660 64-bit Hexa-Core 2.2 GHz
Operating System	Android 8.1 Oreo with Zebra's Mobility Extensions (Mx)

**Table 10** EC30 Technical Specifications

Item	Description
Memory	4 GB RAM/32 GB Flash
Output Power	USB - 5 VDC @ 500 mA max
<b>User Environment</b>	
Operating Temperature	0°C to 50°C (32°F to 122°F)
Relative Humidity	Operating: 5 to 95% non-condensing
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0° C to 40° C (32°F to 104°F)
Humidity	5 to 85% non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) to smooth concrete over 0°C to 50°C (14°F to 122°F).
Tumble	1000 0.5 m (1.6 ft.) tumbles; meets and exceeds IEC tumble specifications
Sealing	IP54 per applicable IEC sealing specifications
Electrostatic Discharge (ESD)	+/-20 kVDC air discharge, +/-10 kVDC direct discharge, +/- 10 kVDC indirect discharge
Vibration	IEC 60721-3-3 - Dynamic conditions per class 3M2
Thermal Shock	-40°C to 70°C (-40°F to 158°F) rapid transition
<b>Interactive Sensor Technology (IST)</b>	
Motion Sensor	3-axis accelerometer with MEMS Gyro
Magnetometer	eCompass automatically detects direction and orientation.
<b>Wireless LAN Data and Voice Communications</b>	
Radio	IEEE 802.11a/b/g/n/ac/d/h/i/k/r/w; Wi-Fi <sup>™</sup> certified; IPv4, IPv6; 2X2 MIMO
Data Rates Supported	5GHz: 802.11a/n/ac - up to 866.7 Mbps 2.4GHz: 802.11b/g/n - up to 144 Mbps
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
Security and Encryption	WEP (40 or 104 bit); WPA/WPA2 Personal (TKIP, and AES); WPA/WPA2 Enterprise (TKIP and AES) — EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0-MSCHAPv2, PEAPv1-EAP-GTC and LEAP Data in Motion: FIPS 140-2 Level 1 Data at Rest: FIPS 140-2 Level 1
Certifications	WFA (802.11n, 802.11ac, WMM-AC, Voice Enterprise, WMM-PS), Miracast
Fast Roam	PMKID caching; Cisco CCKM; 802.11r; OKC

**Table 10** EC30 Technical Specifications

Item	Description
<b>Wireless PAN Data and Voice Communications</b>	
Bluetooth	Class 2, Bluetooth v5.0 (Bluetooth Smart technology); Bluetooth Wideband support HFPv1.6; Bluetooth v5.2 Low Energy (LE)
<b>Data Capture Specifications</b>	
Scanning	SE2100 imager (1D and 2D) with LED aimer.
<b>2D Imager Engine Specifications</b>	
Field of View	Horizontal - 41.5° Vertical - 31.7°
Image Resolution	640 horizontal X 480 vertical pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles (107,639 lux)
Focal Distance	From front of engine: 10.7 cm (4.2 in.)
Illumination System	LEDs: Ultra white Pattern Angle: 42° horizontal, 32.0° vertical at 50% intensity

**Table 11** Data Capture Supported Symbolologies

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

## Decode Distances

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

**Table 12** SE2100 Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
5.0 mil Code 128	2.0 in. 5.1 cm	4.8 in. 12.2 cm
5 mil Code 39	1.7 in. 4.3 cm	5.8 in. 14.7 cm
6.6 mil PDF417	1.6 in. 4.1 cm	4.9 in. 12.4 cm

Table 12 SE2100 Decode Distances (Continued)

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
10 mil Data Matrix	1.2 in. 3.0 cm	4.9 in. 12.4 cm
100% UPCA	2.0 in. 5.1 cm	10.3 in. 26.2 cm
20 mil Code 39	2.1 in. 5.3 cm*	13.0 in. 33.0 cm
10 mil QR Code	1.1 in. 2.8 cm	5.2 in. 13.2 cm
<p>*Limited by width of bar code in field of view.</p> <p>Notes: Photographic quality bar code at 15° tilt pitch angle under 30 fcd ambient illumination.</p> <p>Distances measured from front edge of scan engine chassis.</p>		

## I/O Connector Pin-Outs

Figure 89 I/O Connector

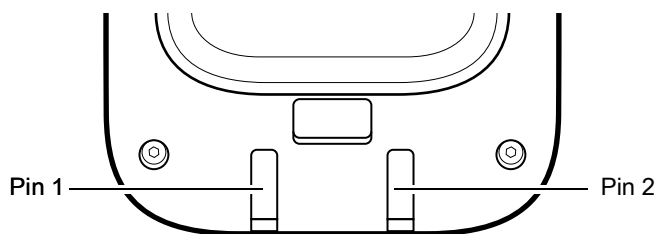


Table 13 I/O Connector Pin-Outs

Pin	Signal	Description
1	GND	Power / signal ground.
2	Cradle_IN	Cradle power / communication signal.

## 2-Slot Charge Only Cradle Technical Specifications

Table 14 2-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 10.6 cm (4.17 in.) Width: 19.56 cm (7.70 in.) Depth: 13.25 cm (5.22 in.)
Weight	748 g (26.4 oz.)
Input Voltage	12 VDC



**Table 14** 2-Slot Charge Only Cradle Technical Specifications

Item	Description
Power Consumption	30 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10 kV contact +/- 10 kV indirect discharge

## 10-Slot Charge Only Cradle Technical Specifications

**Table 15** 10-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 90.1 mm (3.5 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)
Weight	1.31 kg (2.89 lbs.)
Input Voltage	12 VDC
Power Consumption	65 watts 90 watts with 4-Slot Battery Charger installed.
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

## 10-Slot SmartLock Charge Only Cradle Technical Specifications

**Table 16** 10-Slot SmartLock Charge Only Cradle Technical Specifications

Item	Description
Dimensions	Height: 90.1 mm (3.5 in.) Width: 449.6 mm (17.7 in.) Depth: 120.3 mm (4.7 in.)
Weight	1.31 kg (2.89 lbs.)
Input Voltage	12 VDC
Power Consumption	65 watts 90 watts with 4-Slot Battery Charger installed.
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

# Index

## A

advanced data formatting rules	96
approved cleanser	134
approved cleanser active ingredients	134
apps	
RxLogger	51
RxLogger Utility	57

## B

barcode input	72
enabled	72
battery safety guidelines	133

## C

cleaning	134, 135
camera and exit window	136
cradle connectors	136
display	135
frequency	135
housing	135
instructions	134
materials	135
cleaning instructions	135
cradle	
connector cleaning	136

## D

data capture plus	70
datawedge	
advanced data formatting rules	96
APIs	107
associating applications	68
auto import	106
auto switch to default on event	73
barcode input	72
configuration and profile file management	106
configuring ADF plug-in	96
creating a new profile	67

data capture plus	70
decoders	73
disabling	67
enterprise folder	106
exporting a configuration file	105
hardware trigger	72
importing a configuration file	104
input plugins	65
intent output	90
intent overview	91
introduction	63
IP output	92
keep enabled on suspend	88
keystroke output	89
multibarcodes params	88
options menu	67
output plug-ins	65
plug-ins	64
process plug-ins	65
profile configuration	68
profile context menu	66
profile0	64
profiles	64
profiles screen	65
programming notes	106
reader params	84
reporting	107
scan params	87
scanner selection	72
settings	104
UDI params	88
UPC EAN params	82
voice input	88
decoder params	
Codabar	76
Code 11	76
Code 128	76
Code 39	77
Code 93	78
Composite AB	78
decode lengths	81
Discrete 2 of 5	78

DotCode	78
GS1 DataBar Limited	79
HAN XIN	79
Interleaved 2 of 5	79
Matrix 2 of 5	79
MSI	80
UK Postal	80
UPCA	80
UPCE0	81
UPCE1	81
US Planet	81
decoders	73
disconnect host computer	62

## F

file transfer	61
---------------	----

## H

hard reset	15
harmful ingredients	134

## M

maintenance	133
approved cleanser active ingredients	134
battery safety guidelines	133
clean camera and exit window	136
clean cradle connectors	136
clean display	135
clean housing	135
cleaning frequency	135
cleaning instructions	134
cleaning materials required	135
device cleaning instructions	135
harmful ingredients	134
maintaining the device	133
special cleaning notes	135
multibarcodes params	88

## N

notational conventions	11
------------------------	----

## P

photo transfer	62
----------------	----

## R

reader params	84
reset device	14
hard reset	15

soft reset	14
RxLogger	51
configuration	51
configuration file	56
disable logging	56
enable logging	56
extract log files	56
RxLogger Utility	57

## S

scan params	87
scanning	63
settings	
datawedge	104
soft reset	14
software version	11
software versions	10
symbolologies	143

## T

transferring files using USB	61
troubleshooting	136

## U

UDI params	88
UPC EAN params	82
USB	61

## V

voice input	88
-------------	----

## W

Wi-Fi direct	43
WPS pin entry	45
WPS push button	44

