# PS20

## Personal Shopper


# Product Reference Guide

for Android ™ 8.1 Oreo

ZEBRA

MN-003238-04EN Rev A

# Copyright



# 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 | 09/2018 | Initial release. |
| -02 Rev A | 11/2018 | Add support for MR1 release. |
| -03 Rev A | 04/2019 | Various updates. |
| -04 Rev A | 09/2021 | Update GMS Restricted. |

# Table of Contents

**Index**

# About This Guide

## Introduction

This guide provides information about setting up and configuring the device with an Android operating system and installing its accessories.

**NOTE:** Some screens or windows shown in this guide may differ from the actual screens shown on the device.

## Configurations

This guide covers the following configurations:

*Table 1*

| Configuration | Radios | Display | Memory | Data Capture Options | Operating System |
|---|---|---|---|---|---|
| PS20 Base | WLAN: 802.11 a/b/g/n/d/h/i/k/r/v/ac<br>WPAN: Bluetooth v5.0 | WVGA 4.0" color | 4 GB RAM/16 GB Flash | SE2100 | Android Open Source Project (AOSP)/ Google Mobile Services (GMS) 8.1 |
| PS20 Plus | WLAN: 802.11 a/b/g/n/d/h/i/k/r/v/ac<br>WPAN: Bluetooth v5.0 | WVGA 4.0" color | 4 GB RAM/16 GB Flash | SE4710 + Digimarc | Android Open Source Project (AOSP)/ Google Mobile Services (GMS) 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**
   - **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, describes the features and basic operation of the device, lists the accessories for the device and explains how to install and charge the batteries and start the device for the first time.
- Using the Device, provides basic instructions for using the device with an Android OS.
- Wireless, provides instructions for setting up WLAN and Bluetooth connections.
- Applications, provides information on various apps pre-installed on the device.
- Data Capture, provides information for capturing barcode data.
- Cradle Installation, provides installation instructions for the cradles and other accessories.
- USB Communication, provides instructions for connecting the device to a host computer.
- DataWedge, provides information for configuring DataWedge.
- Application Deployment, provides instructions for downloading software and files to the device.
- Settings, provides various setting for the device.
- Maintenance and Troubleshooting, includes instructions on cleaning and storing the device, and provides troubleshooting solutions for potential problems during operation.
- Specifications, includes a table listing the technical specifications for the device and accessories.

# 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 and Software

The following documents provide more information about the PS20 Personal Shopper:

- PS20 Personal Shopper Quick Start Guide, p/n MN-003318-XX
- PS20 Regulatory Guide, p/n MN-003276-XX

For the latest version of this guide and all guides, go to: 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.

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.

## Provide Documentation Feedback

If you have comments, questions, or suggestions about this guide, send an email to EVM-Techdocs@zebra.com.

# Getting Started

## Introduction

This chapter describes the features of the PS20 and explains how to install and charge the battery, how to capture data using the integrated Imager and how to reset the PS20.

## Unpacking

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

Verify that the box contains all the equipment listed below:

- PS20 (includes lithium-ion battery)
- Regulatory Guide

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact Support immediately. See Service Information on page 17 for contact information.

### Removing the Screen Protection Film

A screen protection film is applied to the PS20 screen to protect the screen during shipping. To remove the screen protector, carefully lift the thin film off the touch screen display.

# Features

Figure 1 Features - Front View

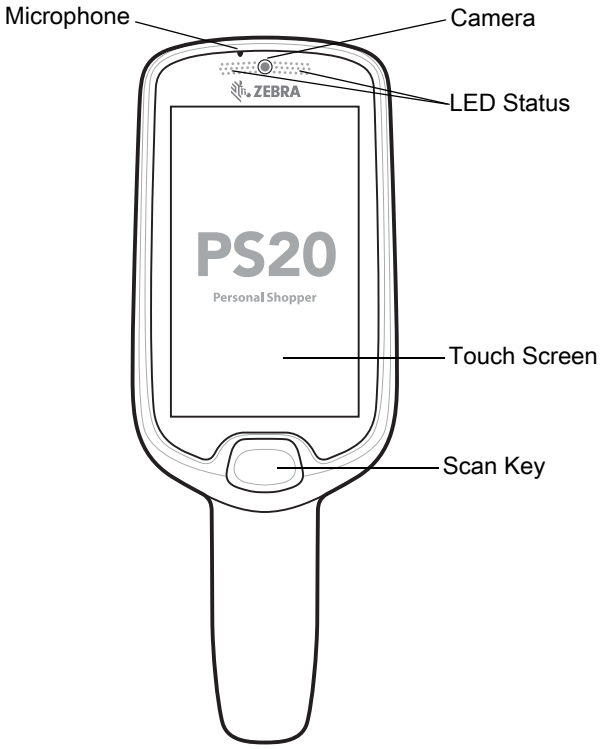



*Table 2 Features- Front View*

| Item | Function |
|---|---|
| Microphone | Use for audio input and SmartLens locationing. Allows shoppers to speak to a store associate via push-to-talk or to a virtual assistant via speech-to-text. |
| Camera | With the front-facing camera, the device supports Visible Light Communications (VLC) indoor positioning/locationing applications. In addition, the camera is used for image/face recognition. Available on Plus configurations. |
| LED Status | Indicates the battery charge state while charging or the scan/decode status.<br>Red: Barcode scan in progress (Scan key is pressed).<br>Single Green Blink: Successful decode. |
| Touch Screen | Displays all information needed to operate the device. |
| Scan Key | Use for trigger input for scanner or as a Select/Enter key. |

Figure 2 Features - Back and Side View

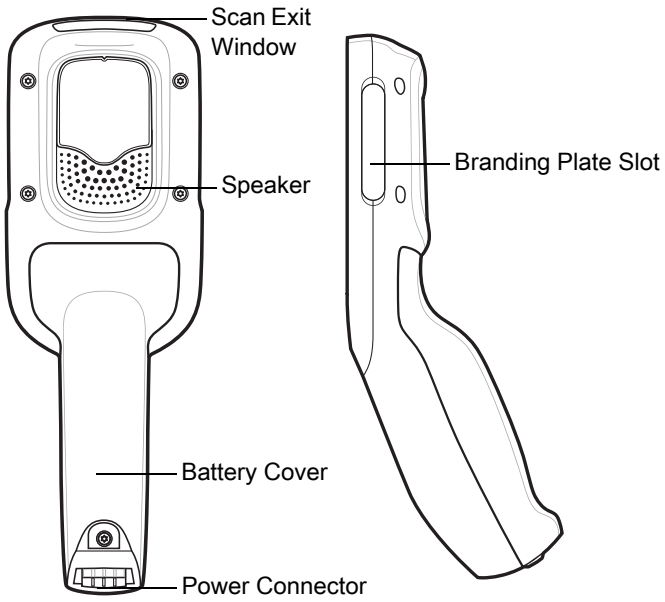



*Table 3 Features*- Back and Side View

| Item | Function |
|---|---|
| Scan Exit Window | Provides data capture using the scanner. |
| Speaker | Provides audio output for video, music, notifications, and PTT. |
| Battery Cover | Encloses the battery and attaches to the device's handle. |
| Power/Cradle I/OConnector | Provides charging via cradle and cradle communication to lock/unlock the cradle slots. Use to perform a hard reset with the terminal reboot tool. |
| Branding Plate Slot | Provides space for custom logo. |

# Accessories

*Table 4 Accessories*

| Accessory | Part Number | Description |
|---|---|---|
| PS20 Lithium Ion Battery | BTRY-PS20-35MA-01 | PS20 PowerPrecision+ Lithium Ion Battery. |
| | BTRY-PS20-35MA-10 | PS20 PowerPrecision+ Lithium Ion Battery (QTY-10). |
| High Density (HD) Three Slot Cradle (Locking). | CRD-MC18-3SLCKH-01 | The cradle is used for docking up to three PS20 units in HD installation configuration. The cradle slots are equipped with a mechanism that locks the PS20 units inside the slots. The devices are placed with the display facing to the front. Requires power supply unit (PWR-BGA12V108W0WW), DC line cord and country specific AC line cord (sold separately). |
| High Density (HD) Three Slot Cradle (Non-Locking) | CRD-MC18-3SLOTH-01 | The cradle is used for docking up to three PS20 units in HD installation configuration. The devices are placed with the display facing to the front. Requires power supply unit (PWR-BGA12V108W0WW), DC line cord and country specific AC line cord (sold separately). |
| Super High Density (SHD) Three Slot Cradle (Locking) | CRD-MC18-3SLCKS-01 | The cradle is used for docking up to three PS20 units in SHD installation configuration. The cradle slots are equipped with a mechanism that locks the PS20 units inside the slots. The devices are placed with the display facing up. Requires power supply unit (PWR-BGA12V108W0WW), DC line cord and country specific AC line cord (sold separately). |
| Single Slot Cradle | CRD-MC18-1SLOT-01 | The cradle is used for docking a single PS20. The devices are placed with the display facing to the front. Requires power supply unit (PWR-BGA12V108W0WW), DC line cord and country specific AC line cord (sold separately). |
| Release Key | KT-MC18-CKEY-20 | Tool used to mechanically unlock the PS20 from the Three Slot Cradle and the Single Slot Cradle (QTY-20). |
| Terminal Reboot Tool | KT-MC18-REBOOT-05 | Tool used to perform cold boot of the PS20 (QTY-5). |
| Cradle Cover Removal Tool | KT-MC18-CTOOL-01 | Tool used for removing the Three Slot Cradle cover. |

*Table 4 Accessories (Continued)*

| Accessory | Part Number | Description |
|---|---|---|
| Deployment Kit | KT-MC18-CSTKIT-01 | PS20 Deployment Starter Kit. Includes:<br>20-pack of Release Key (KT-MC18-CKEY-20)<br>5-pack of Terminal Reboot Tool KT-MC18-REBOOT-05)<br>One Three Slot Cradle Cover Removal Tool (KT-MC18-CTOOL-01) |
| Cart Holder Mounting Kit | PSS-3SH01-00R | Kit for mounting the PS20 on a shopping cart. |
| Soft Holster | SG-PS20-SFTHLT-01 | Allows for wearing the PS20 on the hip (includes belt clip) or crossbody, with an additional shoulder strap. |
| Tempered Glass Screen Protector | MISC-PS20-SCRN-05 | Provides additional protection for PS20 display (5-pack). |
| Programming Cable | CBL-PS20-USBCHG-01 | PS20 USB communication cable for connecting the device to a host computer. |
| Interconnection Cable Long | 25-66430-01R | PS20 cradle interconnection cable (60 Inch / 1.5 Meter). Connects cradles to each other to run off one power supply unit (PWR-BGA12V108W0WW). |
| Interconnection Cable Short | 25-66431-01R | PS20 cradle interconnection cable (12.6 Inch / 32 centimeter). Connects cradles to each other to run off one power supply unit (PWR-BGA12V108W0WW). |
| Cradle Interconnection Extension Cable | CBL-MC18-EXINT1-01 | PS20 cradle interconnection extension cable (12.6 Inch / 32 centimeter). Connects two interconnection cables (25-66431-01R sold separately) together to provide additional length which might be required in some installation designs. |
| DC Charging Cable | CBL-DC-394A1-01 | DC charging cable (19.5 Inch / .5 Meter) used to connect a power supply unit (PWR-BGA12V108W0WW) to one Single Slot Cradle. |
| DC “Y” Charging Cable Long | CBL-DC-392A1-02 | DC “Y” charging cable (79.4 Inch / 2 Meter). Connects a power supply unit (PWR-BGA12V108W0WW) to two separate Three Slot Cradles. |
| DC “Y” Charging Cable Short | CBL-DC-393A1-02 | DC “Y” charging cable (39.7 Inch / 1 Meter). Connects a power supply unit (PWR-BGA12V108W0WW) to two separate Three Slot Cradles. |
| Power Supply Unit | PWR-BGA12V108W0WW | 100-240VAC, 12VDC, 9A. Requires country specific AC line cord and DC cable (sold separately). |

*Table 4 Accessories (Continued)*

| Accessory | Part Number | Description |
|---|---|---|
| AC Line Cord | 23844-00-00R | AC Line Cord, 7.5 feet long, grounded, three wire for power supplies. Associated Country: United States |
| AC Line Cord | 50-16000-221R | AC Line Cord, 1.8 meter, meter grounded, three wire, USA NEMA 5-15P. Associated Country: United States |
| AC Line Cord | 50-16000-671R | AC Line Cord, 1.8 meter, grounded, three wire, CIE 23-16 plug. Associated Country: Italy. |
| AC Line Cord | 50-16000-217R | AC Line Cord, 1.9 meter, grounded, three wire, AS 3112 plug. Associated Countries: Australia, New Guinea |
| AC Line Cord | 50-16000-218R | AC Line Cord, 1.8 meter, grounded, three wire, NEMA 1-15P plug. Associated Country: Japan. |
| AC Line Cord | 50-16000-219R | AC Line Cord, 1.8 meter, grounded three wire, BS1363 plug. Associated countries: Hong Kong, Iraq, Malaysia, Singapore, United Kingdom. |
| AC Line Cord | 50-16000-220R | AC Line Cord, 1.8 meter, grounded three wire CEE 7/7plug. Associated countries: Europe, Abu Dhabi, Bolivia, Dubai, Egypt, Iran, Russia, Vietnam. |
| AC Line Cord | 50-16000-257R | AC Line Cord, 1.8 meter, grounded three wire, IEC 60320 C13 plug. Associated Country: China. |
| AC Line Cord | 50-16000-669R | 1.9 meter grounded three wire, BS 546 Plug. Associated country: India. |
| AC Line Cord | 50-16000-672R | 1.9 meter grounded three wire, S132 Plug. Associated country: Israel. |
| AC Line Cord | 50-16000-678R | 36 inch grounded three wire.<br>Associated country: United States |

# Status LED

The Status LED indicates imaging and charging status.

Figure 3 PS20 Status LED

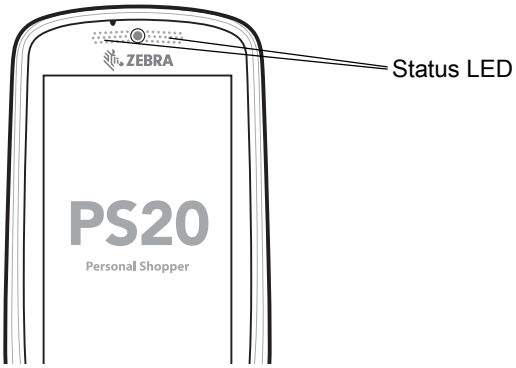


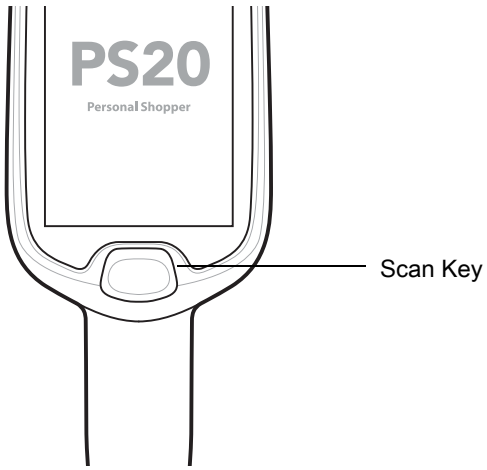

*Table 5 Status LED Indications*

| LED State | Indication |
|---|---|
| **Imaging** | |
| Off | Normal operation or PS20 is turned off. |
| Red | Imaging in progress (Scan key is pressed). |
| Single Green Blink | Successful decode. |
| **Charging (PS20 docked in cradle)** | |
| Off | Power not applied to cradle.<br>PS20 not inserted properly.<br>Charging LED feature disabled. |
| Blinking Green | Charging. |
| Solid Green | Charging complete. |
| Blinking Red | Charging error, for example:<br>Temperature is too low or too high.<br>Charging has gone on too long without completion (typically eight hours). |

# Scan Key

The Scan key operates the imager when a scanning application is active. When the PS20 is turned off, press the Scan key for three seconds to power on the PS20.

Figure 4 Scan Key




# Setup

To start using the device for the first time:

- Charge the battery 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 in a powered USB cable. Fully charging the battery pack to 100% is recommended immediately after exiting ship mode to calibrate the state of charge.

# Charging the Battery

Use one of the following accessories to charge the PS20.

Table 6 Charging Cradles

| Description | Part Number | Cables | | |
|---|---|---|---|---|
| | | DC Cable | Interconnect Cable | Extension Cable |
| Single Slot Cradle | CRD-MC18-1SLOT-01 | CBL-DC-394A1-01<br>CBL-DC-393A1-02<br>CBL-DC-392A1-02 | 25-66431-01R<br>25-66430-01R | ____ |
| High Density (HD) Three Slot Cradle (Locking) | CRD-MC18-3SLCKH-01 | CBL-DC-394A1-01<br>CBL-DC-393A1-02<br>CBL-DC-392A1-02 | 25-66431-01R<br>25-66430-01R | CBL-MC18-EXINT1-01 |
| High Density (HD) Three Slot Cradle (Non-Locking) | CRD-MC18-SLOTH-01 | CBL-DC-394A1-01<br>CBL-DC-393A1-02<br>CBL-DC-392A1-02 | 25-66431-01R<br>25-66430-01R | CBL-MC18-EXINT1-01 |
| Super High Density (HD) Three Slot Cradle (Locking) | CRD-MC18-3SLCKS-01 | CBL-DC-394A1-01<br>CBL-DC-393A1-02<br>CBL-DC-392A1-02 | 25-66431-01R<br>25-66430-01R | CBL-MC18-EXINT1-01 |

**NOTE:** Ensure that you follow the guidelines for battery safety described in the PS20 Product Reference Guide.

1. To charge the battery, connect the charging accessory to the appropriate power source.
2. Insert the PS20 into a cradle. The PS20 turns on and begins charging.

Figure 5 Single Slot Cradle

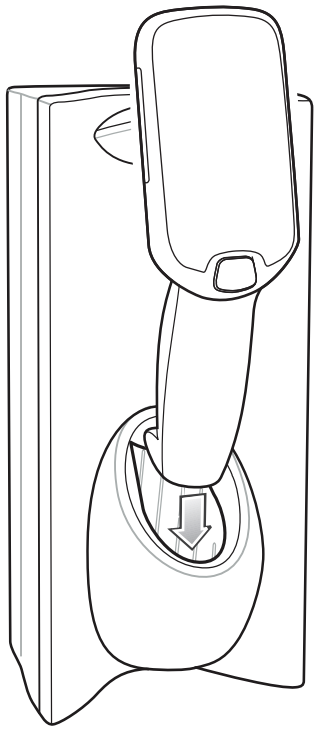
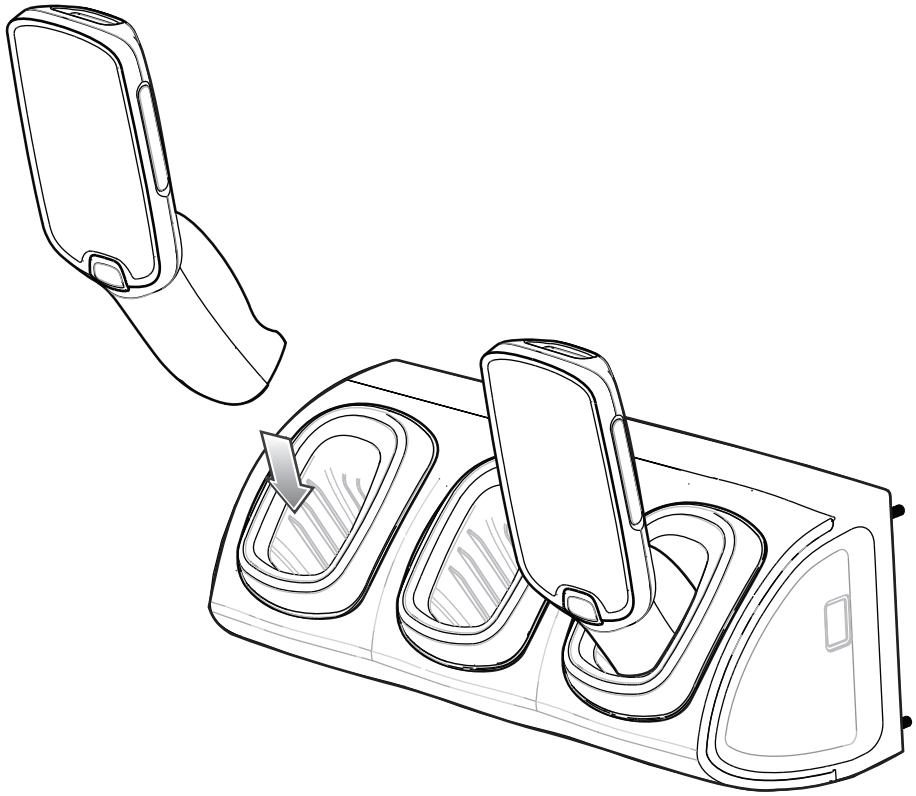


Figure 6 Three Slot Cradle



The battery charges 0 to 90% depending on the following conditions, measured at room temperature:

- When connected to a 1.0 cradle (normal charge mode), charge time is less than four hours.
- When connected to a 1.5 cradle (fast charge mode), charge time is less than three hours.

**NOTE:** To charge the battery in the device, it is recommended to use a charging cradle instead of the USB cable, since it is more time efficient.

## Charging Temperature

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

## LED Status Indicators

By default, the charging LED indication is disabled.

To enable the charging LED indication:

1. Swipe down from the status bar to open the quick access panel and then touch ⚙.
2. Touch **Display**.
3. Touch **Charging LED**. The option switch turns green.
4. Touch ◯.

*Table 7 LED Status Indicators*

| LED State | Indication |
|---|---|
| **Imaging** | |
| Off | Normal operation or PS20 is turned off. |
| Red | Imaging in progress (Scan key is pressed). |
| Single Green Blink | Successful decode. |
| **Charging (PS20 docked in cradle)** | |
| Off | Power not applied to cradle.<br>PS20 not inserted properly.<br>Charging LED feature disabled. |
| Blinking Green | Charging. |
| Solid Green | Charging complete. |
| Blinking Red | Charging error, for example:<br>Temperature is too low or too high.<br>Charging has gone on too long without completion (typically eight hours). |

# Replacing the Battery

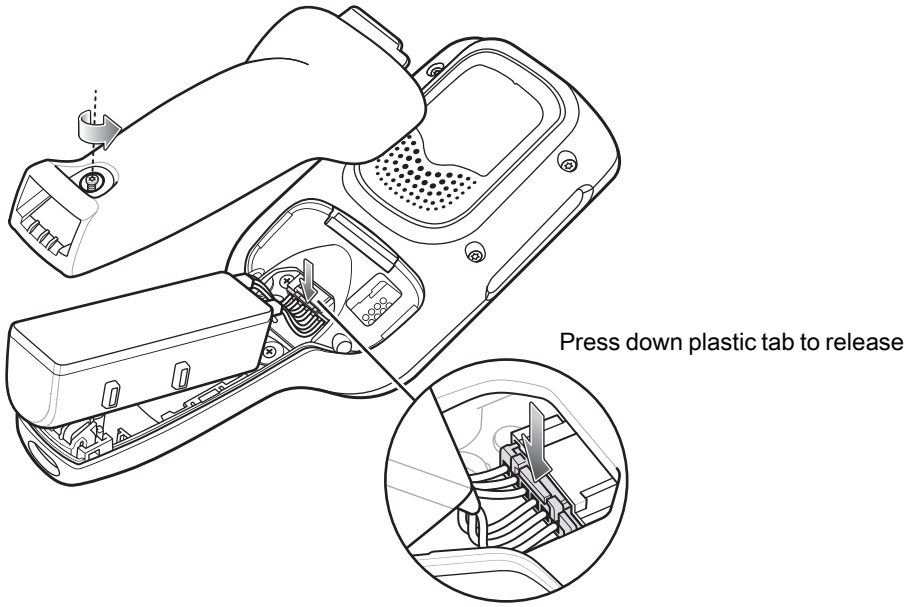
To replace the battery:

1. Touch and hold the soft power button until the menu appears.
2. Touch **Power Off**.
3. Touch **OK**.

**CAUTION:** The PS20 must be off before removing the battery. Failing to turn off the PS20 before removing the battery may damage the data stored on flash memory or corrupt the operating system files.

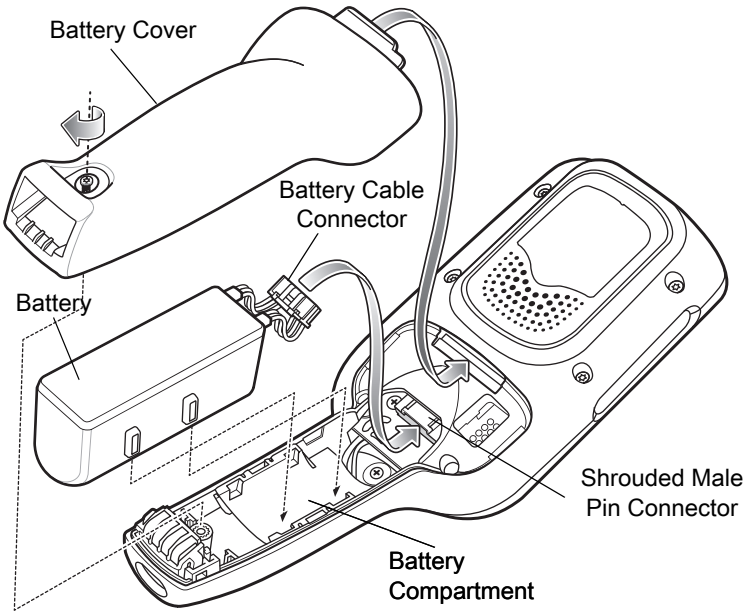
4. Loosen the captive screw that secures the battery cover, using a Phillips (PH00) screwdriver.
5. Lift the battery cover from the handle.
6. Inside the battery compartment, press down the plastic tab of the battery cable connector and slide it out of the shrouded male pin connector.
7. Remove the battery from the battery compartment.

Figure 7 Remove the Battery




8. With the replacement battery, guide and press the battery cable connector into the shrouded male pin connector inside the battery compartment. The connector is designed to only fit one way.
9. Place the battery inside the battery compartment.
10. Place the battery cover onto the handle.
11. Secure the battery cover with the screw, using a Phillips (PH00) screwdriver.

Figure 8 Installing the Battery




# Compatibility

The table below displays compatibility between the PS20 and MC18 devices and accessories.

Table 8 Compatibility

| | PS20 Batteries | MC18 Batteries | MC18 Cradles |
|---|---|---|---|
| PS20 | Yes | No | Yes |
| MC18 | No | Yes | Yes |

- PS20 PowerPrecision+ batteries are compatible with all PS20 devices and MC18 Single Slot and Three Slot cradles.
- PS20 PowerPrecision+ batteries are not compatible with MC18 devices.
- MC18 PowerPrecision+ batteries are not compatible with PS20 devices.

# Battery Comparison

The table below displays a comparison of the PS20 batteries with the MC18 batteries.

Table 9 Battery Comparison

| Feature | MC18 | PS20 |
|---|---|---|
| Battery Type | PowerPrecision+ | PowerPrecision+ |
| Battery Capacity | 2,275 mAh | 3,500 mAh |
| Charging Mode | Standard and Fast | Standard and Fast |

# Powering on the Device

The PS20 starts automatically as soon as power is applied; either with a charged battery installed or when inserted into the cradle.

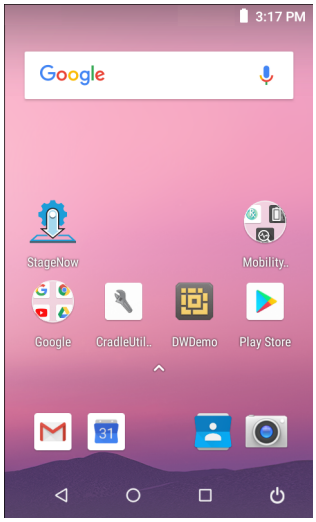
If charged battery is installed and the PS20 is turned off, press the Scan key to turn on.

When the PS20 is powered on for the first time, it initializes its system. The splash screen appears for a short period of time.

Figure 9 Splash Screen


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

Figure 10 Home Screen




## Google Account Setup

**NOTE:** The device has to be connected to the internet in order to set up a Google™ account. A Google account is only required on devices with GMS software.

The first time the device starts, the Setup Wizard displays. Follow the on-screen instructions to set up a Google account, configure Google Pay ™ for purchasing items from the Google Play ™ store, to enter your personal information, and enable backup/restore features.

# Zebra Visibility Services

The device captures and provides device analytics to a system administrator. The first time the device boots (or after a Factory reset), the **Zebra Services** agreement screen displays.

Figure 11 Zebra Services


Touch the **Device Data** switch to disable the device from sending analytics data.

# Releasing the PS20 from the Charging Cradles

Use one of the following methods to release the PS20 from the charging cradles:

- Software Release Using the Menu
- Software Release Using the Cradle Utility
- Manual Release using a Release Key.

**NOTE:** Devices can also be removed via any customer application that used the EMDK personal shopper interface.

## Software Release Using the Menu

The PS20 cradles contain a locking mechanism that locks the PS20 inside the cradle when docked. The PS20 releases from the cradle when a software command is received from the system.

To remove the PS20 from the cradle using the menu:

1. Touch and hold the soft power button until the menu appears.
2. Touch **Cradle unlock**. The cradle unlocks the PS20.
3. Remove the PS20 from the cradle.

## Software Release Using the Cradle Utility

The PS20 cradles contain a locking mechanism that locks the PS20 inside the cradle when docked. The PS20 releases from the cradle when a software command is received from the system.

To remove the PS20 from the cradle using the Cradle Utility:

1. On the Home screen, swipe up from the bottom of the screen.
2. Touch **CradleUtility**.
3. Tap the **CRADLE UNLOCK** tab to set the cradle unlock information.
4. Touch **Unlock Cradle**.

## Manual Release Using a Release Key

The PS20 cradles contain a locking mechanism that locks the PS20 inside the cradle when docked. If the PS20 fails to unlock during normal operation, use a release key (KT-MC18-CKEY-20) to unlock the PS20.

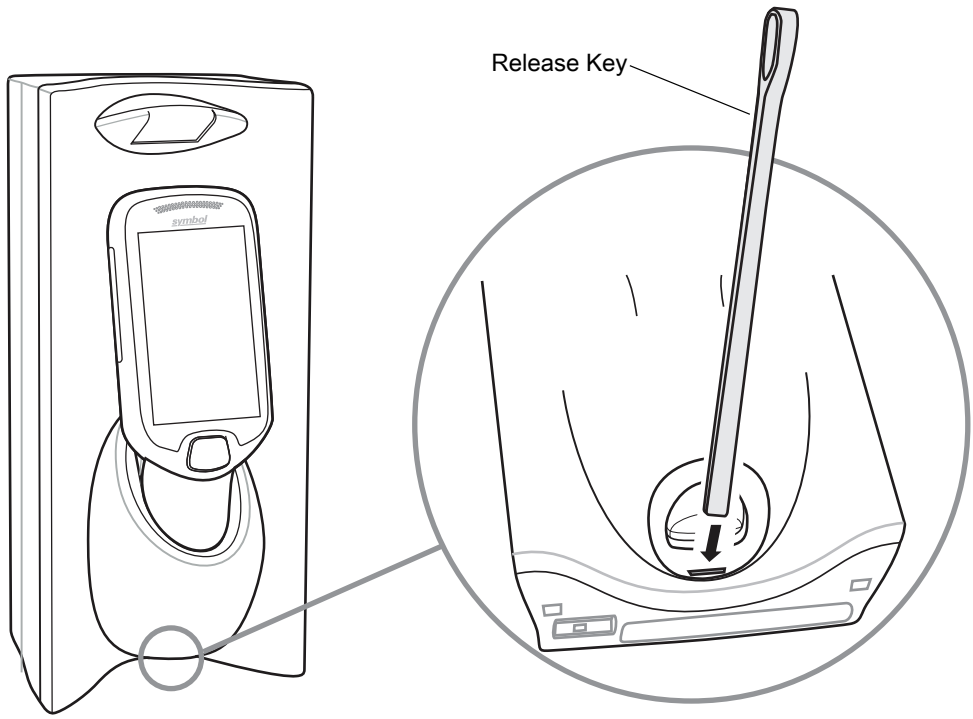
**CAUTION:** Do not use any device to unlock the cradle other than the tools described below. Failure to comply could result in damage to the cradle and void the warranty.

### Manual Release of the PS20 from the Single Slot Cradle

To release a locked PS20 from a Single Slot Cradle:

1. Insert the release key into the slot located at the bottom side of the cradle.
2. While pressing the release key all the way into the slot, remove the PS20 from the cradle.

Figure 12 Manual Release of PS20 from a Single Slot Cradle

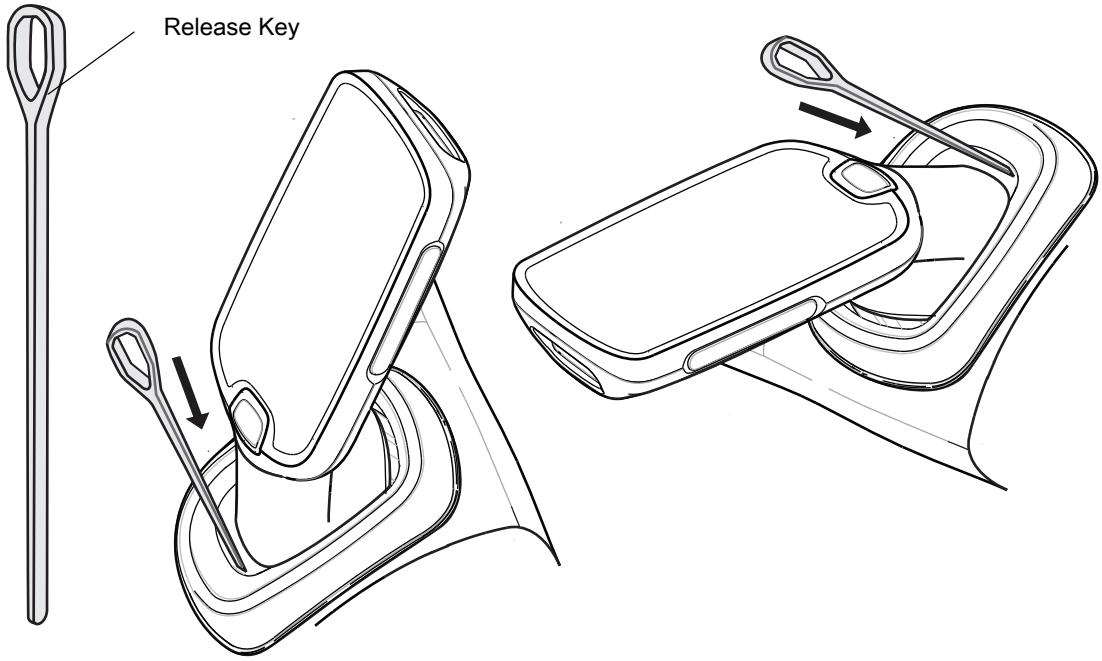


### Manual Release of the PS20 from the Three Slot Cradle

To release a locked PS20 from a Three Slot Cradle:

1. Insert the release key straight into the slot, to a point where the bend stops.
2. Hold the release key pressed inside the slot and remove the PS20 from the slot.

Figure 13 Manual Release of the PS20 from a Three Slot Cradle




# USB Cable Battery Cover

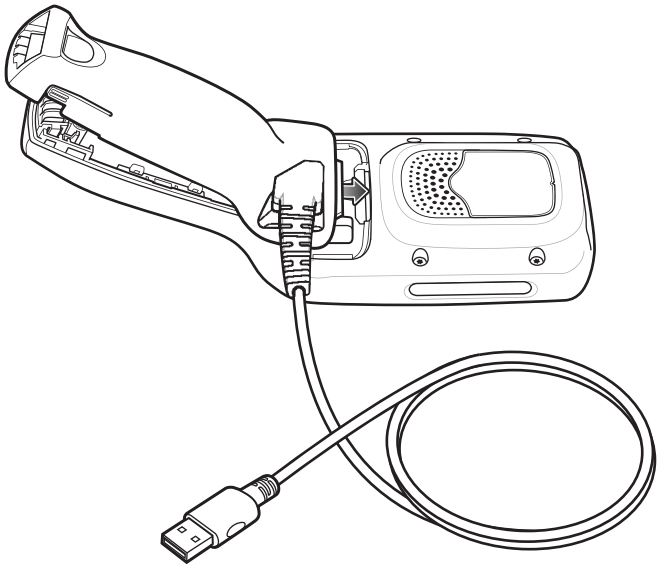
## Installing the USB Cable Battery Cover

Use the USB Cable Battery Cover to connect the device to a host computer.

To install the USB Cable Battery Cover:

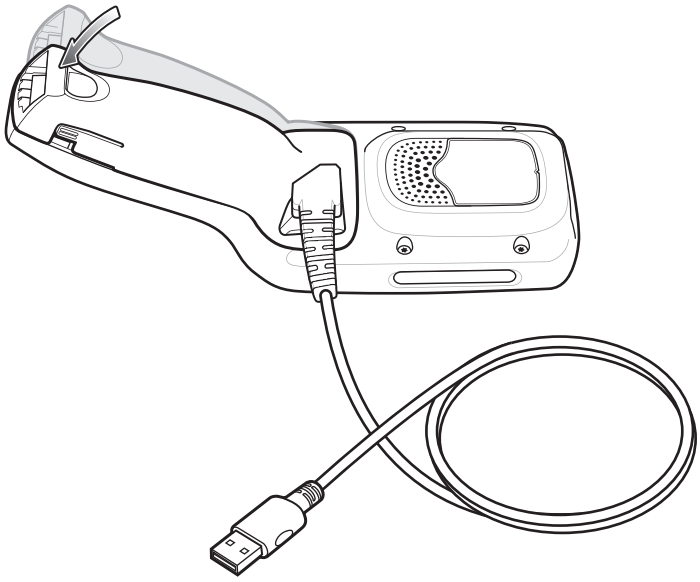
1. Remove the standard battery cover that comes installed on the device, if it is not already removed.
   a. Loosen the captive screw that secures the battery cover, using a Phillips (PH00) screwdriver.
   b. Lift the battery cover from the handle.
2. Slide the tab on the top of the USB Cable Battery Cover into the slot on the back of the device.

Figure 14 Install USB Cable Battery Cover - Top



3. Push the bottom of the USB Cable Battery Cover down, until it snaps into place.

Figure 15 Install USB Cable Battery Cover - Bottom

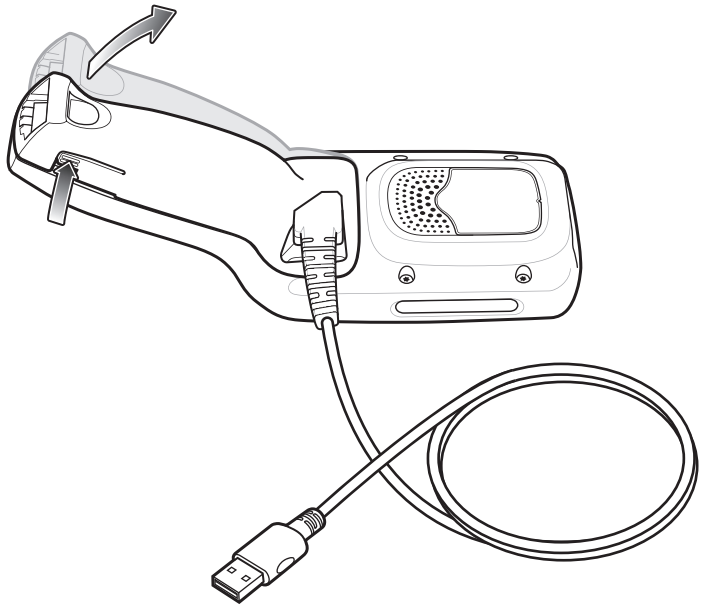


## Removing the USB Cable Battery Cover

To remove the USB Cable Battery Cover:

1. Squeeze the left and right tabs in on the bottom of the USB Cable Battery Cover.
2. Lift the bottom of the USB Cable Battery Cover up.
3. Slide the top of the USB Cable Battery Cover out to remove.

Figure 16 Remove USB Cable Batter Cover



# Soft Holster

The soft holster provides a holder for the MC18/PS20 and allows for wearing the device on the hip, using a belt clip, or crossbody, using the detachable shoulder strap.

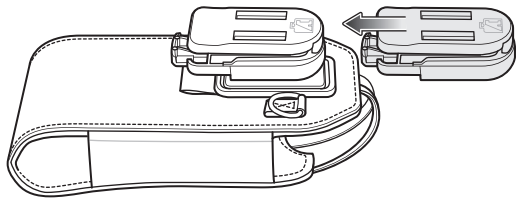
Always place the device with the correct orientation when using the soft holster with a belt clip or shoulder strap, as shown in the following diagrams.

## Using the Belt Clip

To attach the soft holster to a belt or waist band:

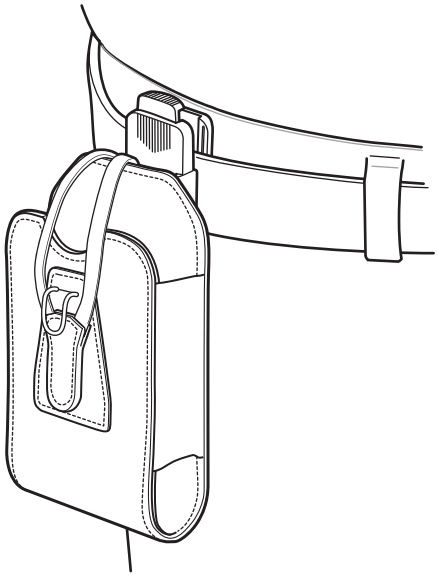
1. Secure the belt clip on the soft holster, if it is not already attached.

Figure 17 Secure Belt Clip on Soft Holster



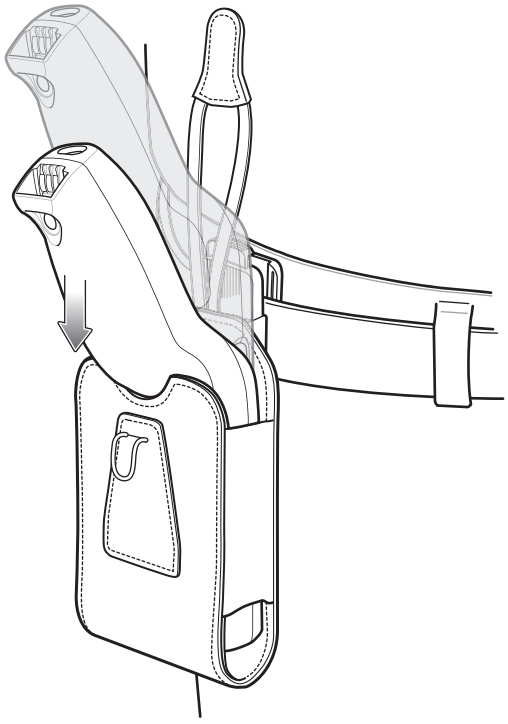
2. Secure the belt clip on the belt or waistband.

Figure 18 Secure Belt Clip on Belt



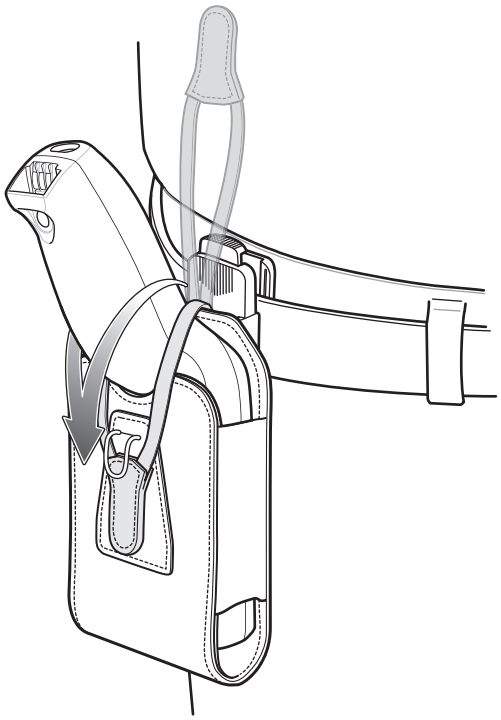
3. To insert the device, slide the device into the soft holster, with the screen facing the user.

Figure 19 Insert Device



4. Secure the device with the restraining strap and place over the device and hook to secure in place.

Figure 20 Secure with Strap



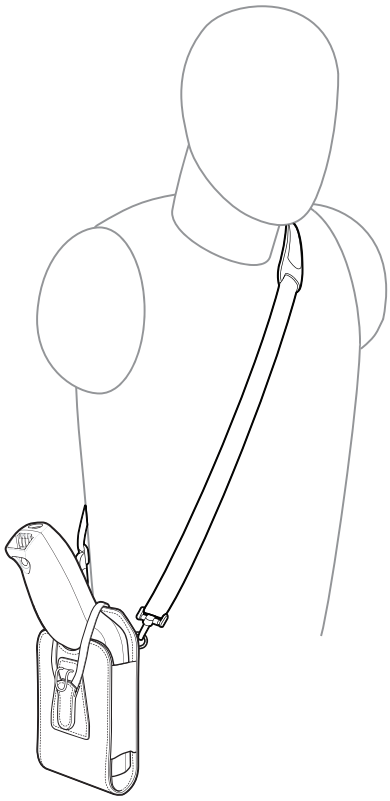
5. To remove the device, lift the restraining strap to release. Lift the device out of the soft holster.

## Using the Shoulder Strap

To attach the soft holster to a shoulder strap:

1. Connect the clips on the shoulder strap to the rings on the soft holster, if not already attached.
2. Place the shoulder strap over your head and rest on your shoulder.

Figure 21 Shoulder Strap



3. Lift the strap and insert the device into the soft holster, with the screen facing the user.
4. Secure the device with the restraining strap and place over the device and hook to secure in place.

# Battery Management

**NOTE:** Prior to checking the battery charge level, remove the device from any AC power source (cradle or cable).

To check the charge status of the main battery, open **Settings** and touch **System > About phone > Battery Information**.

**Battery present status** indicates if the battery is present and **Battery level** lists the battery charge (as a percentage of fully charged). The battery percentage can also be viewed next to the battery icon in the quick access panel. Swipe down with two fingers from the status bar to open the quick access panel.

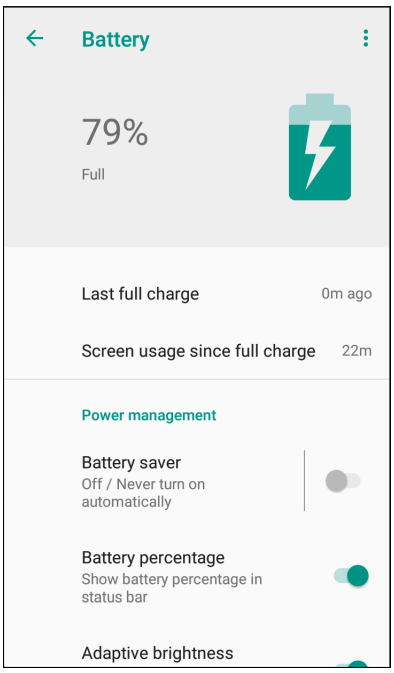
## Monitoring Battery Usage

The **Battery** screen provides battery charge details, power management options, and a list of apps that consume the most battery power.

Use the power management options to extend battery life, or touch an app to display details about its power consumption. Different apps display different information. Some apps include buttons that open screens with settings to adjust power use. Use the **DISABLE** or **FORCE CLOSE** buttons to turn off apps that consume too much power.

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Battery**.

Figure 22 Battery Screen



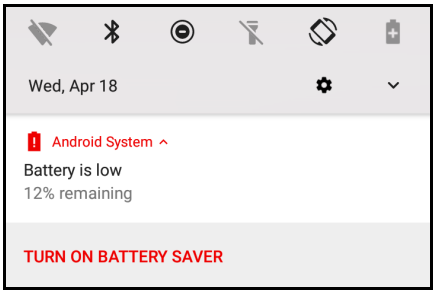

## Low Battery Notification

When the battery charge level drops below 18%, the device displays a notice to connect the device to power. The user should charge the battery using one of the charging accessories.

When the battery charge drops below 10%, the device displays a notice to connect the device to power. The user must charge the battery using one of the charging accessories.

When the battery charge drops below 5%6%, the device turns off. The user must charge the battery using one of the charging accessories.

Figure 23 Low Battery Notification



### Battery Optimization

Observe the following battery saving tips:

- Set the screen to turn off after a short period of non-use.
- Reduce screen brightness.
- Turn off all wireless radios when not in use.
- Turn off automatic syncing for Email, Calendar, Contacts, and other apps.
- Minimize use of apps that keep the device from suspending, for example, music and video apps.

### Turning Off the Radios

To turn off all the radios:

1. Swipe down from the Status bar to open the Quick Settings panel.
2. Touch **Airplane mode**. The airplane icon appears in the Status bar indicating that all the radios are off.

## Setting the Date and Time

You are only required to set the time zone or set the date and time if the wireless LAN does not support Network Time Protocol (NTP).

To set the date and time:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **System** > **Date & time**.
3. Touch **Automatic date & time** to disable automatic date and time synchronization.
4. Touch **Set date**.
5. In the calendar, set today's date.
6. Touch **OK**.
7. Touch **Set time**.
8. Touch the green circle, drag to the current hour and then release.
9. Touch the green circle, drag to the current minute and then release.
10. Touch **AM** or **PM**.
11. Touch **OK**.
12. Touch **Use 24-hour format**.
13. Touch .

## Display Settings

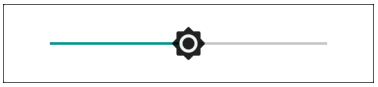
Use Display settings to change the screen brightness, enable night light, change the background image, enable screen rotation, set sleep time, and change font size.

## Setting the Screen Brightness

To manually set the screen brightness using the touchscreen:

1. Swipe down with two fingers from the Status bar to open the Quick Access panel.
2. Slide the icon to adjust the screen brightness level.

Figure 24 Brightness Slider



## Setting Screen Timeout

To set the screen sleep time:

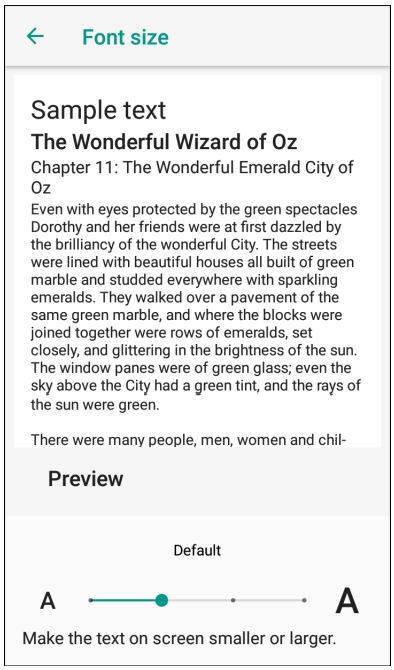
1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Display** > **Advanced** > **Sleep**.
3. Select one of the sleep values.
   - **15 seconds**
   - **30 seconds**
   - **1 minute**
   - **2 minutes**
   - **5 minutes**
   - **10 minutes**
   - **30 minutes**
   - **Never** (default).
4. Touch ◯.

## Setting Font Size

To set the size of the font in system apps:

1. Swipe down from the Status bar to open the Quick Settings panel and then touch ⚙.
2. Touch **Display** > **Advanced**.
3. Touch **Font size**.

Figure 25 Font Settings




4. Select one of the font size values.
   - Small
   - Default
   - Large
   - Largest.
5. Touch ◯.

# Setting Display Size

By default, display size is set to default.

To change the display size:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Display** > **Advanced**.
3. Touch **Display size**.
4. Touch - and + to change the display size.
   - Small
   - Default
   - Large.
5. Touch ◯.

## Setting Screen Saver

To change the screen saver:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Display** > **Advanced**.
3. Touch **Screen saver**.
4. Select the following:
   - **Current screen saver**
     - **PSSScreenSaver** (default)
     - **Clock**
     - **Colors**
     - **Photo Frame**
     - **Photo Table**
     - **Photos**
   - **When to start**
     - **While charging**
     - **While docked**
     - **While charging or docked** (default)
     - **Never**
5. Touch **START NOW** to see the screen saver.
6. Touch ◯.Ambient Display on page 35

**NOTE:** To configure the screen saver settings, push screensaverconfig.xml to /enterprise/device/settings/screensaver. For more information, see Ambient Display on page 35.

## Configuring Screen Saver Settings

To configure screen saver settings:

1. Prepare an xml file with the name **`screensaverconfig.xml`** and with the following fields:
   - ENABLE – set to true to enable the screen saver; set to false to disable the screen saver.
   - EXCEPTION_TIME_START – time in 24-hour format (only hours), after which the screen saver shall be disabled.
   - EXCEPTION_TIME_STOP – time in 24-hour format (only hours), after which the screen shall be enabled again.
   - SCREEN_TIMEOUT_CHARGING – The setting in **Display** > **Advanced** > **Sleep** while on the cradle (idle timeout). The value corresponds to the screen timeout delay in milliseconds, while on the cradle.
   - SCREEN_TIMEOUT_DISCHARGING – The setting in **Display** > **Advanced** > **Sleep** while out of the cradle (idle timeout). The value corresponds to the screen timeout delay in milliseconds, while out of the cradle.

**NOTE:** -1 for screen timeout indicates that the screen will never time out.

2. Push the configured **`screensaverconfig.xml`** file to the folder /enterprise/device/settings/screensaver.
3. If a different screen saver image is preferred rather than the default Zebra logo, create a 24-bit bmp image named **`screensaver.bmp`** and push it to the folder /enterprise/device/settings/screensaver.
4. Reboot the device.

### Example screensaverconfig.xml

```
<?xml version="1.0" encoding="utf-8"?>
<screensaver>
<ENABLE>true</ENABLE>
<EXCEPTION_TIME_START>20</EXCEPTION_TIME_START>
<EXCEPTION_TIME_STOP>6</EXCEPTION_TIME_STOP>
<SCREEN_TIMEOUT_CHARGING>15000</SCREEN_TIMEOUT_CHARGING>
<SCREEN_TIMEOUT_DISCHARGING>30000</SCREEN_TIMEOUT_DISCHARGING>
</screensaver>
```

The above example of the **`screensaverconfig.xml`**:

- Enables the screen saver feature.
- Defines no-screen saver time from 8 pm to 6 am.
- Sets the screen timeout to be 15 seconds on the cradle.
- Sets the screen timeout to be 30 seconds out of the cradle.

## Ambient Display

The Ambient display setting wakes the screen when notifications are received.

To disable ambient display:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Display** > **Advanced**.
3. Touch **Ambient display**.
4. In the **When to show** section, enable or disable an option using the switch.
5. Touch ◯.

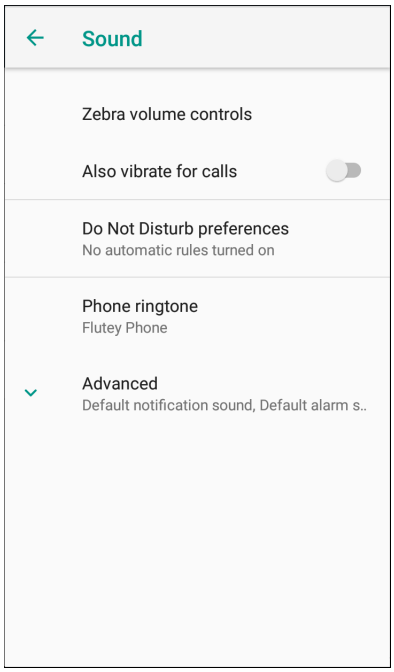
# General Sound Setting

Use the **Sound** settings to configure media and alarm volumes.

To access sound settings:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Sound**.
3. Touch an option to set sounds.

Figure 26 Sound Screen




- **Zebra volume controls**
  - **Ring volume** - Controls the ringtone volume.
  - **Media volume** - Controls the music, games, and media volume.
  - **Alarm volume** - Controls the alarm clock volume.
  - **Notifications volume** - Controls the notification volume.
  - **Scanner volume** - Controls the scanner volume.
  - **Volume presets**
    - - Mutes the ring, notifications, and scanner so that the device does not make sounds or vibrate.
    - - All sounds except media and alarms are silenced and vibrate mode is active.
    - - Enables all sounds at the user defined levels.
- Also vibrate for calls - Switch on or off.
- **Do Not Disturb preferences** - Mutes some or all sounds and vibrations.
  - **Priority only allows** - Use to set the priorities for the following:
    - **Reminders** - Switch on or off.
    - **Events** - Switch on or off.
    - **Alarms** - This is always enabled.
    - **Messages** - Choose to allow messages from anyone, starred contacts, any contact, or none. To star contacts, use the Contacts app.
    - **Calls** - Choose to allow calls from anyone, starred contacts, any contact, or none. To star contacts, use the Contacts app.
    - **Repeat callers** - Choose whether or not the phone rings if the same person calls again within 15 minutes.
  - **Block visual disturbances**
    - **Block when screen is on** - This option prevents notifications from displaying over the screen (peeking) while you are actively using the device.

        - **Block when screen is off** - This option prevents notifications from turning on the screen or pulsing the LED light when a new notification is received while you are not using the device.
    - **Automatic rules** - Choose when to automatically silence the device. Touch a default rule, such as Weekend or Weeknight, or create your own rule. To create your own rule, tap **Add more** and then **Time rule**.
- **Phone ringtone** - Touch to select a sound to play when the phone rings.
- **Advanced** - Touch to display advanced sound options.
    - **Default notification sound** - Touch to select a sound to play for all system notifications.
    - **Default alarm sound** - Touch to select a sound to play for alarms.
    - **Other sounds and vibrations**
        - **Dial pad tones** - Play a sound when pressing keys on dial pad (default - disabled).
        - **Screen locking sounds** - Play a sound when locking and unlocking the screen (default – enabled).
        - **Charging sounds** - Not applicable.
        - **Touch sounds** - Play a sound when making screen selections (default – enabled).
        - **Vibrate on tap** - Vibrate the device when making screen selections (default – disabled).
    - **Emergency alerts** - Touch to configure emergency broadcast settings and notifications.

# Resetting the Device

The reset functions include the following:

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

## Performing a Soft Reset

Perform a soft reset if applications stop working.

1. Press and hold the soft Power button until the menu appears.
2. Touch **Restart**.
   The device reboots.

## Performing a Hard Reset

**CAUTION:** Perform a hard reset only if the device stops responding.

### When in a Cradle

To perform a hard reset when the device is docked inside the cradle:

1. Ensure power is applied to the cradle.
2. Press and hold the Scan key for 10 seconds until the display powers off.

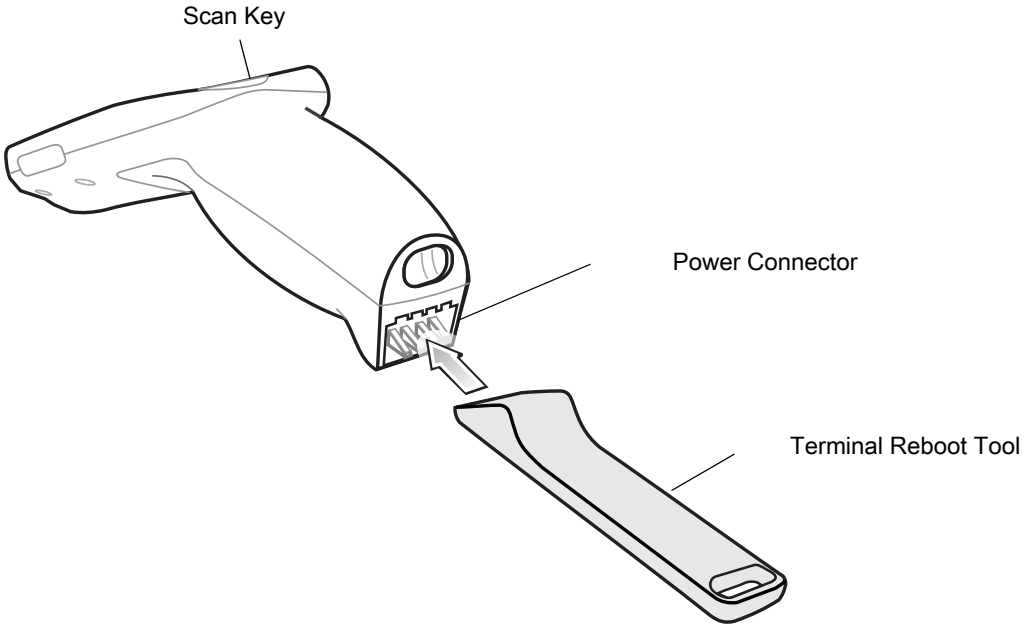
3. Release the Scan key.
4. Briefly press and release the Scan key.
   The device reboots.

### When Out of the Cradle

To perform a hard reset when the device is out of the cradle:

1. Insert the Terminal Reboot Tool into the Power Connector.

Figure 27 Terminal Reboot Tool




2. Press and hold the Scan key for 10 seconds until the display powers off.
3. Release the Scan key.
4. Remove the Terminal Reboot Tool.
5. Briefly press and release the Scan key.
   The device reboots.

# Using the Device

## Introduction

This chapter describes the screens, status and notification icons, and controls on the device, and provides basic instructions for using the device.

## Google Mobile Services

**NOTE:** This section applies to Google Mobile Services (GMS) devices only.

Devices with GMS contain apps and services that provide additional functionality.

GMS includes:

- Apps - GMS adds a variety of Google apps and associated widgets including Chrome, Gmail, Drive, and Maps.
- Services:
  - Speech to Text - Allows for free format speech to text in many languages for both connected and disconnected network. Launch by touching the microphone icon on the keyboard.
  - TalkBack Service - Provides spoken feedback on various parts of the user interface. To enable, go to **Settings** > **Accessibility**.
  - Network Location Provider - Adds a location provider which uses mobile network tower information and Wi-Fi access point information to provide a location without using GPS. To enable, go to **Settings** > **Security & location** > **Location**.
  - Widevine DRM - Enables Digital Rights Management (DRM) so that protected streaming video content can be played. Enable DRM Info from the Google Play ™ store.
  - Google Cloud Messaging - Allows the device to receive data from the server and other devices on the same connection.
  - Backup and Restore - Allows the users settings and apps to be backed up to a Google server and subsequently restored from that server after a factory reset.
- Google Accounts - Create and use a Google account to synchronize mail, files, music, photos, contacts and calendar events.

## Home Screen

Turn on the device to display the Home screen. Depending on the configuration, the Home screen may appear different. Contact your system administrator for more information.

After a suspend or screen time-out, the Home screen displays with the lock slider. Touch the screen and slide up to unlock. For screen locking information, see Un-Locking the Screen.

The Home screen provides additional screens for placement of widgets and shortcuts. Swipe the screen left or right to view the additional screens.

**NOTE:**

By default, non-GMS devices do not have the same icons on the Home screen as GMS. Icons are shown below for example only.

Home screen icons can be configured by the user and may look different than shown.


The Home screen consists of the following:

*Table 10 Home Screen Items*

| Item | Description |
|---|---|
| 1 — Status Bar | Displays the time, status icons (right side), and notification icons (left side). For more information see Notification Icons on page 51 and Managing Notifications on page 51. |
| 2 — Power Icon | Places the PS20 in suspend mode when touched and opens menu when touched and held. |
| 3 — Menu Icon | Displays running applications. |
| 4 — Home Icon | Displays the Home screen. |
| 5 — Back Icon | Displays the previous screen. |
| 6 — Shortcut Icons | Opens applications installed on the PS20. See App Shortcuts and Widgets on page 54 for more information. |

## Status Bar

The Status bar displays the time, notification icons (left side), and status icons (right side).

**NOTE:** Some Status icons may not appear in the Status bar if there are too many icons to display.

Figure 28 Notification and Status Icons


If there are more notifications than can fit in the Status bar, two dots display indicating that more notifications exist. Swipe down from the Status bar to open the Notification panel and view all notifications and status.

## Status Icons

*Table 11 Status Icons*

| Icon | Description |
|---|---|
| | Alarm is active. |
| | Main battery is fully charged. |
| | Main battery is partially drained. |
| | Main battery charge is low. |
| | Main battery charge is very low. |
| | Main battery is charging. |
| | All sounds, except media and alarms, are silenced and vibrate mode is active. |
| | Do Not Disturb mode active. |
| | Airplane Mode is active. All radios are turned off. |
| | Bluetooth is on. |
| | The device is connected to a Bluetooth device. |
| | Connected to a Wi-Fi network. |
| | Not connected to a Wi-Fi network or no Wi-Fi signal. |
| | Connected to an Ethernet network. |
| | Speakerphone enabled. |

## Notification Icons

*Table 12 Notification Icons*

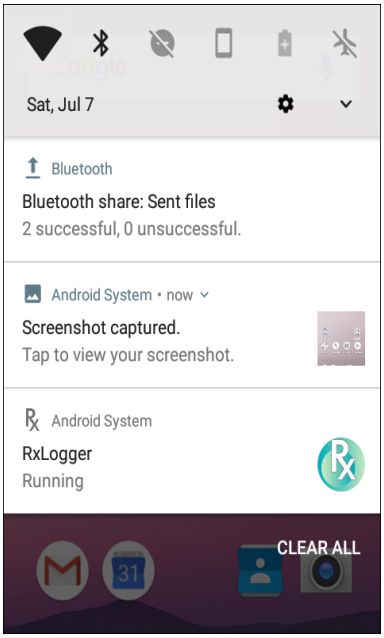
| Icon | Description |
|---|---|
|  | Main battery is low. |
|  | More notifications are available for viewing. |
|  | Data is syncing. |
|  | Indicates an upcoming event. Non-GMS devices only. |
|  | Indicates an upcoming event. GMS devices only. |
|  | Open Wi-Fi network is available. |
|  | Song is playing. |
|  | Problem with sign-in or sync has occurred. |
|  | Device is uploading data. |
|  | Device is downloading data when animated and download is complete when static. |
|  | Device is connected to or disconnected from virtual private network (VPN). |
|  | Preparing internal storage by checking it for errors. |
|  | USB debugging is enabled on the device. |
|  | Indicates that RxLogger app is running. |
|  | Indicates the RS6000 is connected to the device. |
|  | Indicates the RS6000 is connected to the device in HID mode. |

## Managing Notifications

Notification icons report the arrival of new messages, calendar events, alarms, and ongoing events. When a notification occurs, an icon appears in the Status bar with a brief description. See Notification Icons for a list of possible notification icons and their description. Open the Notification panel to view a list of all the notifications.

To open the Notification panel, drag the Status bar down from the top of the screen.

Figure 29 Notification Panel




To respond to a notification, open the Notification panel and then touch a notification. The Notification panel closes and the corresponding app opens.

To clear all notifications, open the Notification panel and then touch **CLEAR ALL**. All event-based notifications are removed. Ongoing notifications remain in the list.

To close the Notification panel, swipe the Notification panel up.

## Setting App Notifications

To set notification settings for a specific app:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Apps & notifications > Notifications > App notifications.**
3. Select an app.
4. Select an available option:
   - **On** / **Off** - Select to turn all notifications from this app **On** (default) or **Off**.
   - **Allow notification dot** - Do not allow this app to add a notification dot to the app icon.
   - **Allow interruptions** - Do not allow notifications from this app to make sound, vibrate, or pop notifications on the screen.
   - **Override Do Not Disturb** - Allow these notifications to interrupt when Do Not Disturb is set to Priority Only.
   - **Categories** - Do not allow specific types of notifications from this app.
   - **Additional settings in the app** - Open the app settings.

**NOTE:** To change the notification settings for an app, slide the notification slightly left or right and touch ⚙.

## Viewing Notification Settings for All Apps

To view the notification settings for all apps:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Apps & Notifications**.
3. Scroll down to **Notifications** to view how many apps have notifications turned off.
4. To set or view notifications settings for a specific app, see Setting App Notifications.

## Controlling Lock Screen Notifications

To control whether notifications can be seen when the device is locked:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Apps & notifications** > **Notifications**.
3. Touch **On the lock screen** and select one of the following:
   - **Show all notification content** (default)
   - **Don't show notifications at all**.

## Blink Light

The Notification LED lights blue when an app, such as email and VoIP, generates a programmable notification or to indicate when the device is connected to a Bluetooth device. By default, LED notifications are enabled.

To change the notification setting:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Apps & notifications > Notifications**.
3. Touch **Blink light** to toggle the notification on or off.

## Quick Access Panel

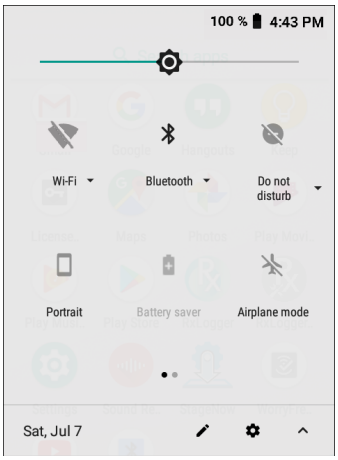
Use the Quick Access panel to access frequently used settings (for example, Airplane mode).

Figure 30 Quick Settings Bar


To see the full Quick Access panel:

- If the device is locked, swipe down once.
- If the device is unlocked, swipe down once with two fingers, or twice with one finger.
- If the Quick Settings bar is open, touch the Down arrow.

Figure 31 Quick Access Panel




**NOTE:** Not all icons are pictured. Icons may vary.

To change a setting, touch the icon:

- Display brightness - Use the slider to decrease or increase the brightness of the screen.
- Wi-Fi network - Turn Wi-Fi on or off. To open Wi-Fi settings, touch the Wi-Fi network name.
- Bluetooth settings - Turn Bluetooth on or off. To open Bluetooth settings, touch **Bluetooth**.
- Battery power - Indicates percentage of battery power remaining. Touch to view battery usage.
- Do not disturb - Control how and when to receive notifications.
- Airplane mode - Turn Airplane mode on or off. When Airplane mode is on the device does not connect to Wi-Fi or Bluetooth.
- Auto-rotate - Lock the device's orientation in portrait or landscape mode or set to automatically rotate.
- Cast - Share phone content on Chromecast or a television with Google Cast built-in. Touch cast screen to display a list of devices, then touch a device to begin casting.
- Screenshot - Takes a snapshot of the current screen.

## App Shortcuts and Widgets

App shortcuts placed on the Home screen allow quick and easy access to apps. Widgets are self-contained apps placed on the Home screen to access frequently used features.

### Adding an App Shortcut to the Home Screen

To add an app shortcut to the Home screen:

1. Go to the desired Home screen.
2. Swipe up from the bottom of the screen.
3. Scroll through the list to find the app icon.
4. Touch and hold the icon until the Home screen appears.
5. Position the icon on the screen and then release.

### Adding a Widget to the Home Screen

To add a widget to the Home screen:

1. Go to the desired Home screen.
2. Touch and hold until the menu appears.
3. Touch **WIDGETS**.
4. Scroll through the list to find the widget.
5. Touch and hold the widget until the Home screen appears.
6. Position the widget on the screen and then release.

### Moving Items on the Home Screen

To move app shortcuts or widgets on the Home screen:

1. Touch and hold the item until it floats on the screen.
2. Drag the item to a new location. Pause at the edge of the screen to drag the item onto an adjacent Home screen.
3. Lift finger to place the item on the Home screen.

### Removing an App Shortcut or Widget from the Home Screen

To remove an app shortcut or widget from the Home screen:

1. Go to the desired Home screen.
2. Touch and hold the app shortcut or widget icon until it floats on the screen.
3. Drag the icon to **X Remove** at the top of the screen and then release.

## Folders

Use **Folders** to organize similar applications together. Tap the folder to open and display items in the folder.

### Creating a Folder

There must be at least two app icons on the Home screen.

To create a folder:

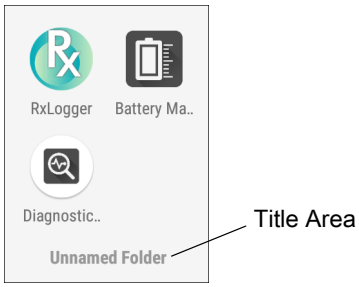
1. Go to the desired Home screen.
2. Touch and hold one app icon.
3. Drag the icon and stack on top of another icon.
4. Lift and release.

### Naming Folders

To name a folder:

1. Touch the folder.

Figure 32 Open Folder




2. Touch the title area and enter a folder name using the keyboard.
3. Touch on the keyboard.
4. Touch anywhere on the Home screen to close the folder. The folder name appears under the folder.

### Removing a Folder

To remove a folder:

1. Touch and hold the folder icon until it enlarges.
2. Drag the folder to **X Remove** and release.

## Home Screen Wallpaper

To change the Home screen wallpaper:

1. Touch and hold the screen until the menu appears.
2. Touch **WALLPAPERS**.
3. Touch **Photos** or **Gallery** to select a photo or select one of the pre-installed wallpapers.
4. Touch **Set wallpaper**.

# Using the Touchscreen

Use the multi-tap sensitive screen to operate the device.

- Tap - Tap to:
  - Select items on the screen.
  - Type letters and symbols using the on-screen keyboard.
  - Press on-screen buttons.
- Tap and Hold - Tap and hold:
  - An item on the Home screen to move it to a new location or to the trash.
  - An item in Apps to create a shortcut on the Home screen.
  - The Home screen to open a menu for customizing the Home screen.
  - An empty area on the Home screen until the menu appears.
- Drag - Tap and hold an item for a moment and then move finger on the screen until reaching the new position.

- Swipe - Move finger up and down or left and right on the screen to:
  - Unlock the screen.
  - View additional Home screens.
  - View additional app icons in the Launcher window.
  - View more information on an app's screen.
- Double-tap - Tap twice on a web page, map, or other screen to zoom in and out.
- Pinch - In some apps, zoom in and out by placing two fingers on the screen and pinching them together (to zoom out) or spreading them apart (to zoom in).

# Using the Android and Gboard Keyboards

Use the Android or Gboard keyboards to enter text in a text field. To configure the keyboard settings, touch and hold **,** (comma) and then select **Android keyboard settings**.

## Editing Text

Edit entered text and use menu commands to cut, copy, and paste text within or across apps. Some apps do not support editing some or all of the text they display; others may offer their own way to select text.

## Entering Numbers, Symbols, and Special Characters

To enter numbers and symbols:

- Touch and hold one of the top-row keys until a menu appears then select a number or special character.
- Touch the Shift key once for a single capital letter. Touch the Shift key twice to lock in uppercase. Touch the Shift key a third time to unlock Capslock.
- Touch **?123** to switch to the numbers and symbols keyboard.
- Touch the **=\<** key on the numbers and symbols keyboard to view additional symbols.

To enter special characters, touch and hold a number or symbol key to open a menu of additional symbols. A larger version of the key displays briefly over the keyboard.

# Apps

The **APPS** screen displays icons for all installed apps. The table below lists the apps installed on the device. Refer to the device Integrator Guide for Android Version 8.1 for information on installing and uninstalling apps.

*Table 13 Apps*

| Icon | Description |
|---|---|
|  | **Battery Manager** - Displays battery information, including charge level, status, health and wear level. |
|  | **Bluetooth Pairing Utility** – Use to pair peripherals with the device by scanning a barcode. |
|  | **Calculator** - Provides the basic and scientific arithmetic functions. |

*Table 13 Apps (Continued)*

| Icon | Description |
|---|---|
|  | **Calendar** - Use to manage events and appointments. GMS/GMS-Restricted only. |
|  | **Calendar** - Use to manage events and appointments. AOSP only. |
|  | **Camera** - Take photos or record videos. For more information see Camera. Available on Plus configurations. |
|  | **Chrome** - Use to access the Internet or intranet. GMS/GMS-Restricted only |
|  | **Chromium** - Use to access the Internet or intranet. AOSP only. |
|  | **Clock** - Use to schedule alarms for appointments or as a wake-up. |
|  | **Contacts** - Use to manage contact information. See Contacts for more information. |
|  | **Cradle Firmware Updater** - Use to update cradle firmware. |
|  | **Cradle Utility** - Use to control cradle functionality. |
|  | **DataWedge** - Enables data capture using the imager. |
|  | **Device Central** - Use to display detailed information about the device and connected peripherals. See Device Central for more information. |
|  | **Diagnostic Tool** - Use to diagnose the device. |
|  | **Drive** - Upload photos, videos, documents, and other files to personal storage site. GMS/GMS-Restricted only. |
|  | **DWDemo** - Provides a way to demonstrate the data capture features using the imager. See DataWedge Demonstration for more information. |

*Table 13 Apps (Continued)*

| Icon | Description |
|---|---|
|  | **Email** - Use to send and receive email. AOSP only. |
|  | **Enterprise Browser** - Industrial browser that provides everything needed to quickly build device apps for barcode scanning, signature capture, payment processing, printing and most other enterprise applications. For more information, refer to techdocs.zebra.com/enterprise-browser/. |
|  | **Files** - Organize and manage files on the device. See Files for more information. |
|  | **Gallery** - Use to view photos stored on the internal storage. For more information, see Gallery for more information. AOSP only. |
|  | **Gmail** - Use to send and receive email using a Google email account. GMS/GMS-Restricted only |
|  | **Google** - Launches Google ™ search app. GMS/GMS-Restricted only |
|  | **Hangouts** - Use to communicate with friends using text messages and photos. GMS/GMS-Restricted only |
|  | **Keep**- Use to create, edit, and share notes. GMS/GMS-Restricted only. |
|  | **License Manager** - Use to manage software licenses on the device. |
|  | **Maps** - Use to see your location on a map (with public transit, traffic, or satellite overlays). Search for any business or place of interest. Provides turn-by-turn navigation with voice guidance, traffic-avoidance, and alternate routes, for drivers, cyclists, walkers, and users of public transportation. GMS/GMS-Restricted only. |
|  | **Music** - Play music stored on the internal storage. AOSP only. |
|  | **Photos** - Use to sync photos with Google account. For more information, see Photo Settings. GMS/GMS-Restricted only. |
|  | **Play Movies & TV** - View movies and video on your device. GMS/GMS-Restricted only. |
|  | **Play Music** - Use to listen to music. GMS/GMS-Restricted only. |

*Table 13 Apps (Continued)*

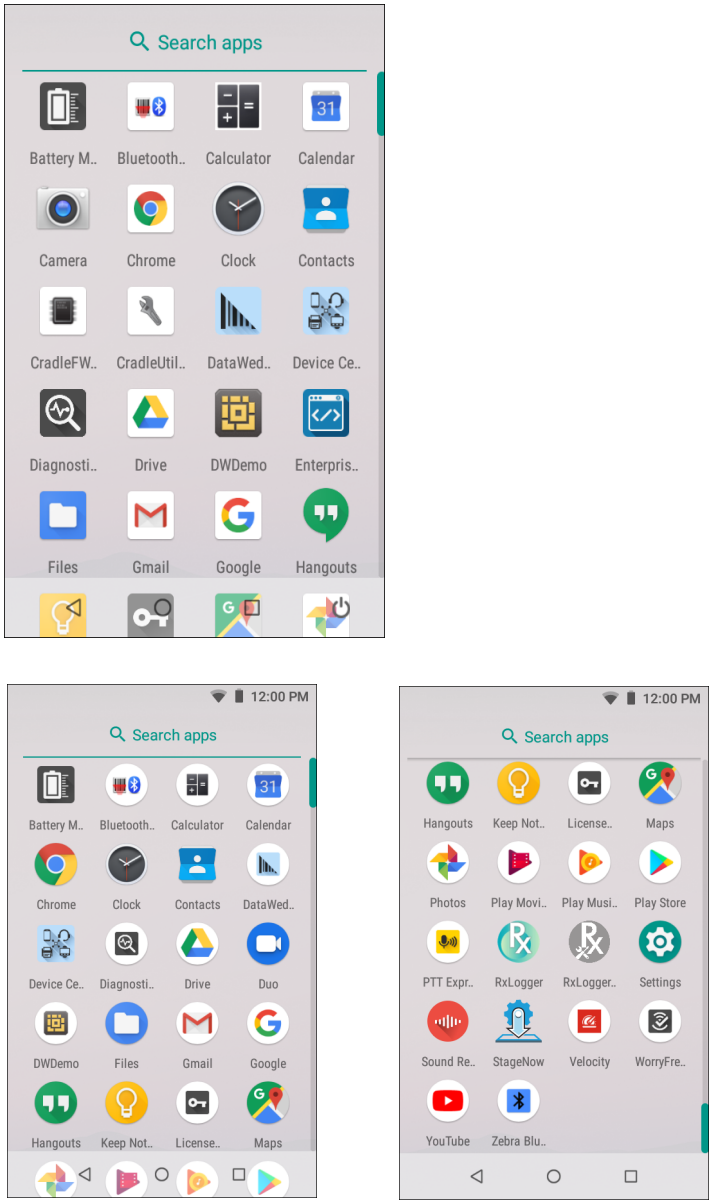
| Icon | Description |
|---|---|
|  | **Play Store** - Download music, movies, books, and Android apps and games from the Google Play Store. GMS/GMS-Restricted only. |
|  | **RxLogger** - Use to diagnose device and app issues. See the device Integrator Guide for Android Version 8.1 for more information. |
|  | **RxLogger Utility** - Use to view, backup, and archive RxLogger data. |
|  | **Search** - Use to search the Web. Requires an Internet connection. AOSP only. |
|  | **Settings** - Use to configure the device. |
|  | **Sound Recorder** - Use to record audio. Available on Plus configurations. |
|  | **StageNow** - Allows the device to stage a device for initial use by initiating the deployment of settings, firmware, and software. |
|  | **Worry Free Wifi Analyzer** - A diagnostic intelligent app. Use to diagnose surrounding area and display network stats, such as coverage hole detection, or AP in vicinity. Refer to the Worry Free Wi-Fi Analyzer Administrator Guide for Android. |
|  | **YouTube** - Use to view videos on the YouTube ™ web site. GMS/GMS-Restricted only. |
|  | **Zebra Bluetooth** - Use to configure Bluetooth logging. |

# Accessing Apps

All apps installed on the device are accessed using the **APPS** window.

1. On the Home screen, swipe up from the bottom of the screen.

Figure 33 APPS Window Example



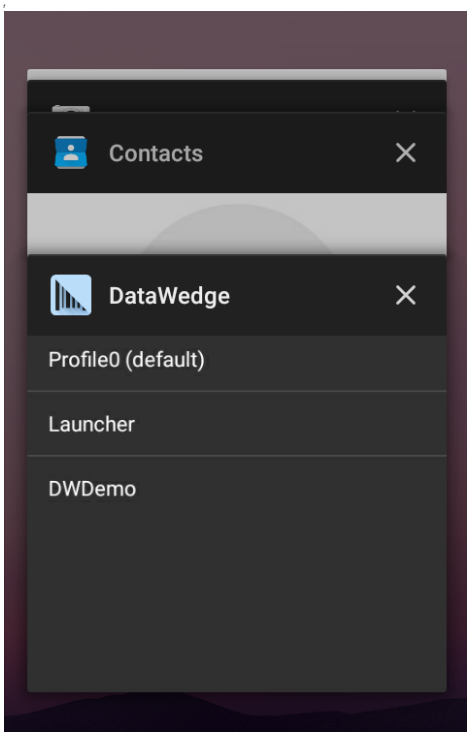

Slide the **APPS** window up or down to view more app icons. Touch an icon to open the app.

## Switching Between Recent Apps

To switch between recent apps:

1. Touch ▢. A window appears on the screen with icons of recently used apps.

Figure 34 Recently Used Apps




2. Slide the apps displayed up and down to view all recently used apps.
3. Swipe left or right to remove app from the list and force close the app.
4. Touch an icon to open an app or touch ◁ to return to the current screen.

# Un-Locking the Screen

Use the Lock screen to protect access to data on the device. Some email accounts require locking the screen. Refer to the device Integrator Guide for information on setting up the locking feature.

When locked, a 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. Swipe 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.

Figure 35 Lock Screen

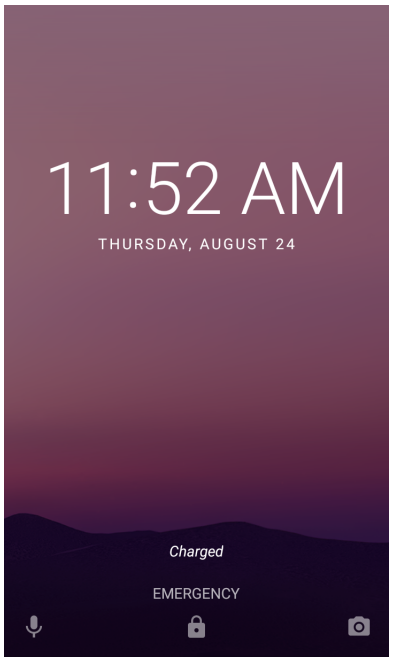



Figure 36 PIN Screen

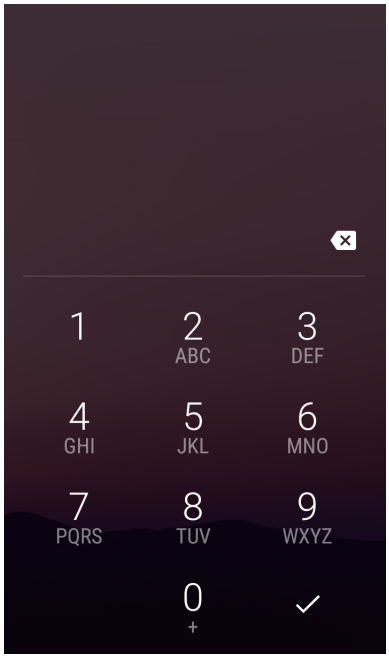


Figure 37 Pattern Screen

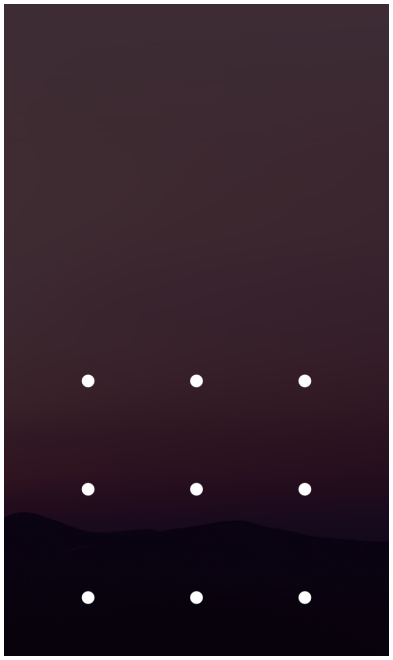
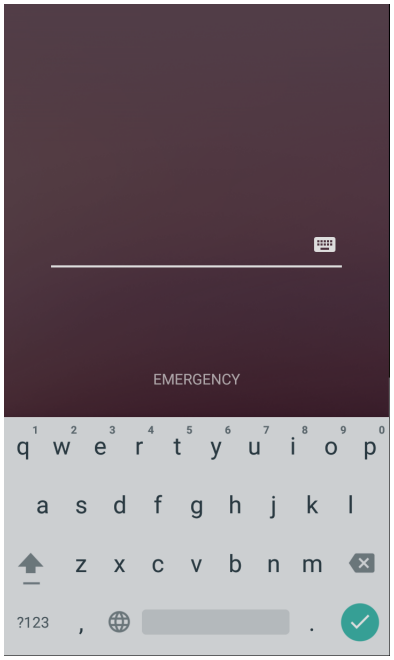


Figure 38 Password Screen




## Suspend Mode

The device goes into suspend mode when you press the Scan button or after a period of inactivity (if the **Never** setting is changed to something else in **Settings** > **Display** > **Advanced** > **Sleep**).

To wake the device from Suspend mode, press the Scan button. The Lock screen displays. Swipe 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. See Un-Locking the Screen.

**NOTE:** If you enter the PIN, password, or pattern incorrectly five times, you must wait 30 seconds before trying again. If you forget the PIN, password, or pattern contact your system administrator.

# Wireless

## Introduction

This section provides information on the wireless features:

- Wireless Local Area Network (WLAN)
- Bluetooth
- Cast.

## Wireless Local Area Networks

Wireless local area networks (WLANs) allow the device to communicate wirelessly inside a building. Before using the device on a WLAN, the facility must be set up with the required hardware to run the WLAN (sometimes known as infrastructure). The infrastructure and the device must both be properly configured to enable this communication.

Refer to the documentation provided with the infrastructure (access points (APs), access ports, switches, Radius servers, etc.) for instructions on how to set up the infrastructure.

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **Wireless & networks** settings configure the device to match the security scheme.

The device supports the following WLAN security options:

- Open
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)/WPA2 Personal (PSK)
- Extensible Authentication Protocol (EAP).
  - LEAP
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication
  - Transport Layer Security (TLS)
  - TTLS - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.
  - PWD

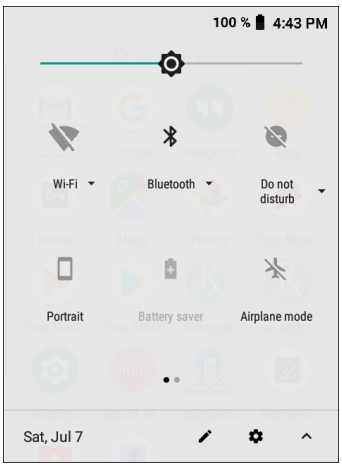
The **Status** bar displays icons that indicate Wi-Fi network availability and Wi-Fi status.

**NOTE:** To extend the life of the battery, turn off Wi-Fi when not in use.

# Connecting to a Wi-Fi Network

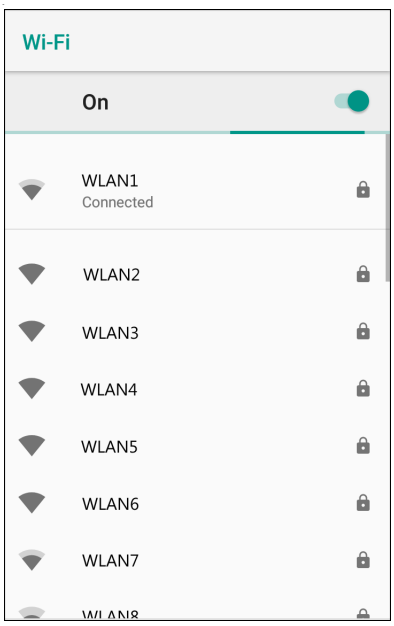
To connect to a Wi-Fi network:

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




2. Touch **Wi-Fi** to open the **Wi-Fi** screen. The device searches for WLANs in the area and lists them.

Figure 39 Wi-Fi Screen




3. Scroll through the list and select the desired WLAN network.
4. For open networks, touch profile once or press and hold and then select **Connect to network** or for secure networks enter the required password or other credentials then touch **Connect**. See the system administrator for more information.

   The device obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the device with a fixed internet protocol (IP) address, Refer to the device Integrator Guide for more information.
5. In the Wi-Fi setting field, **Connected** appears indicating that the device is connected to the WLAN.

## 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 40 WLAN WEP Network Security Dialog Box

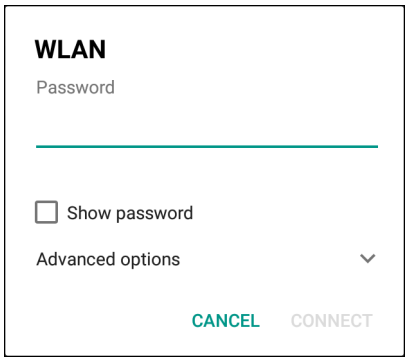
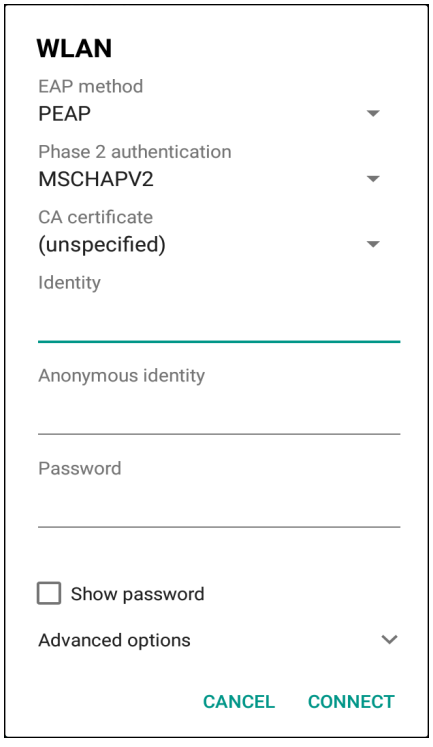



Figure 41 WLAN 802.11 EAP Network Security Dialog Box



7. If the network security is **WEP** or **WPA/WPS2 PSK**, enter the required password and then touch **Connect**.
8. If the network security is 802.1x EAP:
   - Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **TTLS, 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 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 to 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**, **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

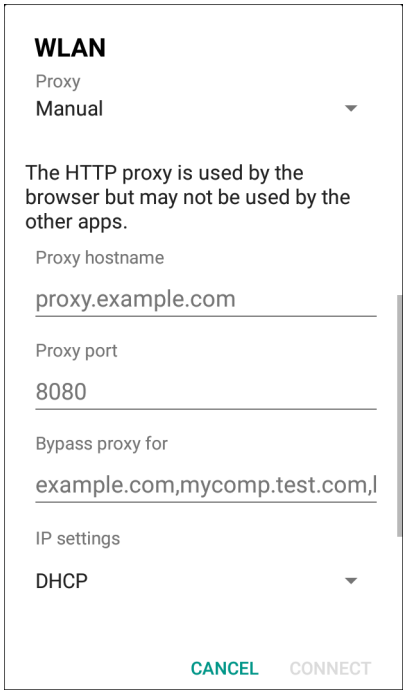
A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server and requests some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates 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 42 Proxy Settings




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 ◯.

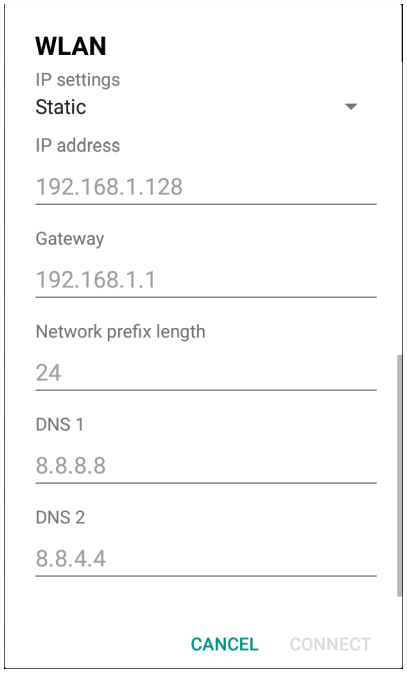
## Configuring the Device to Use a Static IP Address

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 43 Static IP Settings




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 ◯.

# Advanced Wi-Fi Settings

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

Use the **Advanced** settings to configure additional Wi-Fi settings. To view the advanced settings, scroll to the bottom of the **Wi-Fi** screen and select **Wi-Fi preferences > Advanced**.

- **Install Certificates** – Touch to install certificates.
- **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.

## 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.

## Removing a Wi-Fi Network

To remove a remembered or connected network:

1. Swipe down from the status bar to open the quick access panel and then touch ⚙.
2. Touch **Network & Internet > W-Fi**.
3. Scroll down to the bottom of the list and touch **Saved networks**.
4. Touch the name of the network.
5. In the dialog box, touch **FORGET**.
6. Touch ◯.

## Wi-Fi Advanced Features

Some additional Wi-Fi settings cannot be accessed from the User Interface. They can be configured by using Wi-Fi (CSP). Refer to EMDK documentation for the details on the Wi-Fi settings configuration using the Wi-Fi CSP.

- **Auto Time Config** - Using this feature, the device can sync up its time with Zebra WLAN infrastructure. This feature works only when the device is connected to Zebra WLAN infrastructure and the feature is enabled on the WLAN infrastructure side. Default: disabled.

- **PMKID Caching** - Allows the device to skip 802.1x authentication during roaming if it had previously connected to that AP with a full 802.1x authentication. Default: disabled. Note: disable OKC when enabling PMKID Caching.
- **Opportunistic Key Caching** - Use this feature to skip 802.1x authentication during roaming. The device will go for full 802.1x authentication for the first time it connects to the network. For subsequent roaming, the device skips 802.1x authentication. Default: enabled.
- **Cisco Centralized Key Management** - Allows the device to skip 802.1x and key-handshake phases during roaming. This feature is available only when the device is connected to a Cisco infrastructure that supports Cisco Centralized Key Management (CCKM). Default: enabled.
- **Fast Transition** - Fast Transition (FT) is the fast roaming standard, 802.11r. With this feature, the device can skip 802.1x and key-handshake phases during roam. Default: enabled.
- **Fast Transition Resource Information Container** - Allows the device to request TSPEC as part of reassociation frame exchange. This helps to avoid sending a separate resource request after roaming is completed. Default: enbled.
- **Power Save** - The device can be configured to work in different power save modes:
    i. **Active** - Keeps the WLAN radio always in active mode (i.e. power save mode disabled).
    ii. **Power save using WMM-PS** - This is the default power save mode. Device uses WMM-PS power save method if the AP is configured to use this. If the AP is not supporting WMM-PS, the device will use PS-Poll power save method.
    iii. **Power save using PS-Poll** - In this method, the device will use PS-Poll frames to retrieve buffered frames from the AP.
    iv. **Null Data Power Save** - In Null Data Power Save (NDP), the device will stay awake for 100 ms after the last frame is sent or received. The device will send a Null Data packet with power management bit cleared to retrieve buffered frames from the AP.
- **802.11k** - Using 802.11k, the device can discover neighbor APs and adds support for different types of radio resource measurements. Default: enabled.
- **Band Preference** - The device can be configured to prefer one band over another. Default: disabled.**Subnet Roaming** - When the device roams between different sub networks, if it detects that it is roaming to a different subnet, the device will request a fresh IP address. Default: disabled.

# Bluetooth

Bluetooth devices can communicate without wires, using frequency-hopping spread spectrum (FHSS) radio frequency (RF) to transmit and receive data in the 2.4 GHz Industry Scientific and Medical (ISM) band (802.15.1). Bluetooth wireless technology is specifically designed for short-range (10 m (32.8 ft)) communication and low power consumption.

Devices with Bluetooth capabilities can exchange information (for example, files, appointments, and tasks) with other Bluetooth enabled devices such as printers, access points, and other mobile devices.

The device supports Bluetooth Low Energy. Bluetooth Low Energy is targeted at applications in the healthcare, fitness, security, and home entertainment industries. It provides reduced power consumption and cost while maintaining standard Bluetooth range.

## Adaptive Frequency Hopping

Adaptive Frequency Hopping (AFH) is a method of avoiding fixed frequency interferers, and can be used with Bluetooth voice. All devices in the piconet (Bluetooth network) must be AFH-capable in order for AFH to work. There is no AFH when connecting and discovering devices. Avoid making Bluetooth connections and discoveries during critical 802.11b communications. AFH for Bluetooth consists of four main sections:

- Channel Classification - A method of detecting an interference on a channel-by-channel basis, or pre-defined channel mask.
- Link Management - Coordinates and distributes the AFH information to the rest of the Bluetooth network.
- Hop Sequence Modification - Avoids interference by selectively reducing the number of hopping channels.
- Channel Maintenance - A method for periodically re-evaluating the channels.

When AFH is enabled, the Bluetooth radio “hops around” (instead of through) the 802.11b high-rate channels. AFH coexistence allows enterprise devices to operate in any infrastructure.

The Bluetooth radio in this device operates as a Class 2 device power class. The maximum output power is 2.5 mW and the expected range is 10 m (32.8 ft). A definition of ranges based on power class is difficult to obtain due to power and device differences, and whether in open space or closed office space.

**NOTE:** It is not recommended to perform Bluetooth wireless technology inquiry when high rate 802.11b operation is required.

## Security

The current Bluetooth specification defines security at the link level. Application-level security is not specified. This allows application developers to define security mechanisms tailored to their specific need. Link-level security occurs between devices, not users, while application-level security can be implemented on a per-user basis. The Bluetooth specification defines security algorithms and procedures required to authenticate devices, and if needed, encrypt the data flowing on the link between the devices. Device authentication is a mandatory feature of Bluetooth while link encryption is optional.

Pairing of Bluetooth devices is accomplished by creating an initialization key used to authenticate the devices and create a link key for them. Entering a common personal identification number (PIN) in the devices being paired generates the initialization key. The PIN is never sent over the air. By default, the Bluetooth stack responds with no key when a key is requested (it is up to user to respond to the key request event). Authentication of Bluetooth devices is based-upon a challenge-response transaction. Bluetooth allows for a PIN or passkey used to create other 128-bit keys used for security and encryption. The encryption key is derived from the link key used to authenticate the pairing devices. Also worthy of note is the limited range and fast frequency hopping of the Bluetooth radios that makes long-distance eavesdropping difficult.

Recommendations are:

- Perform pairing in a secure environment
- Keep PIN codes private and do not store the PIN codes in the device
- Implement application-level security.

## Bluetooth Profiles

The device supports the Bluetooth services listed in the table below:

*Table 14 Bluetooth Profiles*

| Profile | Description |
|---|---|
| Service Discovery Protocol (SDP) | Handles the search for known and specific services as well as general services. |
| Serial Port Profile (SPP) | Allows use of RFCOMM protocol to emulate serial cable connection between two Bluetooth peer devices. For example, connecting the device to a printer. |
| Object Push Profile (OPP) | Allows the device to push and pull objects to and from a push server. |
| Human Interface Device Profile (HID) | Allows Bluetooth keyboards, pointing devices, gaming devices and remote monitoring devices to connect to the device. |
| Out of Band (OOB) | Allows exchange of information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. Using OOB with NFC enables pairing when devices simply get close, rather than requiring a lengthy discovery process. |
| Generic Attribute Profile (GATT) | Provides profile discovery and description services for Bluetooth Low Energy protocol. It defines how attributes are grouped together into sets to form services. |
| Generic Access Profile (GAP) | Use for device discovery and authentication. |
| OBject EXchange (OBEX) | Facilitates the exchange of binary objects between devices. |

## Bluetooth Power States

The Bluetooth radio is off by default:

- Suspend - When the device goes into suspend mode, the Bluetooth radio stays on.
- Airplane Mode - When the device is placed in Airplane Mode, the Bluetooth radio turns off. When Airplane mode is disabled, the Bluetooth radio returns to the prior state. When in Airplane Mode, the Bluetooth radio can be turned back on if desired.

## Bluetooth Radio Power

Turn off the Bluetooth radio to save power or if entering an area with radio restrictions (for example, an airplane). When the radio is off, other Bluetooth devices cannot see or connect to the device. Turn on the Bluetooth radio to exchange information with other Bluetooth devices (within range). Communicate only with Bluetooth radios in close proximity.

**NOTE:** To achieve the best battery life, turn off radios when not in use.

### Enabling Bluetooth

To enable Bluetooth:

1. Swipe down from the Status bar to open the Quick Access panel.
2. Touch ✱ to turn Bluetooth on.
3. Touch ◯.

### Disabling Bluetooth

To disable Bluetooth:

1. Swipe down from the Status bar to open the Quick Access panel.
2. Touch ✱ to turn Bluetooth off.
3. Touch ◯.

## Discovering Bluetooth Device(s)

The device can receive information from discovered devices without pairing. However, once paired, the device and a paired device exchange information automatically when the Bluetooth radio is on. To find Bluetooth devices in the area:

1. Ensure that Bluetooth is enabled on both devices.
2. Ensure that the Bluetooth device to discover is in discoverable mode.
3. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
4. Swipe down from the Status bar to open the Quick Access panel.
5. Touch **Bluetooth**.
6. Touch **MORE SETTINGS**. The **Bluetooth** screen appears.
7. Touch **Pair new device**. The device begins searching for discoverable Bluetooth devices in the area and displays them under **Available devices**.
8. Scroll through the list and select a device. The Bluetooth pairing request dialog box appears.
9. Touch **Pair** on both devices.
10. The Bluetooth device is added to the **Paired devices** list and a trusted (“paired”) connection is established.

## Changing the Bluetooth Name

By default, the device has a generic Bluetooth name that is visible to other devices when connected.

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Connected devices > Bluetooth**.
3. If Bluetooth is not on, move the switch to turn Bluetooth on.
4. Touch **Device name**.
5. Enter a name and touch **RENAME**.
6. Touch ◯.

## Connecting to a Bluetooth Device

Once paired, connect to a Bluetooth device.

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

2. Touch **Connected device** > **Bluetooth**.
3. In the list, touch the unconnected Bluetooth device.
   When connected, **Connected** appears below the device name.

### Selecting Profiles on the Bluetooth Device

Some Bluetooth devices have multiple profiles. To select a profile:

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Connected Devices** > **Bluetooth**.
3. In the **Paired Devices** list, touch ⚙ next to the device name.
4. Turn on or off a profile to allow the device to use that profile.
5. Touch ◯.

### Unpairing a Bluetooth Device

To unpair a Bluetooth device and erase all pairing information:

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Connected devices** > **Bluetooth**.
3. In the **Paired Devices** list, touch ⚙ next to the device name.
4. Touch **FORGET**.
5. Touch ◯.

## Cast

Use **Cast** to mirror the device screen on a Miracast enabled wireless display.

1. Swipe down from the Status bar to open the Quick Settings bar and then touch ⚙.
2. Touch **Connected Devices**.
3. Touch **Cast**.
4. Touch ⋮ > **Enable wireless display**. The device searches for nearby Miracast devices and lists them.
5. Touch a device to begin casting.
6. Touch ◯.

# Applications

## Introduction

This chapter describes the apps installed on the device.

## Battery Manager

The **Battery Manager** provides detailed information about the battery.

To open Battery Manager, swipe up from the bottom of the Home screen and touch .

Figure 44 Battery Manager Screen

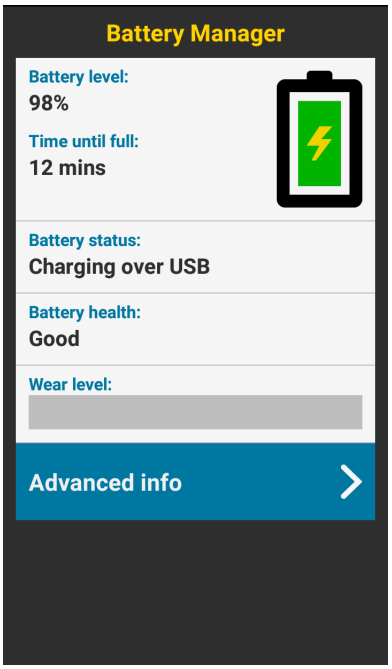


*Table 15 Battery Icon Description*

| Battery Icon | Description |
|---|---|
|  | Battery charge level. |
|  | Battery charging. |
|  | Battery charge level is below 20%. |

- **Battery level** - The current battery charge level as a percentage. Displays **-%** when level is unknown.
- **Time until full** - The amount of time until the battery is fully charged.
- **Time since charging** - The amount of time since the device began charging.
- **Time until empty** - The amount of time until the battery is empty.
- **Battery status**
  - **Not charging** - The device is not connected to AC power.
  - **Charging over AC** - The device is connected to AC power and charging.
  - **Charging over USB** - The device is connected to a host computer with a USB cable and charging.
  - **Discharging** - That the battery is discharging.
  - **Full** - That the battery is fully charged.
  - **Unknown** - The battery status is unknown.
- **Battery health** - The health of the battery. If a critical error occurs,  appears. Touch to view the error description.
  - **Decommission** - The battery is past its useful life and should be replaced. See system administrator.
  - **Good** - The battery is good.
  - **Charge error** - An error occurred while charging. See system administrator.
  - **Over Current** - An over-current condition occurred. See system administrator.
  - **Dead** - The battery has no charge. Replace the battery.
  - **Over Voltage** - An over-voltage condition occurred. See system administrator.
  - **Below Temperature** - The battery temperature is below the operating temperature. See system administrator.
  - **Failure Detected** - A failure has been detected in the battery. See system administrator.
  - **Unknown** - See system administrator.
- **Wear level** - The health of the battery in graphical form. When the wear level exceeds 80%, the bar color changes to red.

- **Advanced info** - Touch to view additional battery information.
  - **Battery present status** - Indicates that the battery is present.
  - **Battery level** - The battery charge level as a percentage of scale.
  - **Battery scale** - The battery scale level used to determine battery level (100).
  - **Battery voltage** - The current battery voltage in millivolts.
  - **Battery temperature** - The current battery temperature in degrees Centigrade.
  - **Battery technology** - The type of battery.
  - **Battery current** - The average current into or out of the battery over the last second in mAh.
  - **Battery manufacture date** - The date of manufacture.
  - **Battery serial number** - The battery serial number. The number matches the serial number printed on the battery label.
  - **Battery part number** - The battery part number.
  - **Battery rated capacity** - Lists the rated capacity of the backup battery in mAh.
  - **Battery decommission status** - Indicates if the battery is past its life span.
    - **Battery Good** - The battery is in good health.
    - **Decommissioned Battery** - The battery is past its useful life and should be replaced.
  - **Base cumulative charge** - Cumulative charge using Zebra charging equipment only.
  - **App version** - The application version number.

# Camera

**NOTE:** This app is available on the Plus configuration.

This section provides information for taking photos and recording videos using the integrated digital cameras.

The device saves photos and videos on the internal storage.

## Taking Photos

**NOTE:** See Photo Settings for camera setting descriptions.

1. Swipe up from the bottom of the Home screen and touch **Camera**.

Figure 45 Camera Mode


2. If necessary, touch the Camera Mode icon and touch .
3. Frame the subject on the screen.

4. To zoom in or out, press two fingers on the display and pinch or expand fingers. The zoom controls appear on the screen.
5. Touch an area on the screen to focus. The focus circle appears. The two bars turn green when in focus.
6. Touch ⊙.

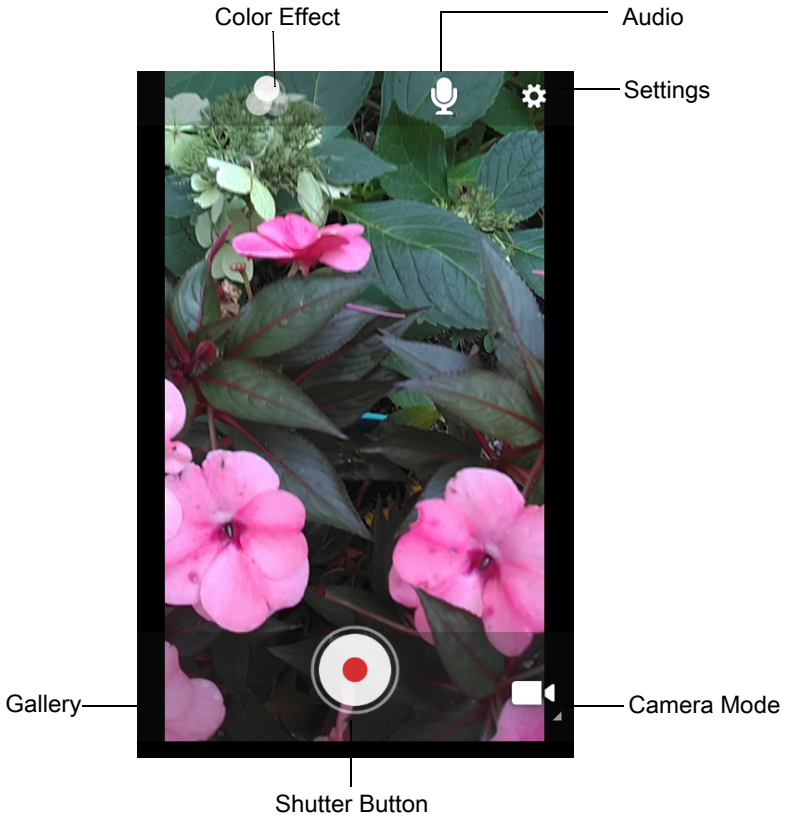
   The camera takes a photo and a shutter sound plays.

   The photo momentarily displays as a thumbnail in the lower left corner.

## Recording Videos

1. Swipe up from the bottom of the Home screen and touch **Camera**.
2. Touch the camera mode menu and touch ■◀.

Figure 46 Video Mode




3. Point the camera and frame the scene.
4. To zoom in or out, press two fingers on the display and pinch or expand fingers. The zoom controls appear on the screen.

5. Touch ⊙ to start recording.
   The video time remaining appears in the top left of the screen.
6. Touch ⊙ to the end recording.
   The video momentarily displays as a thumbnail in the lower left corner.

## Photo Settings

In Photo mode, photo settings appear on screen. Touch ⚙ to display the photo settings options.

### Front Camera

- **Selfie Flash** - Turns screen white to help produce a little extra light in dimmer settings. Options: **Off** (default), or **On**.
- **Picture size** - Set the size (in pixels) of the photo to: **1.3M pixels** (default), **HD720**, **1M pixels**, **WVGA**, **VGA,** or **QVGA**.
- **Picture quality** - Set picture quality setting to: **Low**, **Standard** (default) or **High**.
- **Countdown timer** - Set to: **Off** (default), **2 seconds**, **5 seconds** or **10 seconds**.
- **Storage** – Set location to store the photo to: **Phone**.
- **Face Detection** - Select to turn face detection **Off** (default) or **On**.
- **ISO** - Set how sensitive the camera is to light. Options: **Auto** (default), **ISO Auto (HJR)**, **ISO100**, **ISO200**, **ISO400**, **ISO800** or **ISO1600**.
- **Exposure** - Touch to adjust the exposure settings. Options: **+2**, **+1**, **0** (default), **-1** or **-2**.
- **White balance** - Select how the camera adjusts colors in different kinds of light, to achieve the most natural-looking colors:
  - **Incandescent** - Adjust the white balance for incandescent lighting.
  - **Fluorescent** - Adjust the white balance for florescent lighting.
  - **Auto** - Adjust the white balance automatically (default).
  - **Daylight** - Adjust the white balance for daylight.
  - **Cloudy** - Adjust the white balance for a cloudy environment.
- **Redeye reduction** - Helps eliminate redeye effect. Options: **Disabled** (default), or **Enable**.
- **ZSL** - Set the camera to immediately take a picture when the button is pressed (default – enabled)
- **Selfie Mirror** - Options: **Disable** (default), or **Enable**.
- **Anti Banding** - Allows the camera to avoid problems caused by artificial light sources that are not constant. These sources cycle (flicker) fast enough to go unnoticed to the human eye, appearing continuous. The camera's eye (its sensor) can still see this flicker. Options: **Auto** (default), **60 Hz**, **50 Hz**, or **Off**.

# Video Settings

In Video mode, video settings appear on screen. Touch ⚙ to display the video settings options.

## Front Camera

- **Video quality** - Set video quality to: **HD 720p** (default), or **SD 480p**.
- **Video duration** - Set to: **30 seconds (MMS)** or **30 minutes** (default).
- **Storage** – Set the location to store the photo to: **Phone**.
- **White balance** - Select how the camera adjusts colors in different kinds of light, to achieve the most natural-looking colors.
  - **Incandescent** - Adjust the white balance for incandescent lighting.
  - **Fluorescent** - Adjust the white balance for florescent lighting.
  - **Auto** - Adjust the white balance automatically (default).
  - **Daylight** - Adjust the white balance for daylight.
  - **Cloudy** - Adjust the white balance for a cloudy environment.
- **Image Stabilization** - Set to reduce blurry videos due to device movement. Options: **On** or **Off** (default).

# Contacts

Use the **Contacts** app to manage contacts.

From a Home or Apps screen, touch **Contacts** to open to the main list of contacts. Contacts are listed in alphabetical order. Swipe up or down to scroll through the list.

## Adding a Contact

1. In the **Contacts** app, touch .
2. If there is more than one account with contacts, touch the one you want to use.
3. Type the contact's name and other information. Touch a field to start typing, and swipe down to view all categories.
4. To open a menu with preset labels, such as Home or Work for an email address, touch the label to the right of the item of contact information. Or, to create your own label, touch **Custom** in the menu.
5. Touch the check mark next to **Add New Contact**.

## Editing Contacts

1. In the **Contacts** app, touch a contact name to edit.
2. Touch .
3. Edit the contact information.
4. Touch **SAVE**.

## Deleting Contacts

1. In the **Contacts** app, touch a contact name to delete.
2. Touch .
3. Touch **Delete**.
4. Touch **DELETE** to confirm.

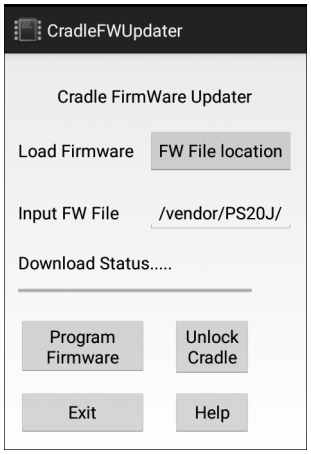
# Cradle Firmware Updater

The **Cradle Firmware Updater** app (**CradleFWUpdater**) allows the manual updating of cradle firmware using the PS20.

To update cradle firmware:

1. Go to the Zebra Support & Downloads web site, zebra.com/support or contact a Zebra Support Representative.
2. Download the **MC18CradleFWvx_x** firmware file to a host computer.
3. Using Android Debug Bridge (adb) or the sideload process, copy the firmware file to the PS20.
4. Swipe up from the bottom of the Home screen and touch **CradleFWUpdater**.
   The **CradleFWUpdater** screen displays.

Figure 47 CradleFWUpdater Screen




5. Dock the device in the cradle.
6. Select **FW File location**.
   The **Files** app opens.
7. Select the appropriate HEX firmware file and select OK.
   The path of the selected file displays in the **Input FW File** text box.
8. Verify the filename and extension.
9. Select **Program Firmware**. A warning dialog displays **Please don't remove device from cradle until FW Update complete. Continue?**.
10. Select **OK** to initiate the firmware update process.

**NOTE:** During the firmware initiation process, the application resets the cradle. If the following error dialog displays: **Please manually reset the cradle and then press OK,** the user is required to manually reset the cradle.

To manually reset the cradle:

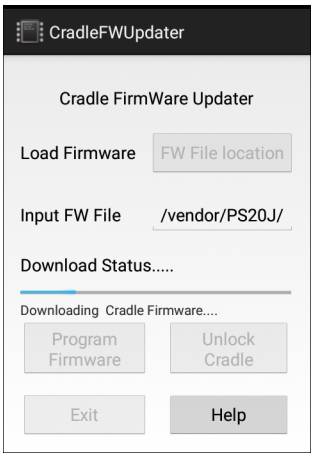
a. Disconnect power from the power supply unit of the cradle.
b. Reconnect power to the power supply unit of the cradle.

c. Select **OK** within 10 seconds after power on and before the LEDs on the cradle start glowing, to remove the error message and continue. Failing to select **OK** before the LEDs starts glowing will re-display the error message. If the user fails continuously 2 times, the firmware update process stops.

d. If the app is successful, it will start the downloading process.

11. After resetting the cradle, the app starts the firmware download process.

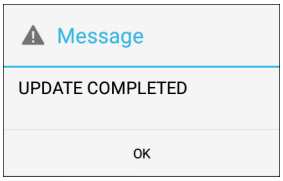
Figure 48 Cradle Firmware Updater - Firmware Download Process Screen




**CAUTION:** Do not attempt to disconnect power from the cradle or remove the device from the cradle during cradle firmware update. Removing the device from the cradle while firmware update is ongoing would result in an incomplete firmware update, leaving the cradle with partial firmware.
To recover from the situation of partially downloaded firmware, open the **Cradle Firmware Updater** app and perform a manual reset of the cradle power when alerted.

12. When **Download Complete** displays on the screen, the firmware update process is completed successfully. Select **Unlock Cradle** to unlock and remove the device from the cradle. Select **Help** for app information and instructions for using the app.

Figure 49 Cradle Firmware Updater - Download Complete Screen




## Sending the Firmware File Using Intents

### To send an intent using ADB:

1. Push the file to any location, preferably an sdcard or the following: enterprise/device/settings/cradleupdate.

2. Send the following intent:

   adb shell am broadcast -a com.symbol.intent.cradlefw.update --es cradleFwPath '<filename-alongwithpath>'

   Example:

   adb shell am broadcast -a com.symbol.intent.cradlefw.update --es cradleFwPath '/enterprise/device/settings/cradleupdate/MC18CradleFWv5_1.txt

### To send an intent using MDM:

1. Push the file to an sdcard.
2. Send the following command to change the permission of the file:

   chmod 644 <file-alongwithpath>

3. Send the following intent:

   adb shell am broadcast -a com.symbol.intent.cradlefw.update --es cradleFwPath '<filename-alongwithpath>'

   Example:

   adb shell am broadcast -a com.symbol.intent.cradlefw.update --es cradleFwPath '/enterprise/device/settings/cradleupdate/MC18CradleFWv5_1.txt

   _chmod 644 /enterprise/device/settings/cradleupdate/MC18CradleFWv5_2.txt

### To send the file using the Recovery Method:

1. Put the device in Recovery Mode.
2. Select Update via adb > FullPackageUpdate.
3. Enter the following at a command prompt:

   adb sideload <packagename>.

4. Reboot the device.

### To send an Airwatch intent:

1. Send the following intent:

   broadcast=true,mode=implicit,action=com.symbol.intent.cradlefw.update,extraString=cradleFwPath=/enterprise/device/settings/cradleupdate/MC18CradleFWv5_2.txt

### To send a SOTI intent:

1. Send the following intent:

   sendintent -b "intent:#Intent;action=com.symbol.intent.cradlefw.update;S.cradleFwPath=/enterprise/device/settings/cradleupdate/MC18CradleFWv5_1.txt;end;"

# Cradle Utility

Use the **Cradle Utility** to:

- Perform cradle operations (for example, unlock cradle or set LED)
- Configure cradle information (for example, Row ID or Column ID)
- Read the cradle manufacturing information
- Read the cradle diagnostics information.

To use the Cradle Utility:

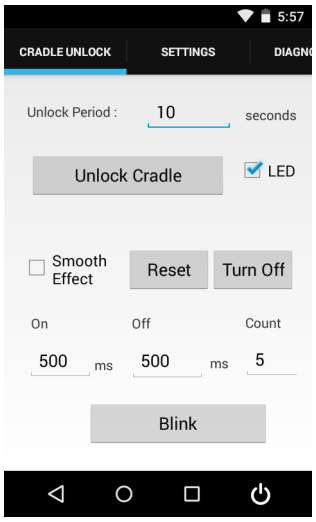
1. Dock the PS20 inside the cradle.
2. Swipe up from the bottom of the Home screen and touch .

**NOTE:** The cradle ID and location information and charge settings are retained across firmware upgrades.

## Controlling the Cradle

1. Tap the **CRADLE UNLOCK** tab to set the cradle unlock information.

Figure 50 Cradle Utility - Cradle Unlock Tab




- **Unlock Period**: The duration in seconds for which the PS20 remains in unlocked state (if not removed from the cradle). For example; if unlock period is set to 15 and unlock signal is received, the PS20 will unlock and lock back after 15 seconds (if its not removed by user).
- **Unlock Cradle**: Press **Unlock Cradle** to manually unlock the PS20 from the cradle.
- **LED**: Check the LED box to enable the cradle LED indication.
- **Smooth Effect**: Check the Smooth Effect box to enable smooth blinking of the LEDs.
- LED Setting > **On**: The duration (in ms) that the cradle LED remains turned on or blinks during unlock.
- LED Setting > **Off**: The duration (in ms) that the cradle LED remains turned off or blinks during unlock.
- LED Setting > **Count**: The number of times the cradle LED blinks when user presses the blink button.

- **Blink**: Tap to test the cradle LED operation.

## Setting the Cradle

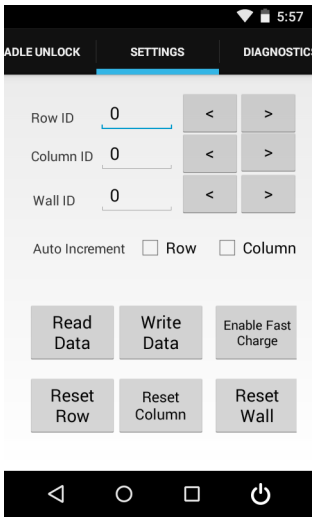
The **Cradle Utility** allows you to manually enter cradle settings. To automatically enter cradle settings, use the optional Smart Cradle Configuration app (**CradleSmartConfig**).

**Setting the cradle charging rate**: Depending on the cradle installation configuration, the store technician can configure each individual cradle slot to enable/disable fast charge. Each cradle can be configured to charge its docked terminal at 1A (normal charging mode - default setting) or 1.5A (fast charging mode).

**NOTE:** The cradle charging rate is retained across firmware upgrades.

1. Tap the **Settings** tab to set the cradle information.

Figure 51 Cradle Utility - Setting Tab

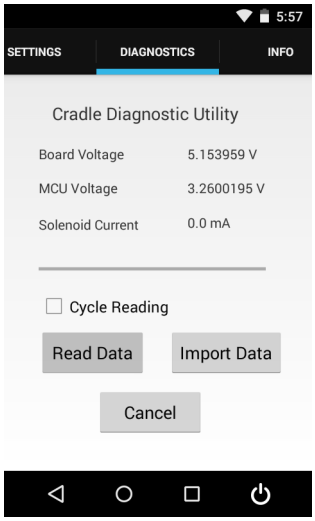



- **Row ID**: The cradle row number in the dispenser wall.
- **Column ID**: The cradle column number in the dispenser wall.
- **Wall ID**: The number of dispenser wall where the cradle is positioned.
- **Read Data**: Retrieve setting data from the cradle memory and display on the screen.
- **Write Data**: Tap this button to program the row/col/wall information onto the cradle. Note that each slot on the Three Slot Cradle needs to be programmed separately.
- **Enable Fast Charge**: Enable the cradle to charge the PS20 at a current of 1.5A (default setting is 1A)
- **Reset Row**: Tap to update the **Row ID** in the text field to “0” on the application.
- **Reset Column**: Tap to update the **Column ID** in the text field to “0” on the application.
- **Reset Wall**: Tap to update the **Wall ID** in the text field to “0” on the application.

## Performing Cradle Diagnostics

1. Touch **Diagnostic** tab to perform the cradle diagnostics:

Figure 52 Cradle Utility - Diagnostic Tab

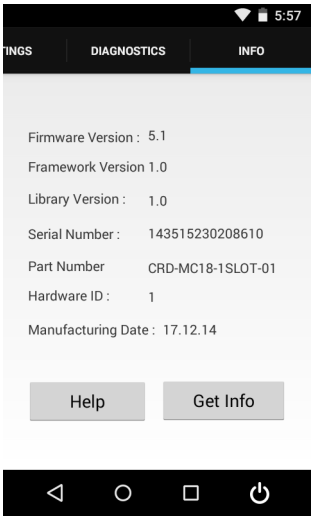



- **Cycle Reading**: Check the **Cycle Reading** box to perform continuous diagnostics and display the cradle status information. During diagnostics, a progress bar is shown of the screen.
- **Read Data**: Tap to start performing diagnostics.
- **Import Data**: Tap to save the recorded results of the diagnostics on a file.

## Viewing Cradle Information

1. Touch **Info** tab.

Figure 53 Cradle Utility - Info Tab



# Smart Cradle Configuration

The Smart Cradle Configuration app (**CradleSmartConfig**) avoids the need to manually enter the row, column, and wall ID's during the cradle wall configuration. Unlike using the Cradle Utility, where these values are entered for each slot, **CradleSmartConfig** guides the user through the configuration process. Additionally, the app implements automatic error checks and provides auditing mechanisms (Quick/Full) once the configuration is completed.

Use **CradleSmartConfig** to:

- Declare the wall map (row, column, wall, current)
- Declare empty/blank spots (kiosk, TV, computer monitor, or unique store shapes)
- Follow a screen guided sequence to read/program each slot based on the guided map
- Catch errors (duplication, skipped slots, and non-programmed slots).

## Support

**CradleSmartConfig** supports the following:

- Single slot and three slot cradles.
- Selectively removing certain cradle slots from the matrix, as placeholders for a kiosk, TV, computer monitor, or unique store shapes.
- Scrolling the screen left/right and up/down.
- A panning view of the cradle wall to be shown below the cradle icons as an indication of where the current focus is.

## Prerequisites/Assumptions

**CradleSmartConfig** requires the following prerequisites or assumes the following:

- The customer knows by a paper map or plan what the rows and columns should be set to for the wall.
- The wall is rectangular.
- Empty/blank spots are known (spots that do not have cradles).
- All three slot cradles should be the same type.
- SmartCradleConfig is installed on the device before starting.
- The default charging rate setting is 1A.

## Error Prevention

**CradleSmartConfig** helps prevent user errors by:

- Detecting if a slot has already been programmed properly.
- Detecting if a slot was missed (for example, 1,2,3,1,2,3,2,3)
- Providing screen guides as to the direction of the next slot to program.
- Guiding when to move up or down a row.
- Audible or visual cues when an error is made.

- Automatically programming Wall/Row/Column/Current once it has detected it moved to the proper next slot.
- Signaling when ready to move to the next slot (audible chime to indicate programming was successful).

## Accessing CradleSmartConfig

To access CradleSmartConfig:

1. Go to the Zebra Support & Downloads web site for the PS20, zebra.com/ps20-info.
2. Download **CradleSmartConfig** to a host computer.

**NOTE:** This app is not pre-loaded on the device and must be downloaded and installed prior to use.

3. Use the sideload process to copy the **CradleSmartConfig.apk** file onto a single PS20 device.
4. Install the app.

## Using CradleSmartConfig

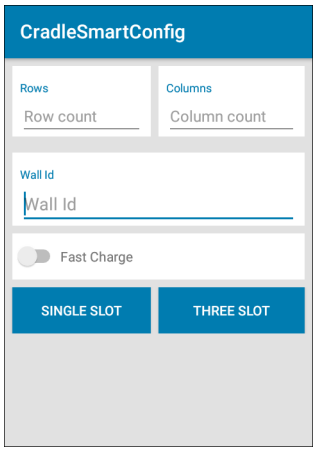
To configure the cradle wall using CradleSmartConfig:

**NOTE:** Prior to using CradleSmartConfig, all new cradles should be mounted to a wall, including all power connections. It is assumed that no programming has occured and all cradles are functioning with a unique serial number programmed in them from the factory.

1. Swipe up from the bottom of the Home screen and touch **CradleSmartConfig** .

   The **CradleSmartConfig** screen displays.

Figure 54 CradleSmartConfig Screen




2. Complete the following:
   - **Rows** - The cradle row number in the dispenser wall.
   - **Columns** - The column number in the dispenser wall.
   - **Wall ID** - The number of dispenser wall where the cradle is positioned.
   - **Fast Charge** - Touch to enable the cradle to charge the PS20 at a current of 1.5A (default setting is 1A).

**NOTE:** The cradle ID, location, and charging rate are retained across firmware upgrades.

3. Select **SINGLE SLOT** to program a wall of single slot cradles or select **THREE SLOT** to program a wall of three slot cradles.

   A map of cradle icons display, based on the number of rows and columns entered in the previous step. For reference, the top left corner is Row 1, Column 1 (R1C1).

4. (Optional) Navigate around the screen.

   To scroll left/right and up/down:

   a. Touch and drag your finger on the screen.

   b. Locate the graphic on the bottom of the screen to show where you are on the map. Scroll bars allow you to drag the screen to see a portion of the total wall.

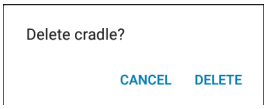
5. (Optional) Delete cradle slots not used. For example, placeholders for a kiosk, TV, computer monitor, or unique store shapes.

   To delete cradle slots:

   a. Touch and hold (long press) the cradle slot icon.

   b. Select **DELETE** to confirm.

Figure 55 Delete Cradle




6. Insert a PS20 device in the first cradle in the top left corner (Row 1, Column 1).

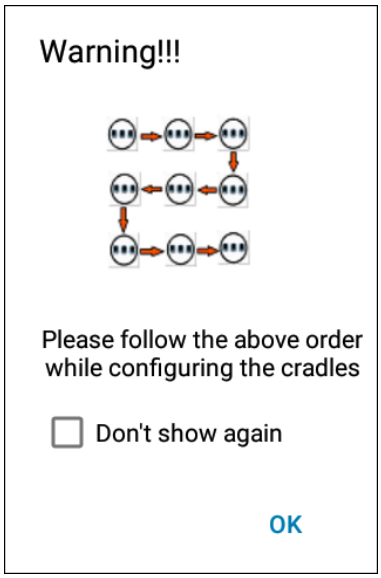
7. Touch **Start**.

   A Warning dialog displays indicating the correct sequence to follow when configuring the cradles.

8. Select **Ok**.

   CradleSmartConfig programs the row, column, and wall information onto the cradle.

Figure 56 Warning Dialog - Follow Specified Order

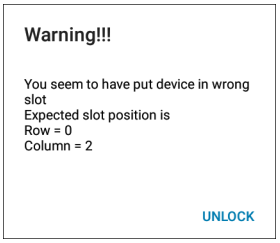



After the first cradle is programmed successfully, a check mark appears in the location of the cradle icon and an arrow on the screen points in the direction of where to insert the device in the next slot. An audible sound or visual cradle charge indication may be present.

9. Remove the device from the first cradle, and move in the specified direction to insert the device in the next slot.

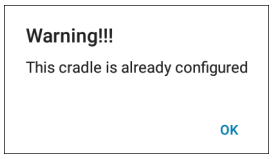
   CradleSmartConfig directs the user to move in the proper direction. If the device is inserted into the wrong slot, the user is prompted.

Figure 57 Warning! Wrong Slot




If the device is inserted into the same slot, a message indicates that the cradle has already been configured.

Figure 58 Warning! Cradle Already Configured

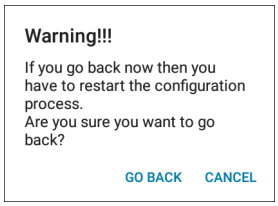



Note that each slot on the Three Slot Cradle needs to be programmed separately. The app guides the user to change rows in a zig-zag pattern for efficiency, with the first row going from left to right with serial numbers (last digits) 1,2,3 and the next row going from right to left with serial numbers (last digits) 3,2,1. The app also guides the user to skip the empty or blank areas. In a single slot cradle, the HW serial number last digit is 0.

10. Moving in the direction specified, repeat until all cradles are configured.

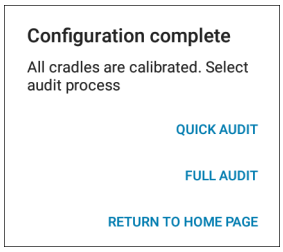
    If the user abandons programming before the entire wall is completed, the user must start over from the beginning.

Figure 59 Warning! Restart Configuration Screen




The app detects when it has reached the end of the wall and the **Configuration complete** dialog displays.

Figure 60 Configuration Complete Dialog




11. Select one of the following:
    - **QUICK AUDIT** - A sample of cradles are validated and the expected data is compared to what is actually found. Blinking cradles are displayed one after the other at the four corners. The device to be validated should be placed in the middle slot of the blinking icon.
    - **FULL AUDIT** - All cradles are validated and the expected data is compared to what is actually found.
    - **RETURN TO HOME PAGE** - Displays the CradleSmartConfig screen.

# Auditing

Auditing validates that the cradles have been programmed correctly. The expected results should match the results found.

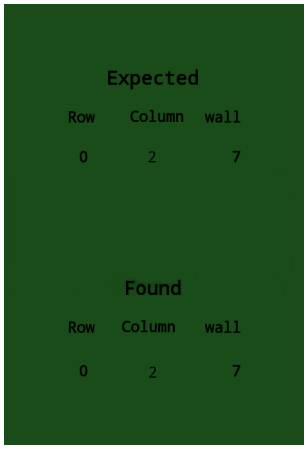
## Quick Audit

To perform a quick audit:

1. The four corner cradles will blink one after another. Place the device in the middle slot of the first blinking cradle icon.

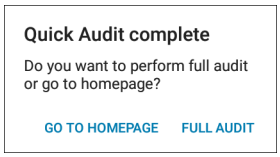
   If the audit was successful and the expected results match the results found, a green screen displays. If the audit failed and the expected results do not match the results found, a red screen displays.

Figure 61 Successful Audit Screen




2. Moving in the direction specified, repeat until all cradles are validated.
   The app detects when it has reached the end of the wall and the **Quick Audit complete** screen displays.

Figure 62 Quick Audit Complete Screen



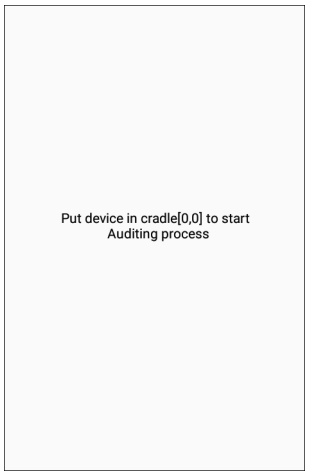

3. Select **FULL AUDIT** to perform a Full Audit or select **GO TO HOMEPAGE** to return to the **SmartCradleConfig** screen.

## Full Audit

To perform a Full Audit:

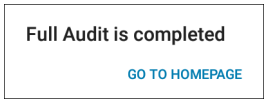
1. Place the device in the first cradle, first slot in the top left corner (Row 1, Column 1).
   The app detects the cradle in operation and starts validating the current slot.

Figure 63 Start Audit Process



2. Moving in the direction specified, repeat until all cradles are validated.
   The app detects when it has reached the end of the wall and the **Full Audit is completed** screen displays.

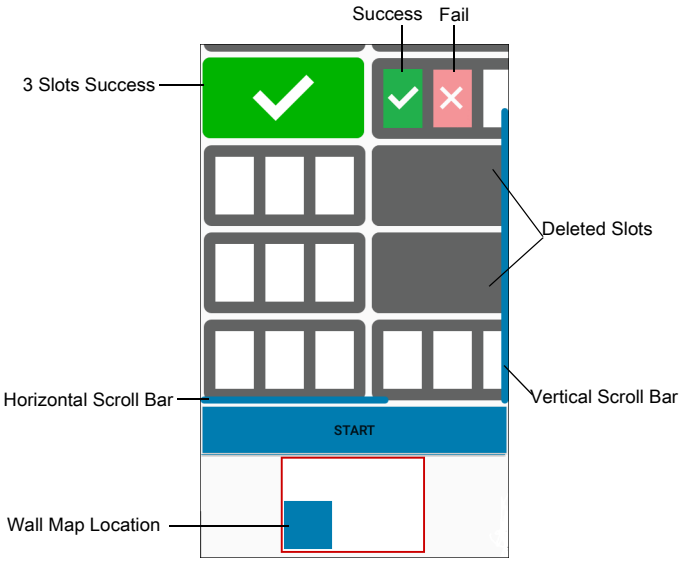
Figure 64 Full Audit Complete Screen



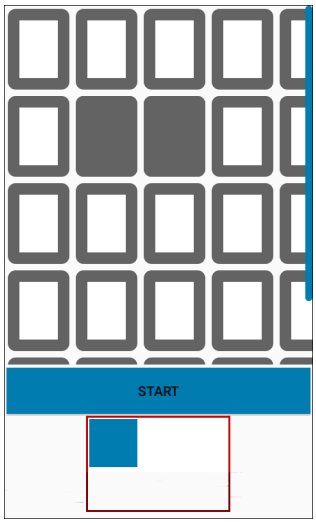

3. Select **GO TO HOMEPAGE** to return to the **SmartCradleConfig** screen.

## Wall Map Examples

Figure 65 Wall Map Examples




Three Slot Cradle: 5 Rows, 3 Columns




Single Slot Cradle: 5 Rows, 5 Columns

# DataWedge Demonstration

**NOTE:** DataWedge is enabled on the Home screen.To disable this feature, go to the DataWedge settings and disable the **Launcher** profile.

Use **DataWedge Demonstration** to demonstrate data capture functionality.

Figure 66 DataWedge Demonstration Window

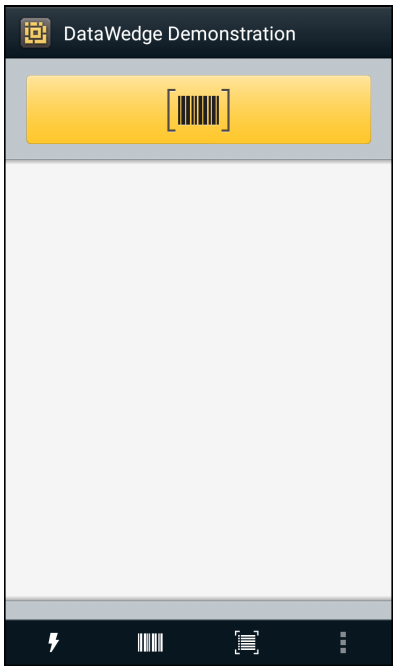



*Table 16 DataWedge Demonstration Icons*

| | Icon | Description |
|---|---|---|
| Illumination | | Imager illumination is on. Touch to turn illumination off. |
| | | Imager illumination is off. Touch to turn illumination on. |
| Data Capture | | The data capture function is through the internal imager. |
| | | AnRS6000 Bluetooth imager is connected. |
| | | AnRS6000 Bluetooth imager is not connected. |

*Table 16 DataWedge Demonstration Icons (Continued)*

| | Icon | Description |
|---|---|---|
| Scan Mode |  | Imager is in picklist mode. Touch to change to normal scan mode. |
| |  | Imager is in normal scan mode. Touch to change to picklist mode. |
| |  | Opens a menu to view the application information or to set the application DataWedge profile. |

## Scanner Selection

To select a scanner, touch ⋮ > **Settings** > **Scanner selection**.

See Data Capture for more information.

Either press the programmable button or touch the yellow scan button to capture data. The data appears in the text field below the yellow button.

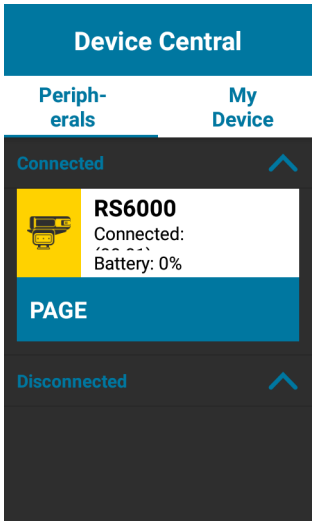
# Device Central

**Device Central** displays detailed information about the device and connected peripherals and supports the following Zebra devices:

**Device Central** features include:

- Discovering and pairing with supported peripherals via Bluetooth or corded connection.
- Paging a connected RS6000 Ring Scanner.
- Displaying the connection status of peripherals.
- Displaying information for a connected peripheral in the notification bar.

Figure 67 Device Central Screen




1. Touch **Get Info** to read the cradle information.

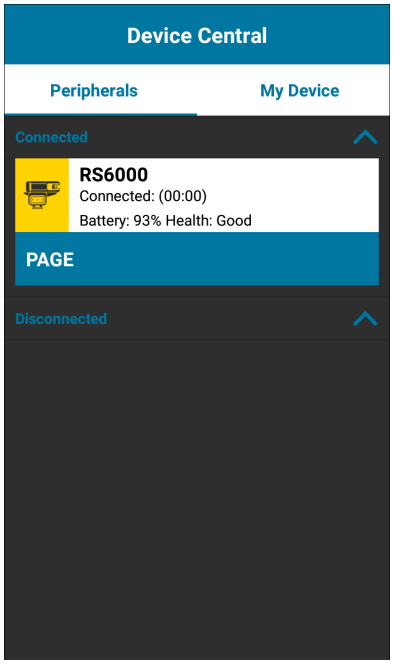
## Device Central Tabs

- **Peripherals** Tab - displays all currently connected and previously connected peripherals. Connected peripherals display the length of time (in minutes) that they have been connected. When an RS6000 is connected the **Page** button displays. See Paging an RS6000 Ring Scanner.

Touch the peripheral information to display the **Device Details** screen.

  - **Device Details** - displays detailed device information for the selected peripheral.
- **My Device** Tab - displays information about the device and the current version of Device Central.
  - **Device Details** - displays the **Phone status** screen.
  - **Device Battery Details** - displays the **Battery** screen.

Figure 68 Peripherals Tab




## Paging an RS6000 Ring Scanner

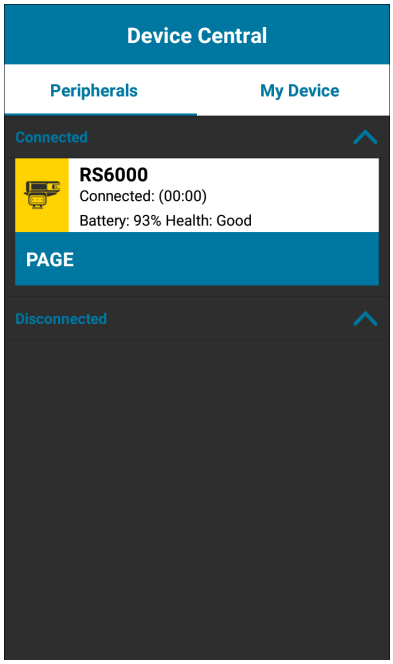
Use **Page** to easily locate the connected RS6000 Ring Scanner:

1. With the RS6000 Ring Scanner connected, swipe up from the bottom of the screen and touch .

**NOTE:** The RS6000 Ring Scanner must be within 10 m (32 ft) of the device.

2. Under the RS6000 peripheral information, touch **Page** to page the RS6000. The paged RS6000 beeps and vibrates.

Figure 69 Page RS6000



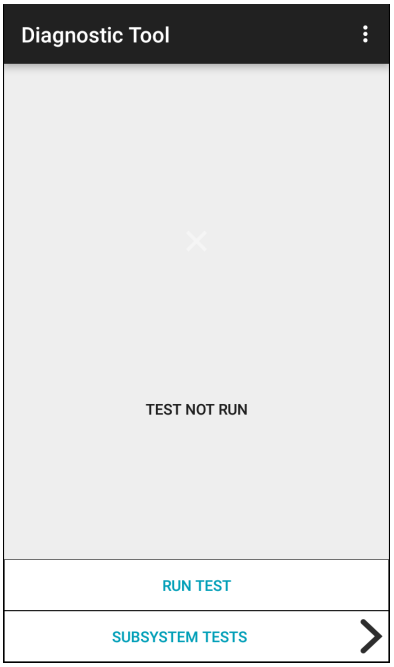

To stop paging, press the scan trigger of the RS6000. On a triggerless RS6000, reset the RS6000 to stop paging. Refer to the RS6000 User Guide.

# Diagnostic Tool

The **Diagnostic Tool** is a utility that determines the health of the device. Use the Diagnostic Tool to troubleshoot the device.

1. Swipe up from the bottom of the Home screen and touch .

Figure 70 Diagnostic Tool




2. Touch **RUN TEST**. The app tests all enabled subsystems (by default, only the Battery and System tests). See Settings to enable subsystem tests.

Figure 71 Test Passed Screen

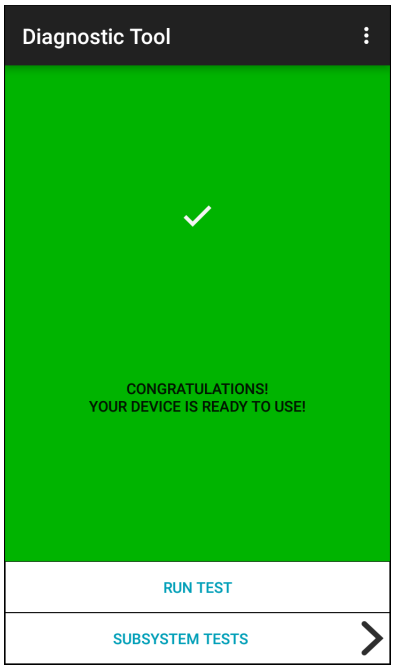
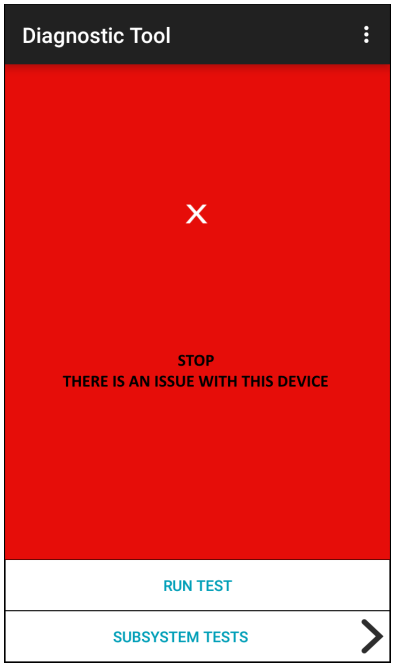
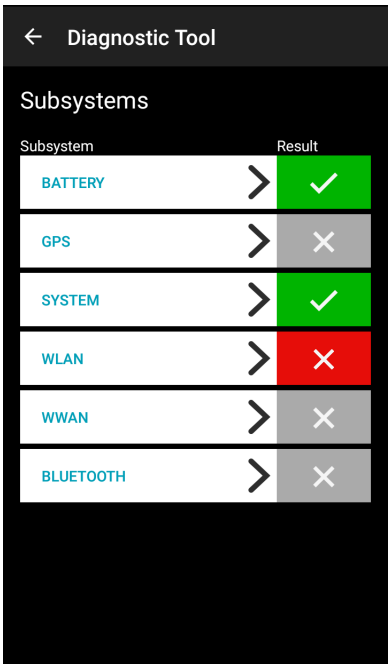



Figure 72 Test Failed Screen




3. To view each subsystem test, touch **Subsystem Tests**.

Figure 73 Subsystem Screen

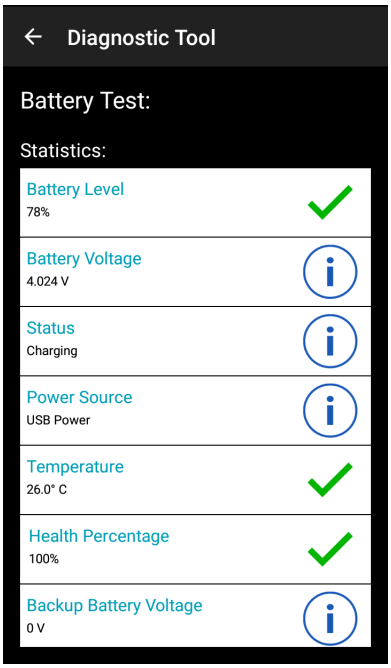



4. Touch one of the subsystems to view details.

*Table 17 Subsystem Test Result Indicators*

| Status Icon | Description |
|---|---|
| ✓ | Test passed. |
| ✗ | Test failed. |
| ✗ | Test not supported or not enabled. |

Figure 74 Battery Subsystem Details




## Settings

By default only the Battery and System tests are enabled. To enable other tests:

1. Touch ⋮ > **Settings**.
2. Touch to the left of the test name. A green box with a checkmark appears.
3. Touch **SAVE**.
4. Touch **Yes** to confirm.
5. Touch ◁.

## Battery Test Information

The Battery Test obtains the following information:

- **Battery Level** - Current battery charge level
- **Battery Voltage** - Current battery voltage
- **Status** - Whether the battery is charging (on AC power) or discharging (on battery power)
- **Power Source** - Whether the device is receiving power from the battery or from an external source
- **Temperature** - Current battery temperature

- **Health Percentage** - Indicates the ratio of present capacity to design capacity at a discharge rate of design capacity.
- **Backup Battery Voltage** - Backup battery voltage.
- **Manufacture Date** - Manufacture date of the battery.

## System Test Information

Use the System Test to determine if the CPU or memory loads are too high, there are too many processes running on the device, or storage on the device is almost full.

The System Test obtains the following information:

- **CPU Load** - Amount of CPU being used
- **Free Physical Memory** - Amount of RAM available
- **Free Storage** - Amount of internal Flash memory available
- **Process Count** - Number of processes currently running.

## WLAN Test Information

If the WiFi radio is not present or disabled, skip this test. This test determines if the device's WLAN configuration is correct or whether there is any connection with an access point or network.

The WLAN test obtains the following information:

- **WLAN Enabled** - WLAN radio is enabled or disabled
- **WLAN Status** - Current status of association with the access point
- **ESSID** - Name of the wireless network
- **BSSID** - MAC address of the connected access point
- **MAC Address** - Device's MAC address
- **Signal** - Strength of the Wi-Fi signal (in dBm)
- **IP Address** - IP address of the device.

## Bluetooth Test Information

The Bluetooth Test obtains the following information:

- **Enabled** - Whether the Bluetooth radio is enabled or disabled
- **Status** - Whether the device is paired to another Bluetooth device
- **Connectable/Discoverable** - Whether the device is discoverable or able to connect
- **Address** - Bluetooth radio MAC address

- **Name** - Bluetooth name for the device.

# Enterprise Browser

The Enterprise Browser is an industrial browser that provides everything needed to quickly build device apps for barcode scanning, signature capture, payment processing, printing and most other enterprise applications.

Enterprise Browser includes a runtime environment inside which a company's application logic can be executed and controlled using HTML5 and CSS3 for presentation and JavaScript to access Enterprise Browser APIs for scanners, cameras, card readers and other device peripherals.

The base Enterprise Browser installation includes all necessary components to allow a Windows development host to easily build device apps and set runtime settings for local or mass-deployment using Zebra StageNow or a mobile device management (MDM) system. If migrating from another platform, Enterprise Browser also can run apps built for PocketBrowser, RhoElements and the RhoMobile Shared Runtime, making it an ideal path for moving apps to a newer UI, device or platform.

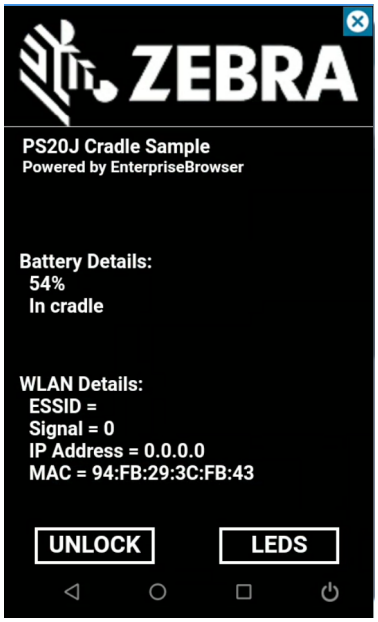
For more information, refer to techdocs.zebra.com/enterprise-browser/.

## Enterprise Browser Application

The device comes with an Enterprise Browser application pre-licensed and pre-loaded. The application is accessible from the apps screen.

1. Swipe up from the bottom of the Home screen, and touch **EnterpriseBrowser**.

Figure 75 Enterprise Browser Screen




The default Enterprise Browser page provides the following information:

- Battery Details:
  - Battery strength in percentage
  - Whether in cradle or not

- WLAN Details:
  - ESSID name
  - Signal
  - IP Address of the device
  - MAC address of the device

The buttons at the bottom of the screen:

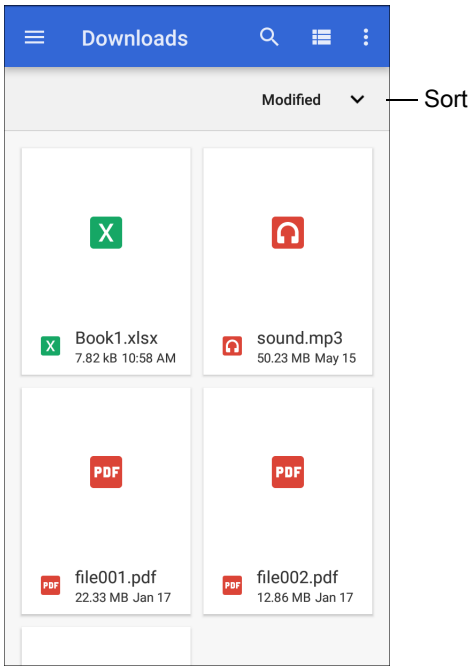
- UNLOCK - Unlocks the device in the cradle.
- LEDS - Illuminates the cradle LEDs.

# Files

Use the **Files** app to view and manage files on the device.

To open **Files**, swipe up from the bottom of the screen and touch .

Figure 76 Files Screen




- Touch and hold an item to open the File Operations menu. Select an option:
  - - Share the file with other devices.
  - - Delete the file.
  - - View additional options.
    - **Open with** - Select which app is used to open the file.
    - **Select all** - Select all folders and files.
    - **Copy to...** - Copy the file.
    - **Move to...** - Move the file or folder to a new location.
    - **Compress** - Compress the selected file(s) into a ZIP file.
    - **Rename** - Rename the file.
- Touch the Sort drop-down to sort files by name, type, size, or date.
- - View all file locations.
- - Search for a specific file on the device.
- / - Change the folder to display items as a list / grid.
- - Open the options menu.
  - **New Window** - Create a new Files window.
  - **New Folder** - Create a new folder.
  - **Select all** - Select all folders and files.
  - **Show/Hide internal storage** - Show or hide internal storage.

# Gallery

**NOTE:** The device supports the following image formats: jpeg, gif, png and bmp.
The device supports the following video formats: H.263, H.264 and MPEG4 Simple Profile.

Available on device with AOSP only.

Use Gallery to:

- View photos
- Play videos
- Perform basic editing of photos
- Set photos as wallpaper
- Set photos as a contact photo
- Share photos and videos.

**Gallery** presents all photos and videos stored on the internal memory.

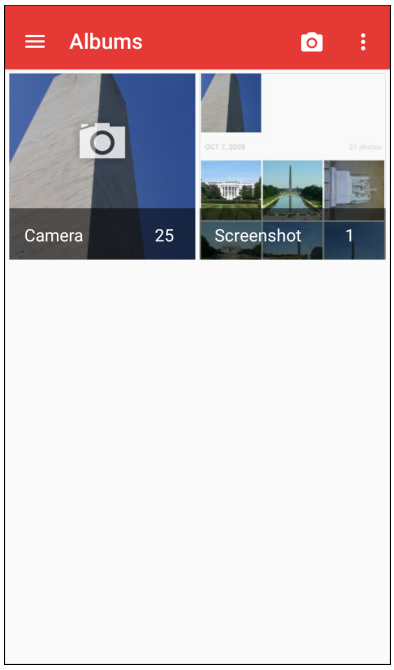
To open **Gallery**, swipe up from the bottom of the Home screen and touch **Gallery**, or in the camera app touch the thumbnail image at the bottom left.

By default, **Gallery** opens to the **Timeline** view.

Figure 77 Gallery - Timeline View


Touch ☰ > **Albums** to view photos sorted by albums or ☰ > **Videos** to view only videos.

Figure 78 Gallery — Albums View




- Touch an album to open it and view its contents. The photos and videos in the album are displayed in chronological order.
- Touch a photo or video in an album to view it.
- Touch ☰ > **Timeline** to return to the default **Gallery** screen.

## Working with Albums

Albums are groups of images and videos in folders. Touch an album to open it. The photos and videos are listed in a chronologically ordered grid. The name of the album displays at the top of the screen.

Figure 79 Photos Inside an Album


Swipe up or down to scroll through the images.

## Sharing an Album

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch and hold an album to highlight it.
3. Touch other albums as required.
4. Touch . The Share menu opens.
5. Touch the app to use to share the selected albums.
6. Follow the instructions within the selected app.

## Getting Album Information

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch and hold an album to highlight it.
3. Touch .
4. Touch **Details**.

### Deleting an Album

To delete an album and its contents:

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch and hold an album to highlight it.
3. Check other albums to delete.
4. Touch .
5. In the **Delete selected item?** menu, touch **OK** to delete the album.

## Working with Photos

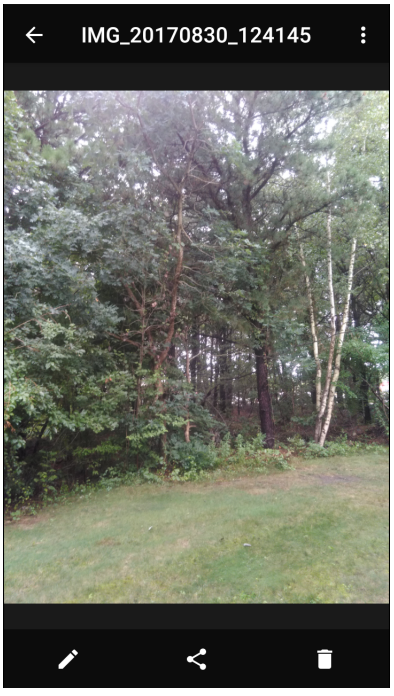
Use **Gallery** to view photos on the device and edit and share photos.

### Viewing and Browsing Photos

To view a photo:

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a photo.

Figure 80 Photo Example

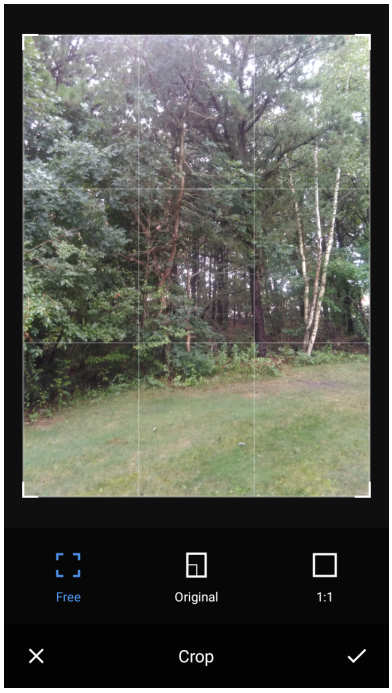


4. Swipe left or right to view the next or previous photo in the album.
5. Turn the device to view the photo in upright (portrait) or sideways (landscape) orientation. The photo is displayed (but not saved) in the new orientation.
6. Touch the photo to view the controls.
7. Double-tap the screen to zoom in or pinch two fingers together or spread them apart to zoom in or out.
8. Drag the photo to view parts that are not in view.

## Cropping a Photo

1. In **Gallery**, touch a photo to view the controls.
2. Touch > > . The cropping tool appears.
3. Use the cropping tool to select the portion of the photo to crop.
   - Drag from the inside of the cropping tool to move it.
   - Drag an edge of the cropping tool to resize it to any proportion.

Figure 81 Cropping Tool




4. Touch ✓ > **SAVE** to save a copy of the cropped photo. The original version is retained.

## Setting a Photo as a Contact Icon

1. Swipe up from the bottom of the Home screen and touch **Gallery**.

2. Touch an album to open it.
3. Touch a photo to open it.
4. Touch ⋮.
5. Touch **Set picture as**.
6. Touch **Contact photo**.
7. In **Contacts**, touch a contact.
8. Touch the white box and crop the photo accordingly.
9. Touch **SAVE**.

### Sharing a Photo

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a photo to open it.
4. Touch <.
5. Touch the app to use to share the selected photo.
6. Follow the instructions within the selected app.

### Deleting a Photo

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a photo to open it.
4. Touch 🗑.
5. Touch **OK** to delete the photo.

## Working with Videos

Use **Gallery** to view and share videos.

## Watching Videos

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a video.
4. Touch to play.
5. Touch the screen to view the playback controls.

## Sharing a Video

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a video to open it.
4. Touch . The Share menu appears.
5. Touch the app to use to share the selected video.
6. Follow the instructions within the selected app.

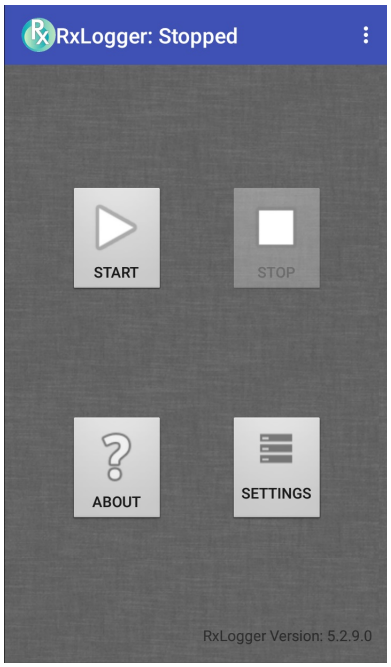
## Deleting a Video

1. Swipe up from the bottom of the Home screen and touch **Gallery**.
2. Touch an album to open it.
3. Touch a video to open it.
4. Touch .
5. Touch **OK**.

# RxLogger

RxLogger is a comprehensive diagnostic tool that provides app and system metrics. Create custom plug-ins that work seamlessly with this tool. RxLogger diagnoses device and application issues, and tracks information for: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging, TCP dumps, Bluetooth logging, GPS logging, logcat, ANR dumps, etc. All logs and files generated are saved in flash storage on the device (internal or external).

Figure 82 RxLogger

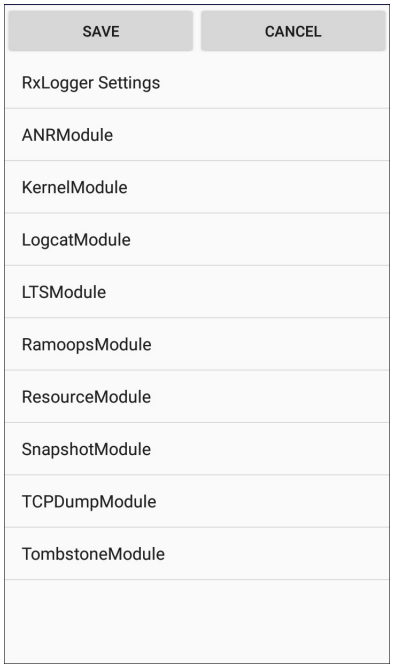



## RxLogger Configuration

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 83** RxLogger Configuration Screen




## Configuration File

RxLogger configuration can be set using an XML file. The **`config.xml`** configuration file is located 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

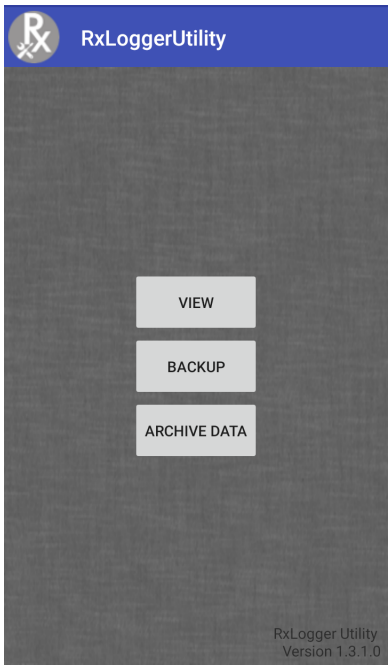
1. Connect the device to a host computer using an USB connection.
2. Using a file explorer, navigate to the **`RxLogger`** folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

# RxLogger Utility

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

In the App View, view logs in the RxLogger Utility.

Figure 84 RxLogger Utility App View




Refer to the Settings chapter for detailed information on the RxLogger Utility.

# Data Capture

## Introduction

The PS20 imager allows collection of data by scanning bar codes.

The imager has the following features:

- Reads a variety of bar code symbologies, including the most popular linear, postal, and 2-D code types (see Specifications).
- Contains advanced intuitive aiming light for easy point-and-shoot operation.

**NOTE:** Bluetooth scanners are not supported.

## Scanning Considerations

Typically, scanning is a simple matter of aim, scan, and decode, with a few quick trial efforts to master it. However, consider the following to optimize scanning performance:

- **Range:** Scanners decode best over a particular working range — minimum and maximum distances from the barcode. This range varies according to barcode density and scanning device optics. Scan within range for quick and constant decodes; scanning too close or too far away prevents decodes. Move the scanner closer and further away to find the right working range for the barcodes being scanned.
- **Angle:** Scanning angle is important for quick decodes. When the illumination/flash reflects directly back into the imager, the specular reflection can blind/saturate the imager. To avoid this, scan the barcode so that the beam does not bounce directly back. Do not scan at too sharp an angle; the scanner needs to collect scattered reflections from the scan to make a successful decode. Practice quickly shows what tolerances to work within.
- Hold the device farther away for larger symbols.
- Move the device closer for symbols with bars that are close together.

**NOTE:** Scanning procedures depend on the app and device configuration. An app may use different scanning procedures from the one listed above.

## Scanning Bar Codes

To scan a barcode:

1. Launch a scanning application.
2. Press the Scan key and aim the device at a barcode.

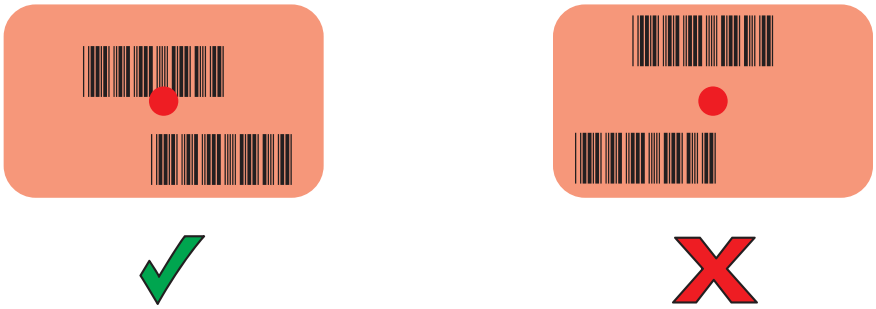
3. Adjust the position of the device so that the:
   - Red aiming dot appears at the center of the barcode on devices with the SE4710 imager.
   - White LED appears around the barcode on devices with the SE2100 imager.

   Ensure the barcode is within the area formed by the aiming pattern. On devices with the SE4710 imager, the aiming dot is used for increased visibility in bright lighting conditions.
4. Press the Scan key.

   The Status LED illuminates red. Upon successful decode, the Status LED changes from red to green and an audible beep sounds.

Figure 85 SE4710 Imager Decode Mode

Figure 86 SE4710 Imager Picklist Mode



**NOTE:** Picklist Mode is only available on the PS20 with the SE4710 imager. When the PS20 is in Picklist Mode, the imager does not decode the barcode until the crosshair or aiming dot touches the barcode.

Figure 87 SE2100 Imager Decode Mode

5. Release the Scan key.

   The barcode data displays on the screen.

### Scanning Tips

Optimal scanning distance varies with bar code density and scanner optics.

- Hold the scanner farther away for larger symbols.
- Move the scanner closer for symbols with bars that are close together.

**NOTE:** Scanning procedures depend on the application and PS20 configuration. An application may use different scanning procedures from the one listed above.

## Decode Screen Notification

Scan Params in DataWedge includes an option for **Decode Screen Notification**. Enable this option to display a translucent green screen overlay as a notification for each successful decode. In addition, Scan Params includes options for **Decode Screen Notification Timer** and **Decode Screen Translucency Level**, which allow you to set the green screen overlay time in milliseconds and the level of translucency.

**NOTE:** For **Decode Screen Notification** to work, **Display over other apps** permission must be granted for the application.

Figure 88 Translucent Green Overlay Decode Screen Notification

# DataWedge

DataWedge is a utility that adds advanced barcode scanning capability to any application without writing code. It runs in the background and handles the interface to built-in barcode scanners. The captured barcode data is converted to keystrokes and sent to the target application as if it was typed on the keypad.

To configure DataWedge refer to the device Integrator Guide or Product Reference Guide.

# Enabling DataWedge

1. Swipe up from the bottom of the Home screen and touch .
2. Touch ⋮ > **Settings**.
3. Touch the **DataWedge enabled** checkbox. A blue checkmark appears in the checkbox indicating that DataWedge is enabled.
4. Touch ◯.

## Disabling DataWedge

1. Swipe up from the bottom of the Home screen and touch .
2. Touch ⋮ > **Settings**.
3. Touch the **DataWedge enabled** checkbox. A blue checkmark disappears from the checkbox indicating that DataWedge is disabled.
4. Touch ◯.

# Hands Free Scanning

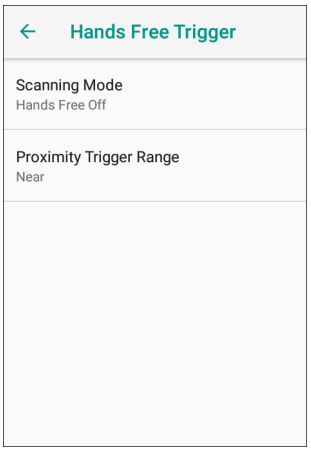
Hands Free Scanning allows the user to capture barcode data when a barcode is placed within the view of the device without pressing the trigger. Hands Free Scanning is enabled using the **Hands Free Trigger** settings or when the device is placed in the cart/mount. Hands Free Scanning is set to disabled by default.

## Settings

Use the Hands Free Trigger setting to configure scanning mode and the proximity trigger sensitivity.

Swipe down from the Status bar to open the Quick Access panel and then touch ⚙ > **Hands Free Trigger**.

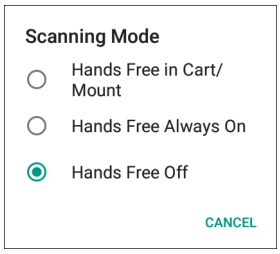
Figure 89 Hands Free Trigger Settings




## Scanning Mode

Use the **Scanning Mode** settings to configure how the device functions while in hands free scanning mode.

Figure 90 Scanning Mode Dialog Box



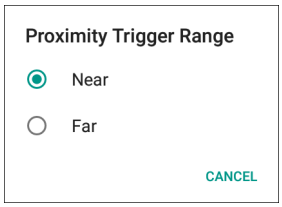

- **Hands Free in Cart/Mount** - Select to enable scanning when the device is in the cart/mount. The device detects the difference between in-motion and stationary states. When the device is in the Motion state, proximity scanning is disabled. When the device is in the Stationary state or in a hands free cart/mount, proximity scanning is enabled.
- **Hands Free Always On** - Select to place the device in hands free scanning mode.
- **Hands Free Off** - Select to disable hands free scanning mode (default).

**NOTE:** In order to use the **Hands Free in Cart/Mount** scanning mode, the devices in a store must be calibrated to the cart orientation first. If the hands free scanning mode is enabled, and if the device is properly calibrated, the device will be detected that it's in a cart and enable the hands free trigger. While in the cart, the device displays a shopping cart notification in the status bar. For more information about creating and deploying the calibration file, see the PS20 Personal Shopper Calibration App User Guide at zebra.com/ps20-info.

## Proximity Range

To configure the proximity sensor range sensitivity, touch **Proximity Trigger Range**.

Figure 91 Proximity Trigger Range Dialog Box




- **Near** - Proximity sensor detects and generates a trigger when the barcode is within 0 to 20 cm (nominal) (default).
- **Far** - Proximity sensor detects and generates a trigger when the barcode is within 0 to 60 cm (nominal).

# Cradle Installation

## Introduction

A typical Personal Shopper system is comprised of a family of hardware devices interconnected through a WLAN radio backbone to the retail establishment's server(s). The hardware devices are the PS20 personal shoppers, single slot or three slot cradles, power supplies and cables. A *dispenser* typically refers to a piece of furniture which has mounted to it the cradles, their power supplies, and cables.

Customers (retail establishments) design their own dispensers to meet their particular floor space and display requirements. The information in this chapter should help a customer to design a dispenser and to understand the installation requirements.

**IMPORTANT:** The MC18 cradles are compatible with the PS20.

## Installation of the Single Slot Cradle

Installation of the Single Slot Cradle include the following mounting steps:

- Select the charging mode (see Charging Modes on page 134)
- Mount the Single Slot Cradles on a dispenser wall (see Mounting the Single Slot Cradle on a Dispenser Wall on page 135)
- Connect the wires to the cables (see Wiring on page 137)
- Set the cradle(s) (see Controlling the Cradle on page 110)

### Charging Modes

Single Slot Cradles can be installed in the following charging modes:

- Standard charging
- Fast charging

There are some general charging considerations that must be taken into account when designing a dispenser and ordering hardware elements of a system:

#### Standard Charging Mode

- In standard charging mode, no more than 12 cradles can be powered off of one power supply unit (p/n PWR-BGA12V108W0WW) using "Y" power cable CBL-DC-392A1-02.
- In standard charging mode, the current draw by each docked PS20 can reach a maximum of 1A.

### Fast Charging Mode

- In fast charging mode, no more than six cradles can be powered off of one power supply unit (p/n PWR-BGA12V108W0WW) using power cable CBL-DC-394A1-01.
- In fast charging mode, the current draw by each docked PS20 can reach a maximum of 1.5A.

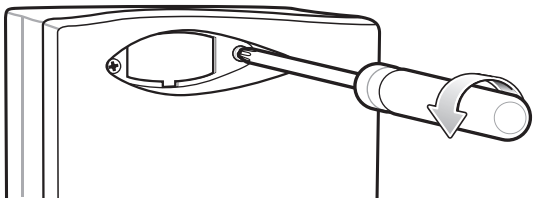
## Mounting the Single Slot Cradle on a Dispenser Wall

The cradle contains two mounting holes in the back housing so that it can be hanged on screws fixed to a supporting furniture. In addition, it comes with plugs and a variety of cable routing outlets. Figure 94 on page 136 provides the necessary information about the location and dimensions of the mounting holes of the cradle.

To mount the Single Slot Cradle:

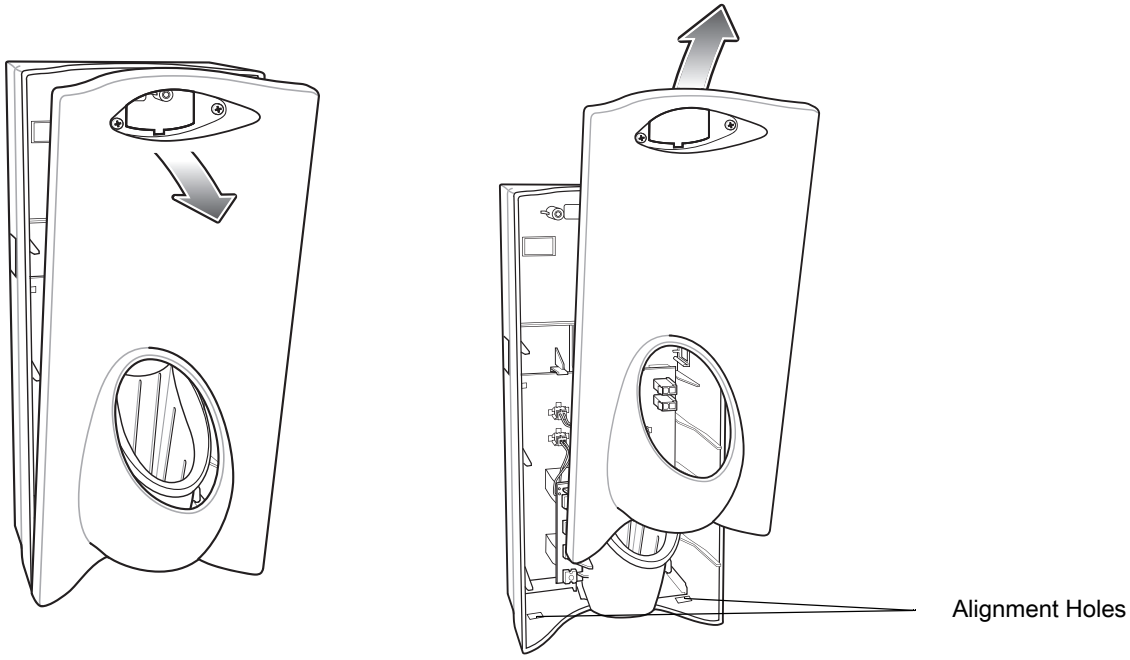
1. Loosen two captive screws securing the front cover to the base.

Figure 92 Remove Screws



2. Pull front cover away from base and then lift out of the base.

Figure 93 Cover Removal




3. Use two screws to hang the cradle on a wall.

Figure 94 Hanging the Cradle on a Wall - Mounting Template

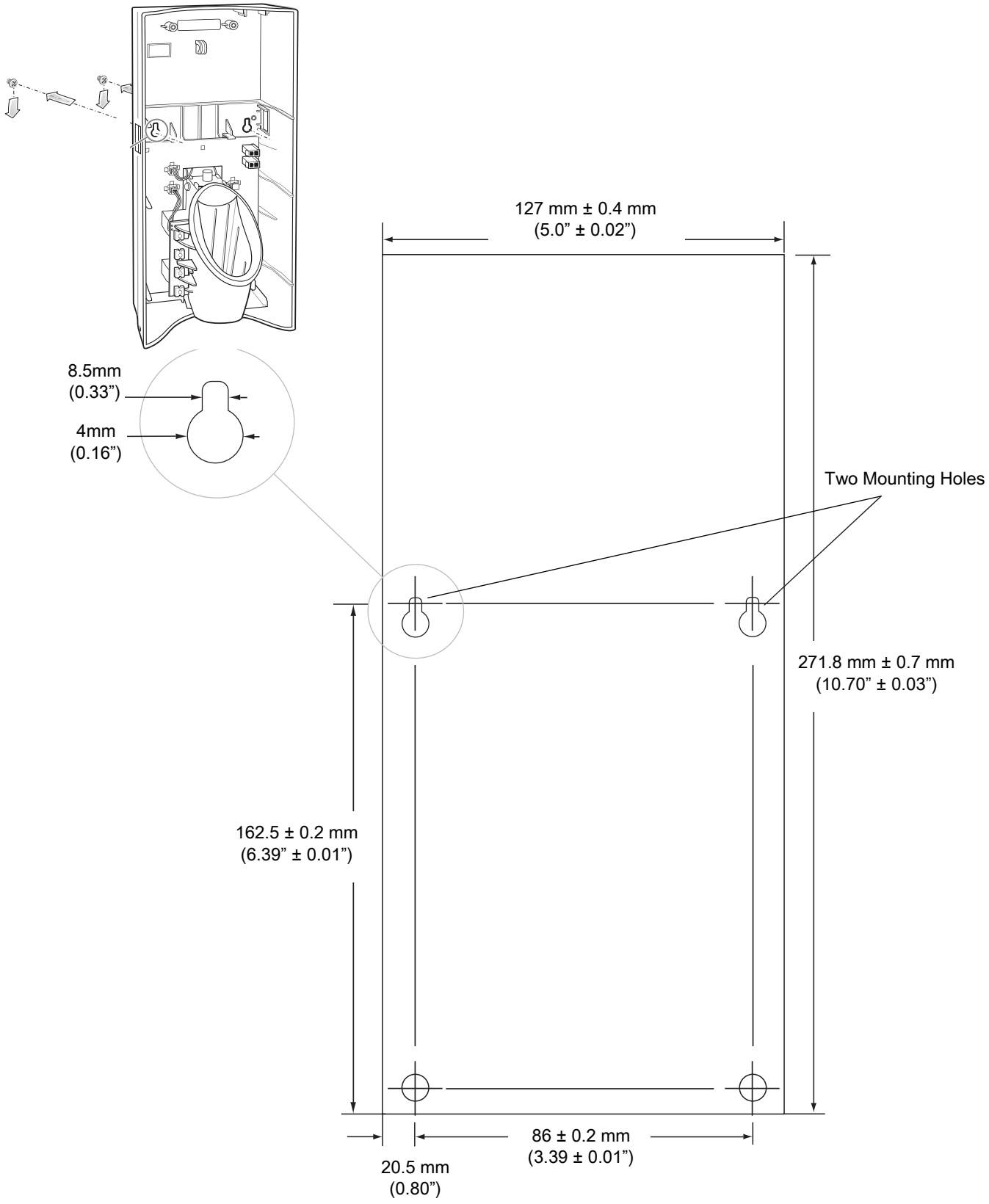
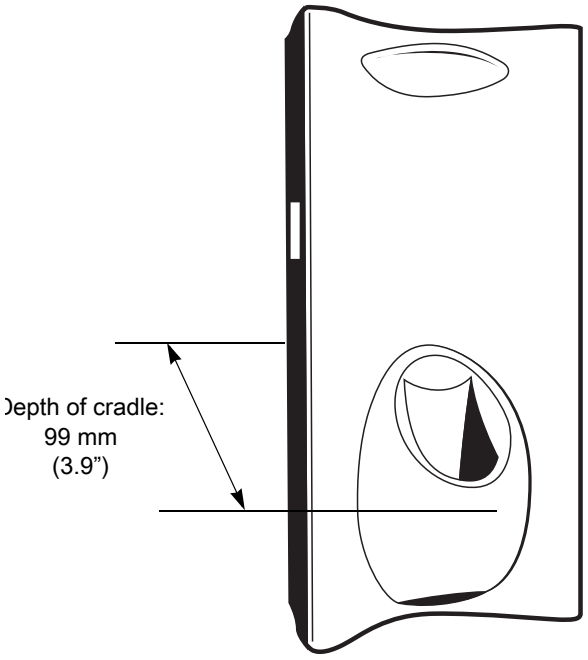


Figure 95 Overall Depth of Cradle

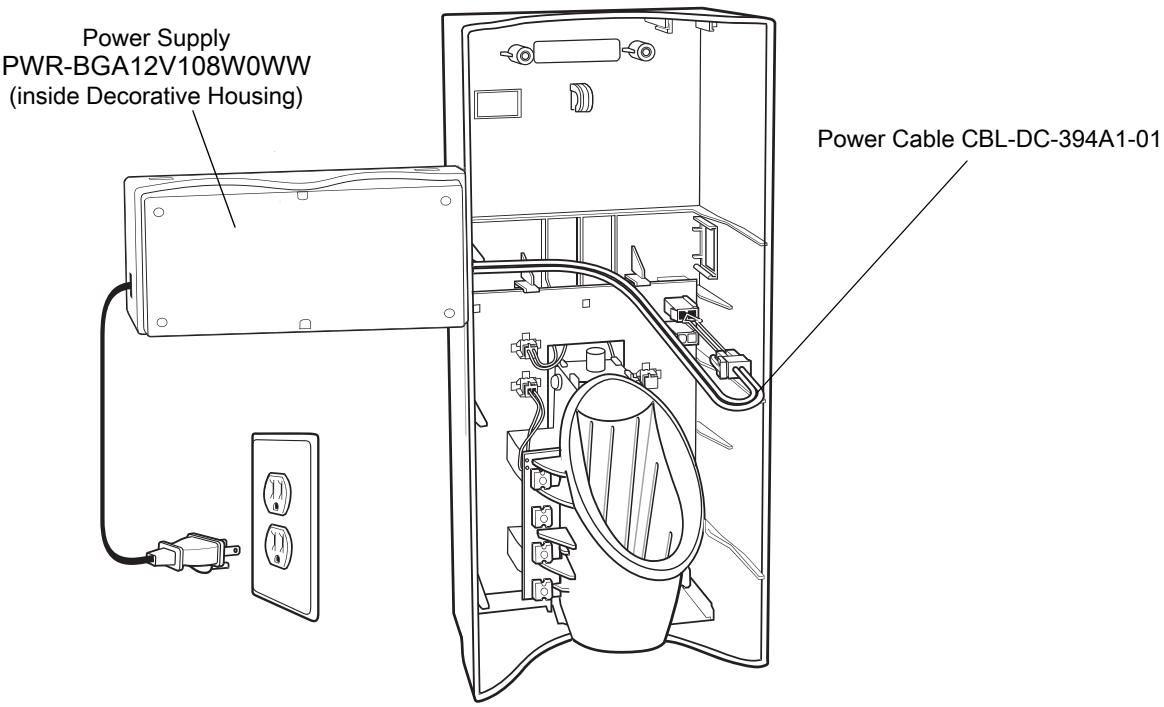



## Wiring

**NOTE:** During installation, ensure all interconnect cables are fully enclosed within the power supply or cradle enclosure.

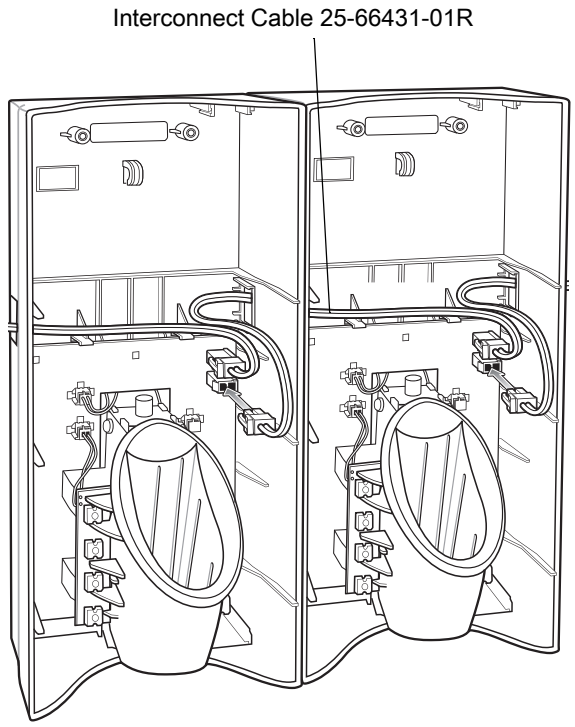
1. Install power supply, including AC line cord and power cable, into Decorative Housing.

Figure 96 Connecting Power Supply



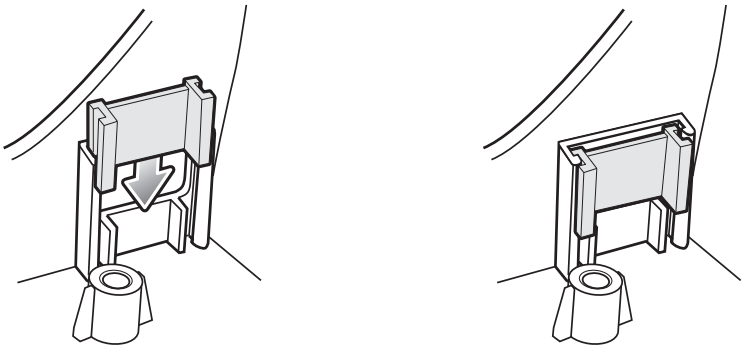
2. Insert power cable through a cable outlet of cradle back housing.
3. Plug connector into power connector on printed circuit board.
4. If more than one cradle is being installed, connect the interconnect cable from the first cradle to the second cradle.

Figure 97 Daisy-Chaining Cradles




5. Use plugs to cover un-used cable outlets.

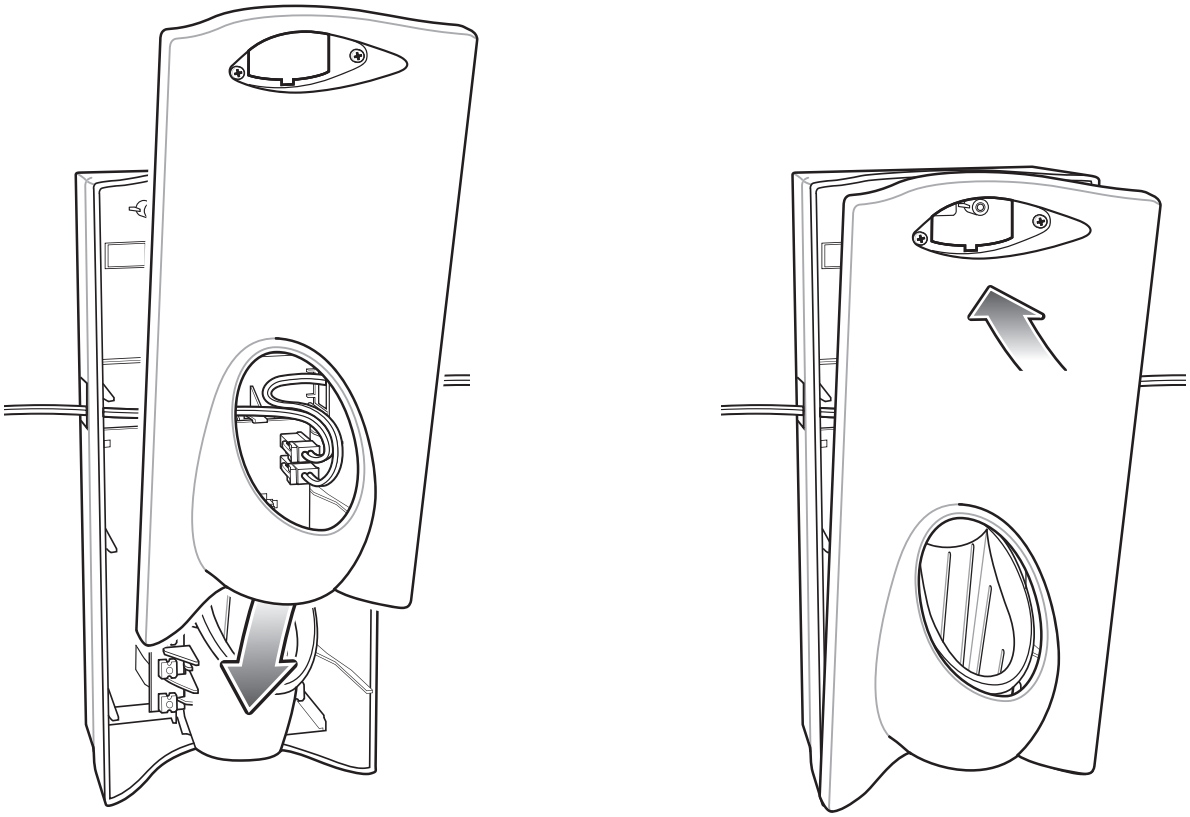
Figure 98 Cable Hole Plug Installation



## Assembly

1. Replace cover.
2. Secure cover with screws.

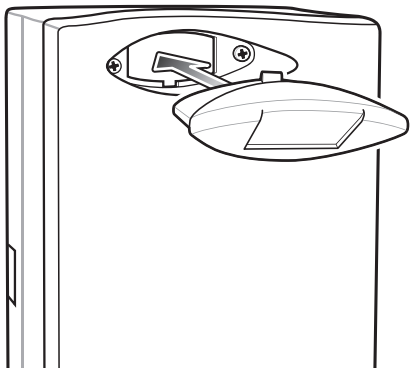
Figure 99 Replace Cover



**NOTE:** Do not install the target cover until you are sure that you do not need to remove the front cover again.

3. Insert bar code target cover.
4. Push target cover into front cover until it snaps into place.

Figure 100 Replace Target Bar Code Cover



## System Cabling

There are some general limitations that must be taken into account when designing a dispenser and ordering hardware elements of a Personal Shopper system:

- No more than six cradles can be powered off each leg of the “Y” power cable.
- A power supply cable runs from the power supply to one or two cradles.

- Cradle interconnection cables run between each successive cradle in the chain.
- The power supply is air cooled, and as such expects some circulation of fresh air around it. Do not enclose it in a small airtight location.
- Power supplies must be mounted in their natural, landscape orientation. They contain fans and their vents must allow for the free flow of air.
- Power supplies should be mounted either above or below dispensers and entrance heads. Mounting of power supplies to the right or left is not preferred.
- When laying out your furniture and cabling plan, routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules. A set of labels, numbered 1 to 12, is part of each power supply unit. These labels are to be used to track the number of loads on a particular supply. Each label is designed to be attached to the cradle interconnection cable when a cradle is added to the daisy chain. When all labels are used, the supply is fully loaded.

Figure 101 on page 140 shows how the maximum number of cradles can be cabled to a power supply using power cable CBL-DC-394A1-01.

Figure 102 on page 141 shows how the maximum number of cradles can be cabled to a power supply using the “Y” power cable CBL-DC-392A1-02. Note that there are only six cradles per leg of the power supply cable, and only 12 cradles in total.

Figure 101 Maximum Number of Charge Cradles per Power Supply

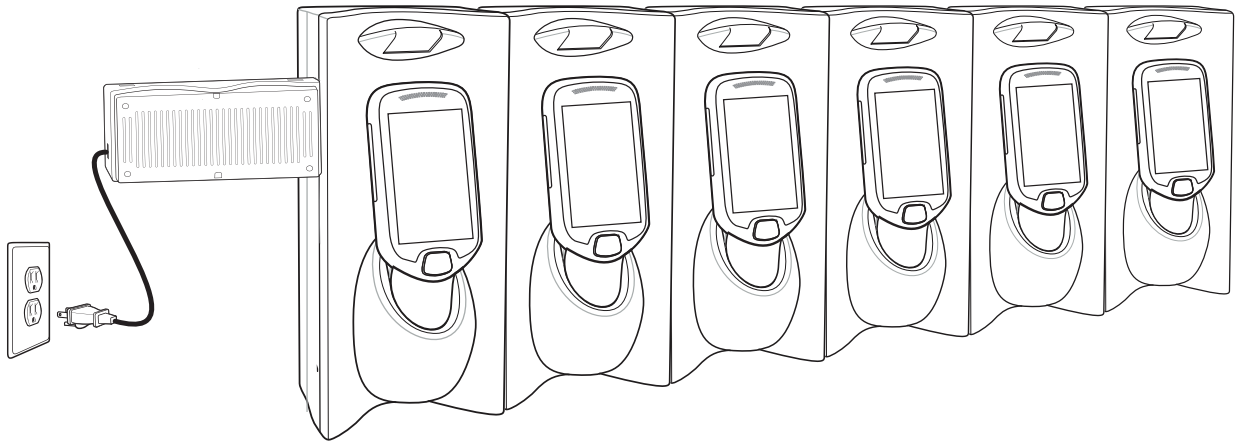
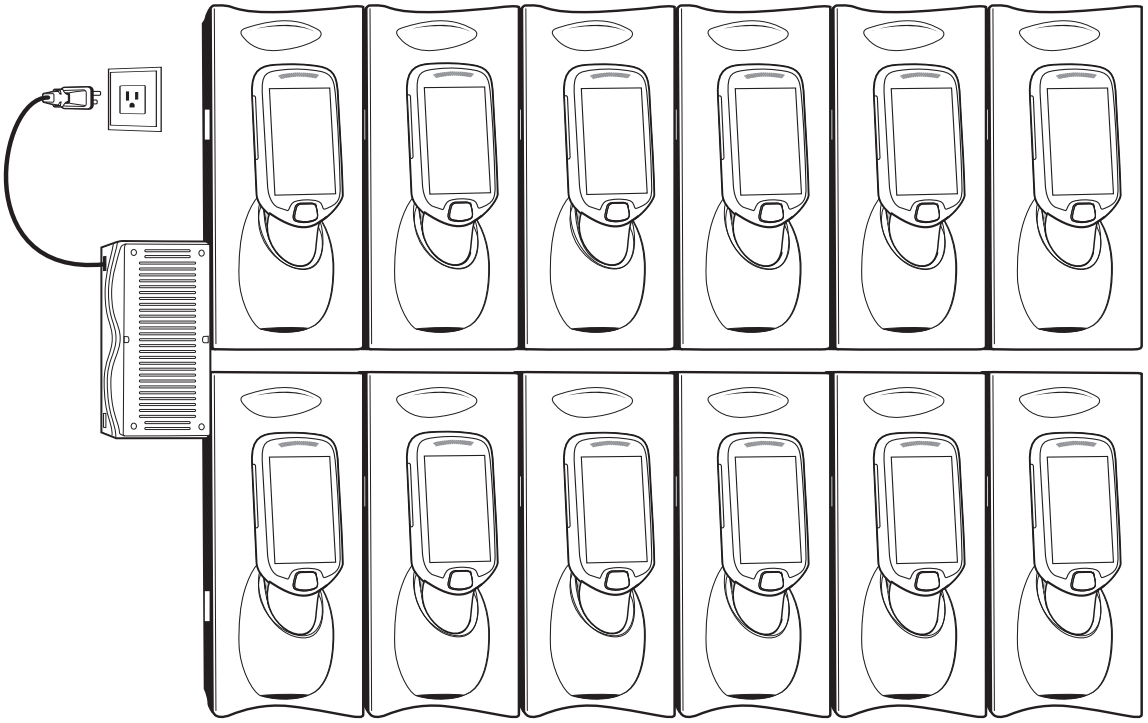


Figure 102 Maximum Number of Charge Cradles per Power Supply with “Y” Power Cable



# Installation of the Three Slot Cradle

Installation of the Three Slot Cradle include the following mounting steps:

- Select the mounting configuration (see Mounting Configurations on page 141)
- Select the charging mode (see Charging Modes on page 143)
- Mount the Three Slot Cradles on a dispenser wall (see Mounting the Three Slot Cradle on a Dispenser Wall on page 145)
- Set the cradle(s) (see Controlling the Cradle on page 110)

## Mounting Configurations

Three slot cradles can be installed in the following mounting configurations:

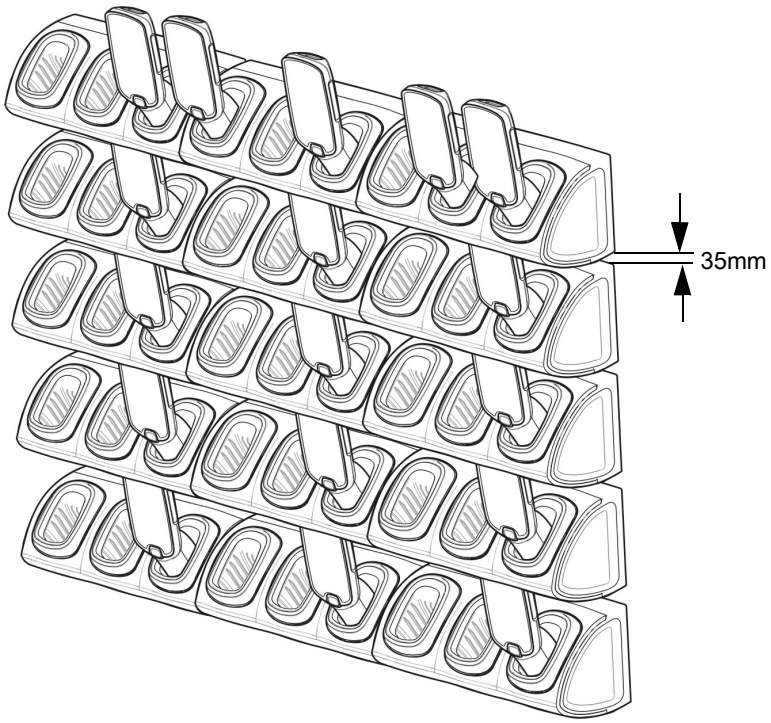
- High Density (HD) configuration - Using HD cradles
- Super High Density (SHD) configuration - Using SHD cradles
- Desktop configuration - Using stand alone cradle(s) on a flat surface

### High Density Configuration

The cradle can be installed in high density configuration so that the display of the PS20 devices are facing the user. In this configuration, cradles are installed with a vertical gap of 35mm between each other.

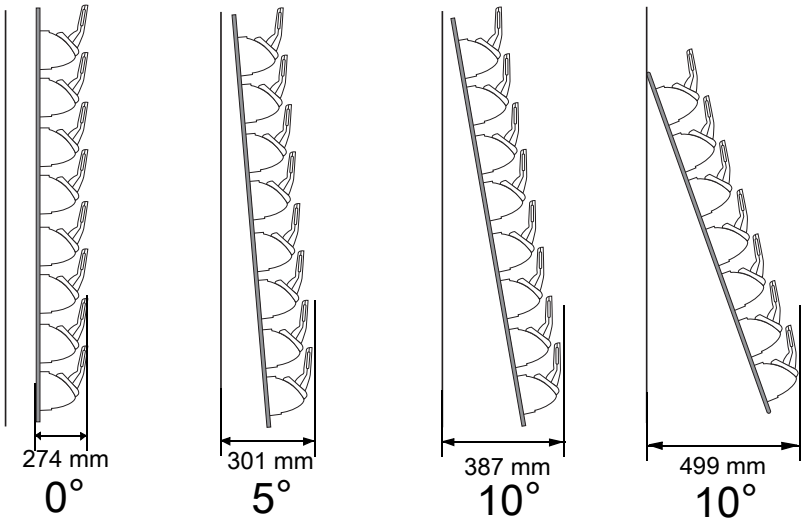
**NOTE:** In high density configuration, the PS20 units have a 10-degree forward-facing tilt that should be taken in consideration, especially if furniture is planned to be placed in front of the dispenser wall.

Figure 103 Installation in High Density Configuration




The installation of the dispenser wall can be designed so that it tilts slightly backward in the following angles:

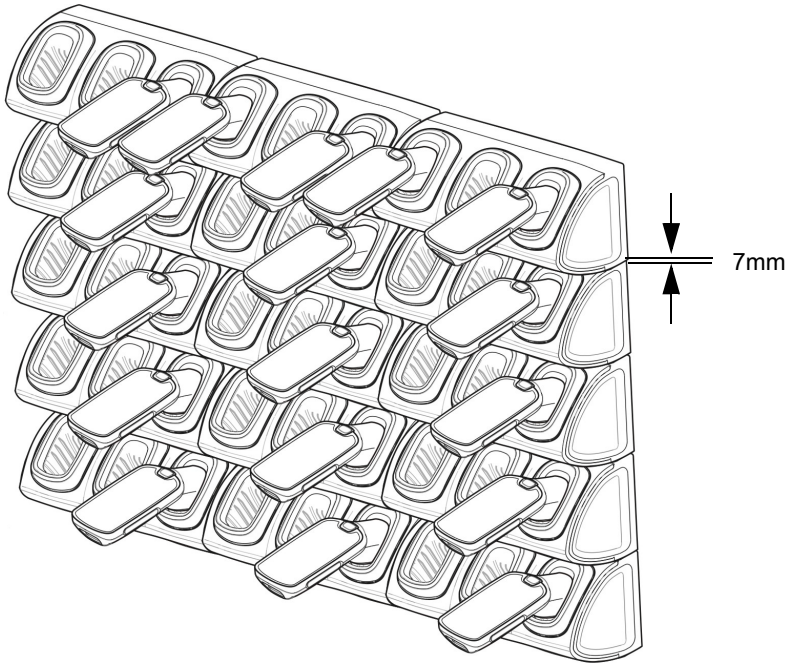
Figure 104 Dispenser Wall Angles




## Super High Density Configuration

The cradle can be installed in super high density configuration so that the display of the PS20 devices are facing up. In such configuration, cradles are installed with a vertical gap of 7mm from each other to allow more cradles per square meter.

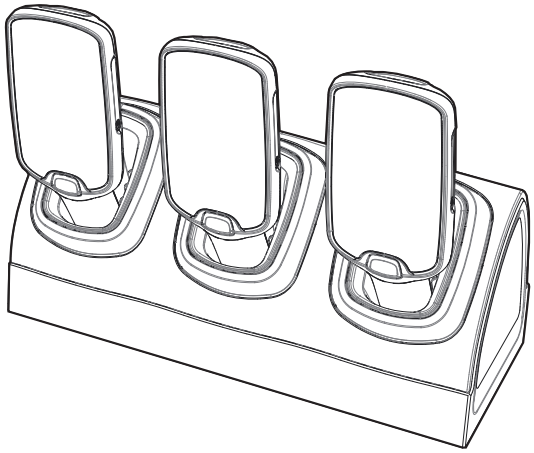
Figure 105 Installation in Super High Density Configuration




### Desktop Configuration

In desktop configuration, the cradle can be placed on a flat tabletop or shelf at checkout or back room locations.

Figure 106 Installation in Desktop Configuration



## Charging Modes

Three Slot Cradles can be installed in the following charging modes:

- Standard charging
- Fast charging

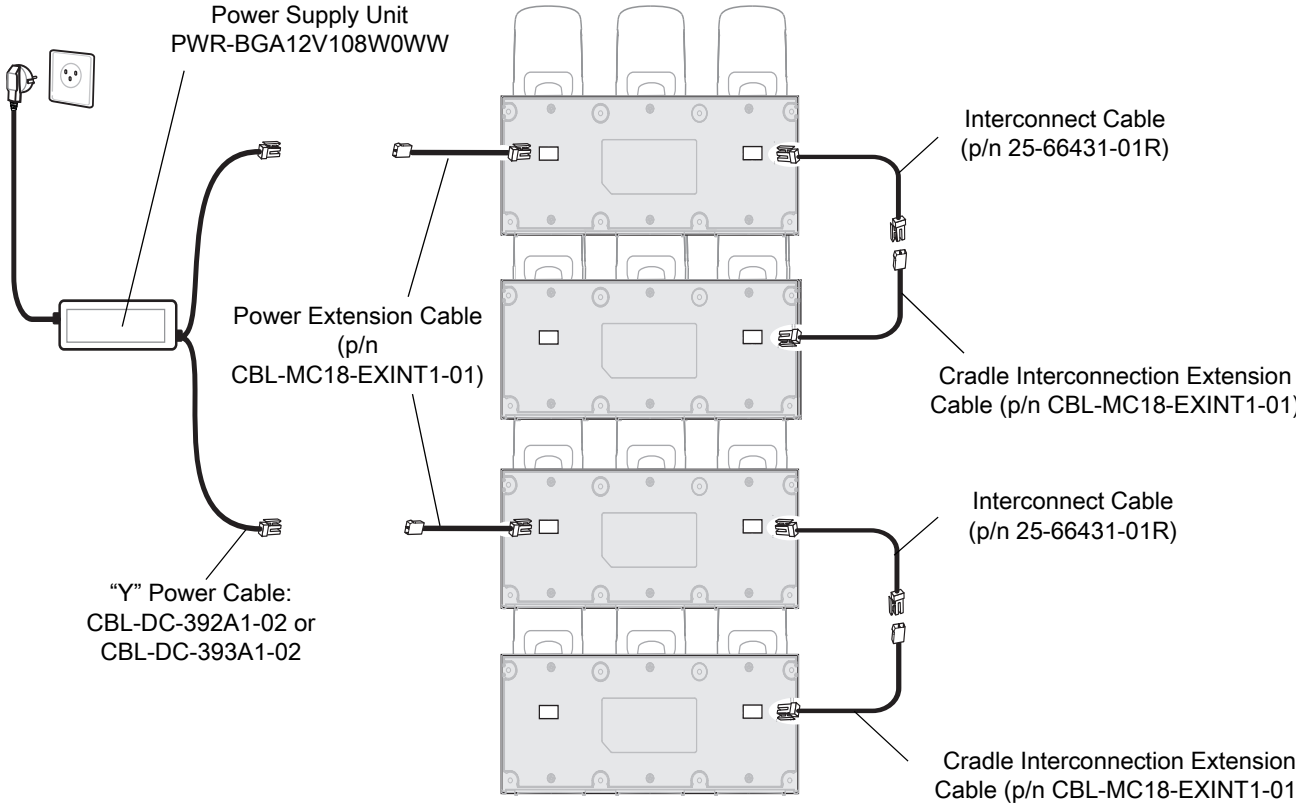
There are some general charging considerations that must be taken into account when designing a dispenser and ordering hardware elements of a system:

## Standard Charging Mode

- In standard charging mode, no more than four cradles can be powered off of one power supply unit (p/n PWR-BGA12V108W0WW) using “Y” power cable (p/n CBL-DC-392A1-02 or p/n CBL-DC-393A1-02), power extension cables (p/n CBL-MC18-EXINT1-01) and interconnect cables (p/n 25-66431-01R).
- In standard charging mode, the current draw by each docked PS20 can reach a maximum of 1A.
- Cable routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules.

Figure  on page 144 shows how the four cradles can be cabled to a power supply unit in standard charging mode.

Figure 107  Standard Charging Mode - Cable Connections

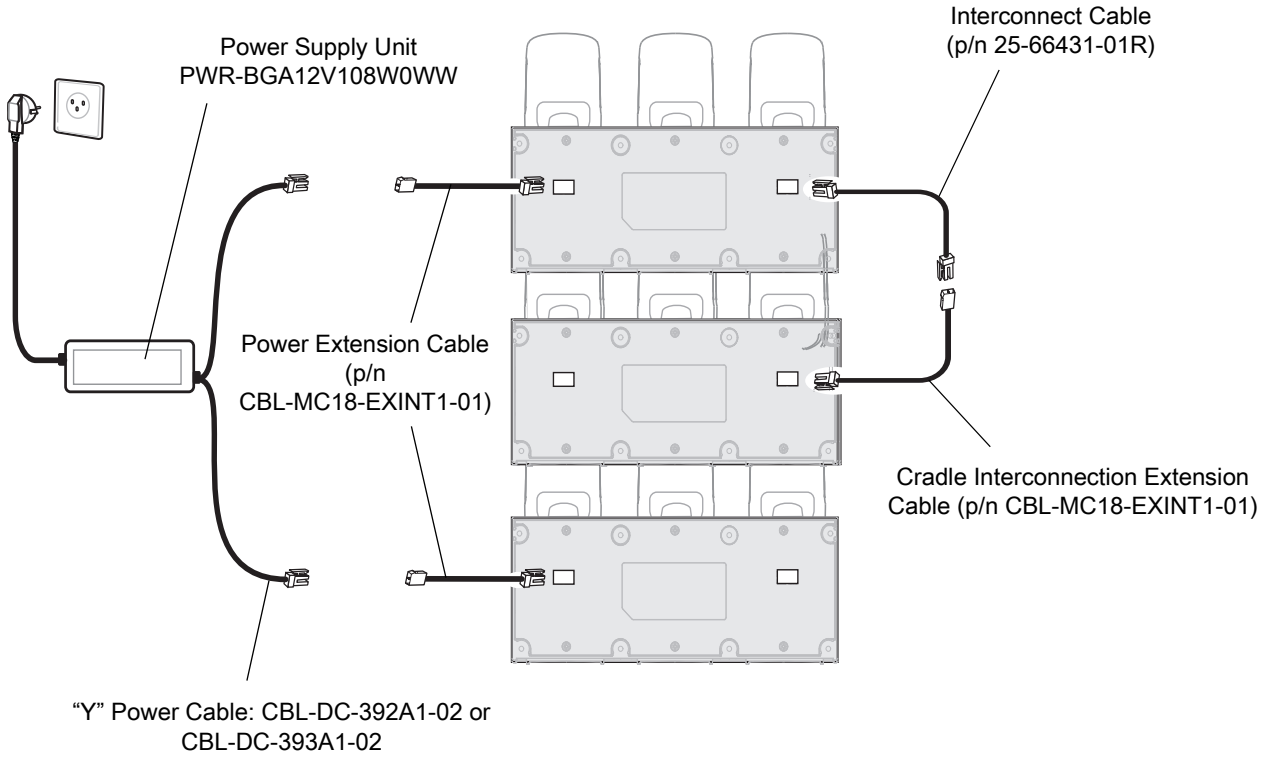



## Fast Charging Mode

- In fast charging mode, no more than three cradles can be powered off of one power supply unit (p/n PWR-BGA12V108W0WW) using “Y” power cable (p/n CBL-DC-392A1-02 or p/n CBL-DC-393A1-02), Interconnect cables (p/n 25-66431-01R) and cradle interconnection extension cables (p/n CBL-MC18-EXINT1-01).
- In fast charging mode, the current draw by each docked PS20 can reach a maximum of 1.5A.
- Cable routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules.

Figure  on page 145 shows how the three cradles can be cabled to a power supply unit in fast charging mode.

Figure 108 Fast Charging Mode Cable Connections




## Mounting the Three Slot Cradle on a Dispenser Wall

The cradle can be bolted to a dispenser wall or any supporting furniture using eight mounting holes. The back cover of the cradle has two access holes for routing power cables to \ from a power supply unit or adjacent cradle. Figure  on page 146 provides a mounting template for cradle installation.

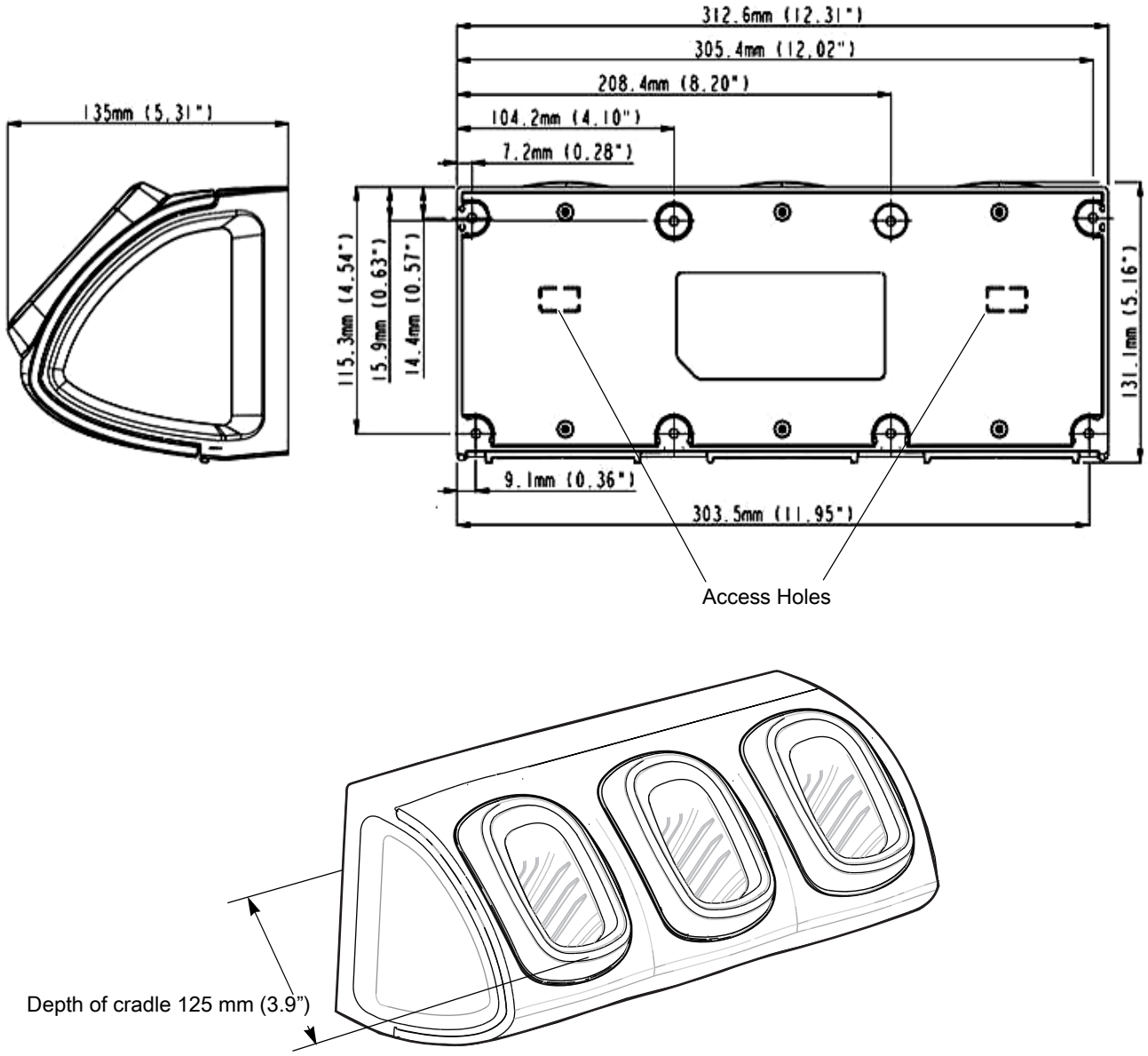
Perform this procedure to mount the cradle on a dispenser wall:

**CAUTION:** DO NOT connect more than four cradles when is standard charging mode or three cradles when in fast charging mode to a single power supply unit.
DO NOT connect the power supply unit to a power outlet until all installation steps are completed.

**NOTE:** The following procedure is an example installation of Three Slot Cradles in fast charging mode - high density configuration.

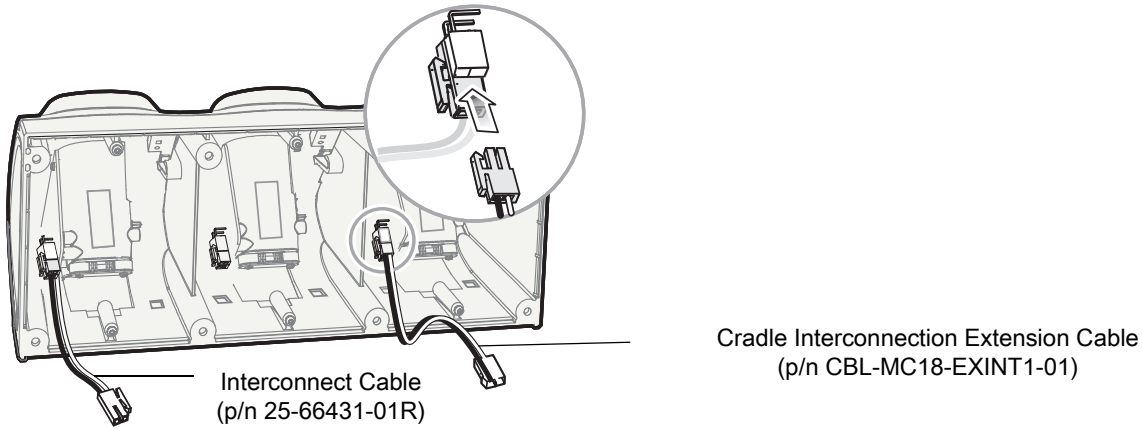
1. Use the wall mount template to plan and mark the screw locations on the dispenser wall.

Figure 109 Three Slot Cradle - Mounting Template and Overall Depth



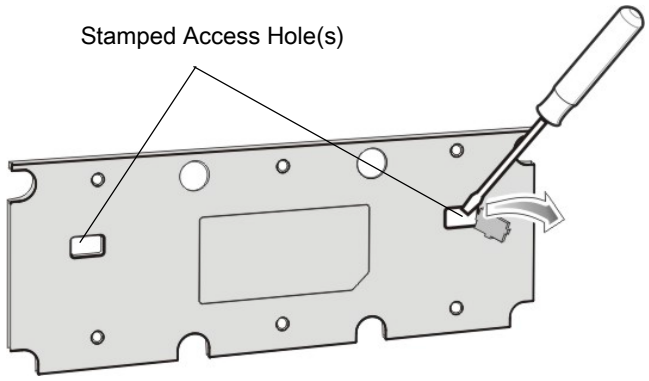

2. In all cradles, plug the power extension cable (p/n CBL-MC18-EXINT1-01) to free the connector on left slot.
3. Plug interconnect cable (p/n 25-66431-01R) to free connector on right slot.

Figure 110 Three Slot Cradle - Cable Connections



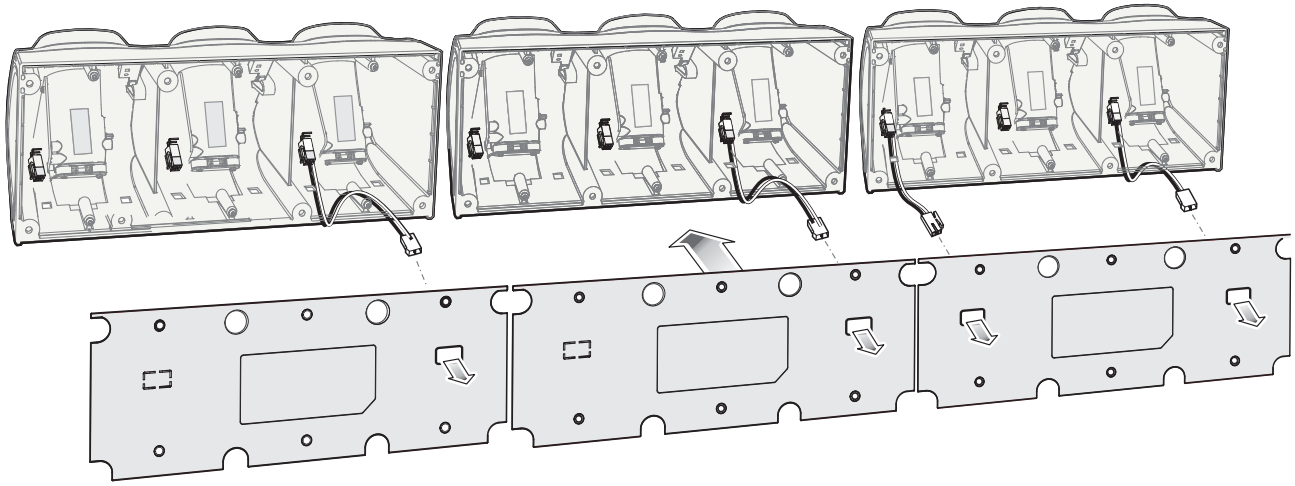

4. On all the back covers, knock-out the stamped access hole(s).

Figure 111 Three Slot Cradle - Stamped Access Hole(s)



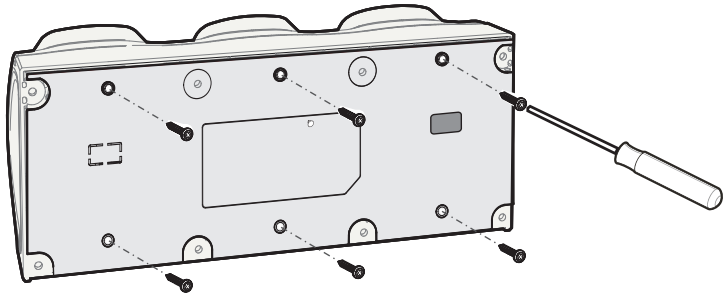

5. Route interconnect cables through access holes in back covers.

Figure 112 Three Slot Cradle - Back Cover Cable Routes



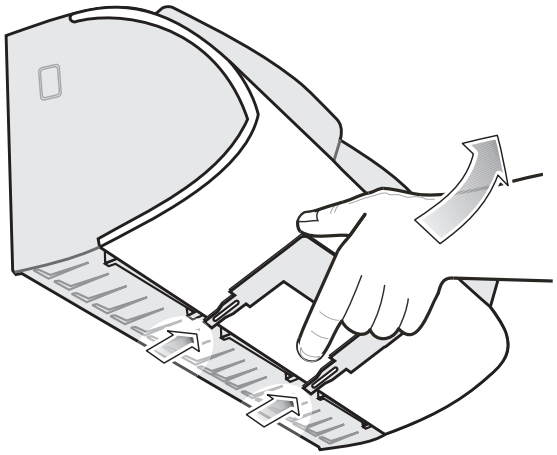
6. Secure the back cover of each cradle using six T10 Torx screws (supplied). Torque screws to 6 Kgf-cm (5.2 in-lb).

Figure 113 Three Slot Cradle - Securing the Back Cover



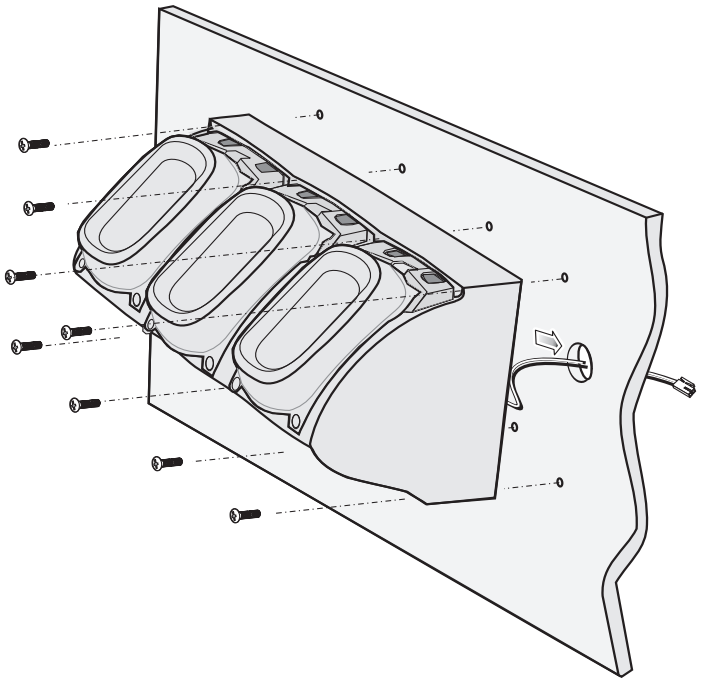
7. Insert the front cover removal tool into two slots, lever upwards and pull to remove front cover from cradle.

Figure 114 Three Slot Cradle - Removing Front Cover



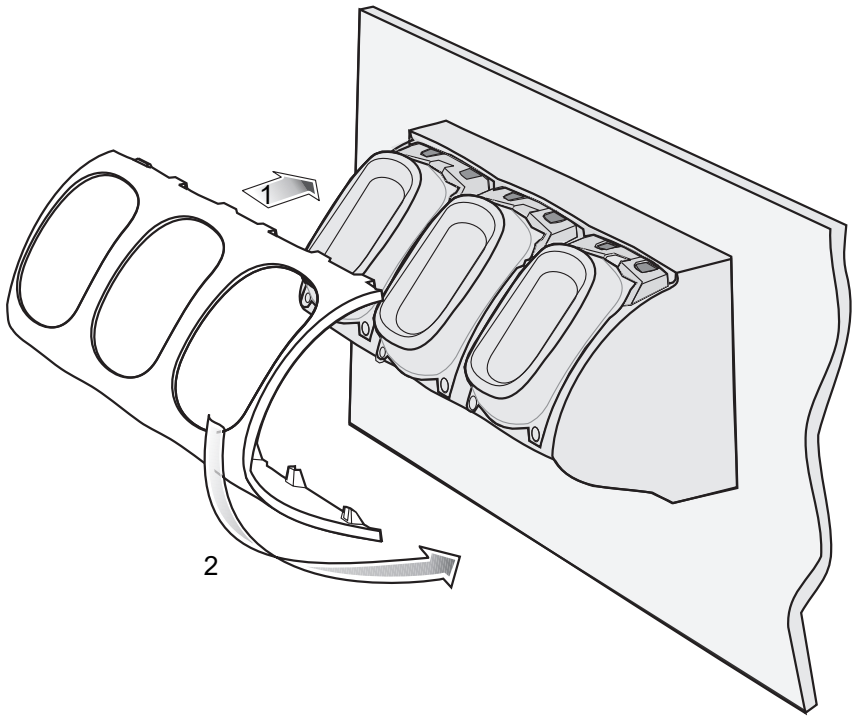
8. Position the cradle on the dispenser wall and route all interconnect cables through the access holes in the dispenser wall.
9. Fasten the cradle to the wall using eight screws (not supplied). Make sure to use additional wall mounting hardware, as needed, for safe mounting, according to the wall type.

Figure 115 Three Slot Cradle - Fastening the Cradle to a Wall



10. Insert tabs on upper side of front cover into slots on cradle and rotate cover down until it snaps into place.

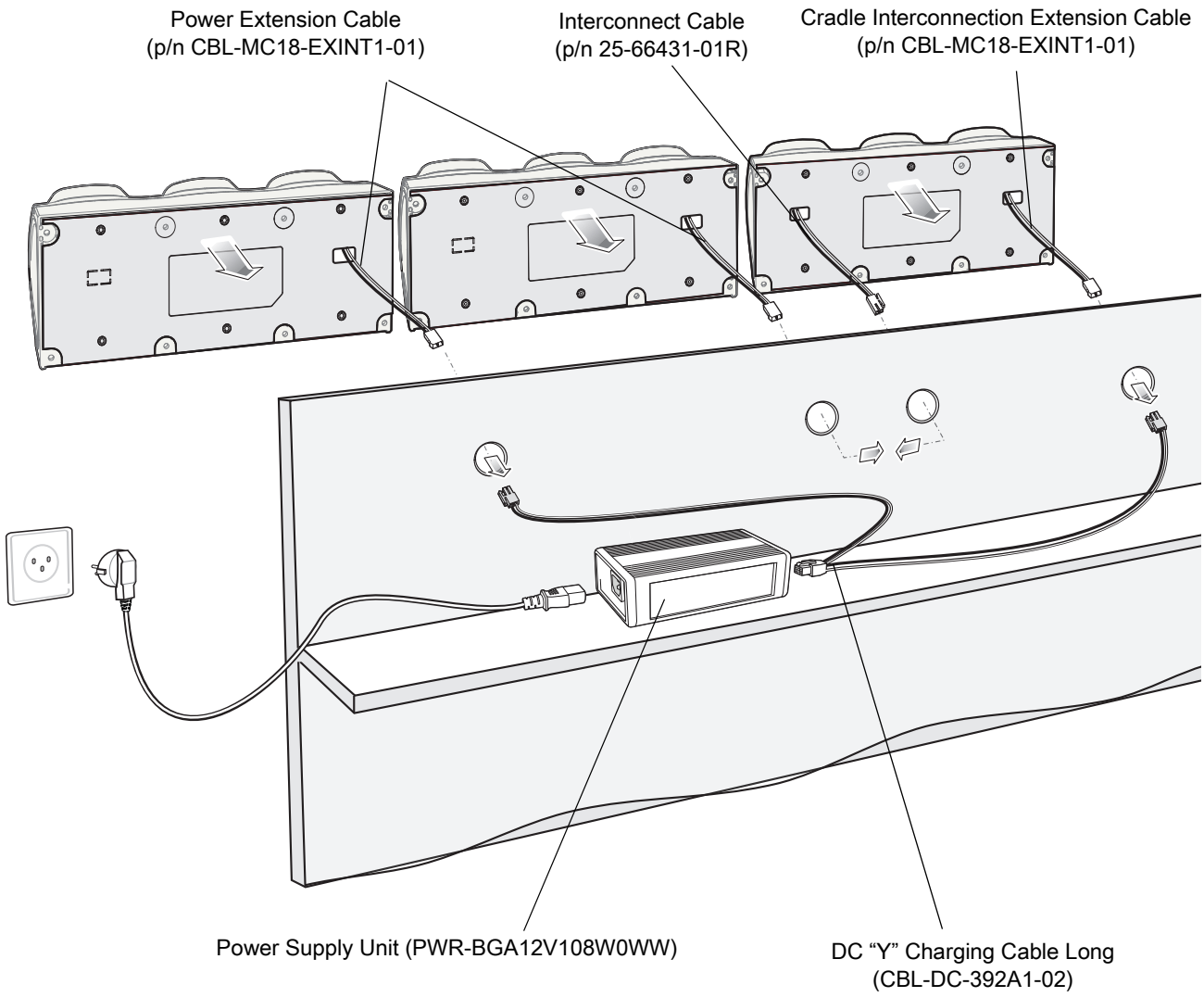
Figure 116 Three Slot Cradle - Connecting the Front Cover




11. Plug Power Extension Cable (p/n CBL-MC18-EXINT1-01) to interconnect cable (p/n 25-66431-01R).
12. Plug “Y” cable (CBL-DC-392A1-02) to Interconnect cables (p/n 25-66431-01R).
13. Plug “Y” cable (CBL-DC-392A1-02) to power supply unit.

14. Secure power supply unit (p/n PWR-BGA12V108W0WW) to the back of the dispenser wall.
15. Connect the power cord to the power supply unit and to a 110/220 VAC outlet.

Figure 117 Three Slot Cradle - Connection to Power Supply Unit




16. Place the socket onto the cradle and secure the four screws.
17. Place the socket cover onto the cradle and secure the two screws.

# 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.

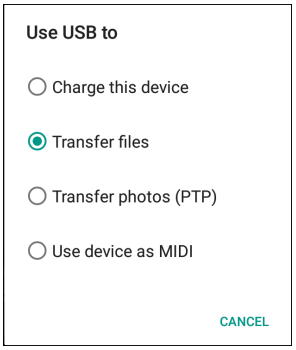
When connecting the device to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

### Transferring Files

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

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

Figure 118 Use USB to Dialog Box




3. Touch **Transfer files**.

**NOTE:** After you change the setting to **Transfer files**, and then disconnect the USB cable, the setting reverts back to **Charge this device**. If the USB cable is reconnected, select **Transfer files** again.

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.

## 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.

## Accessing DataWedge

To access DataWedge:

1. Swipe up from the bottom of the Home screen and touch  .

## Basic Scanning

Scanning can be performed using the following:

- Imager

## 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.

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.

**IMPORTANT:** To avoid the unnecessary use of enable/disable scanner API calls, Zebra recommends that apps register to be notified of changes in scanner status (using the SCANNER_STATUS parameter of the REGISTER_FOR_NOTIFICATION API). This enables apps to receive scanner status changes immediately rather than having to query and wait for the result. Status-change notifications include the active Profile name, which permits an app to use the enable/disable scanner API calls only when status changes effect a relevant Profile.

## 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.

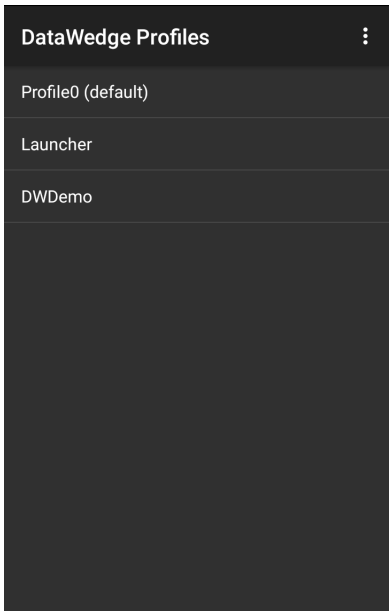
## Profiles Screen

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

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

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

**Figure 119** DataWedge Profiles Screen



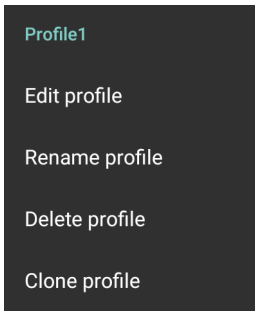

Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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 120 Profile Context Menu

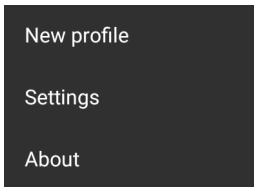



The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

## Options Menu

Touch ⋮ to open the options menu.

Figure 121 DataWedge Options Menu




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

## Disabling DataWedge

1. Swipe up from the bottom of the screen and touch .
2. Touch ⋮.
3. Touch **Settings**.
4. Touch **DataWedge enabled**.

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

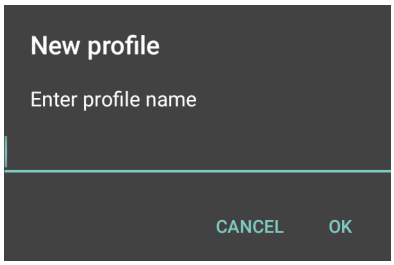
# Creating a New Profile

To create a new profile:

1. Swipe up from the bottom of the screen and touch .
2. Touch ⋮.

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

Figure 122 New Profile Name Dialog Box



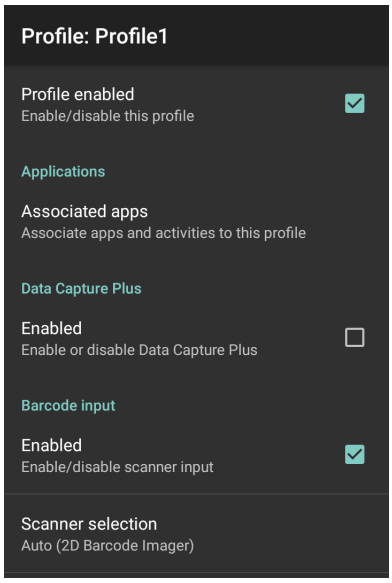

5. Touch **OK**.

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

# Profile Configuration

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

Figure 123 Profile Configuration Screen




The configuration screen lists the following sections:

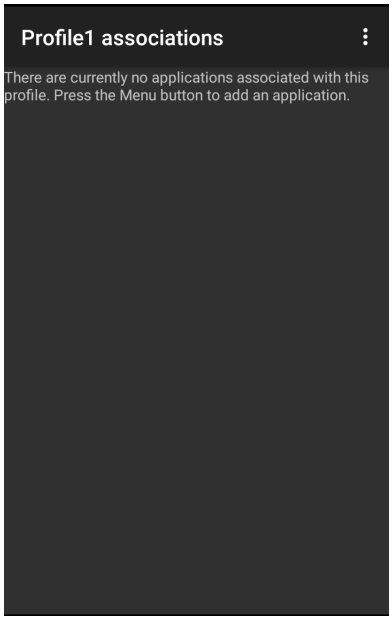
- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode Input
- Keystroke output
- Intent Output
- IP Output.

## Associating Applications

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

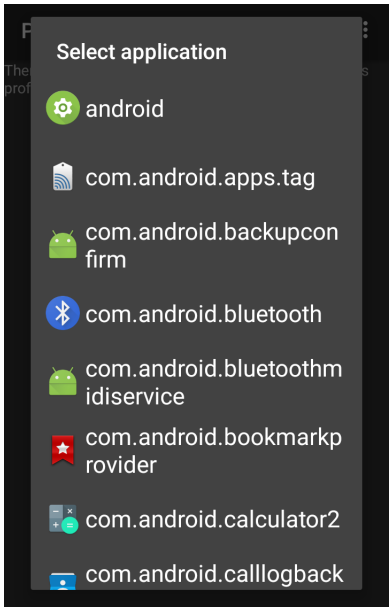
1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.

**Figure 124** Associated Apps Screen



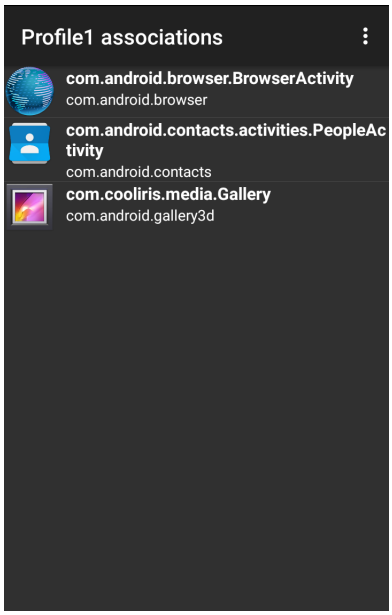

2. Touch ⋮.
3. Touch **New app/activity**.

**Figure 125** 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 ◁.

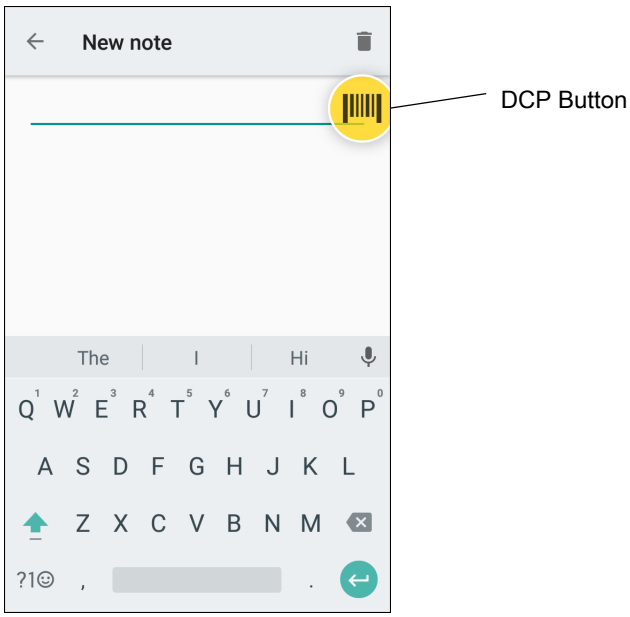
**Figure 126** Selected Application/Activity




# Data Capture Plus

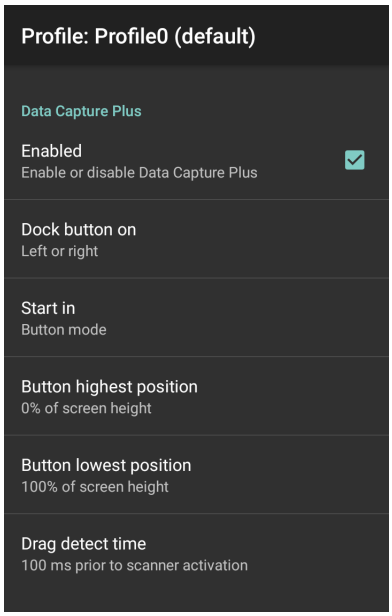
Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching a designated part of the screen. A variable screen overlay acts like a scan button.

Figure 127 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 128 Data Capture Panel Settings



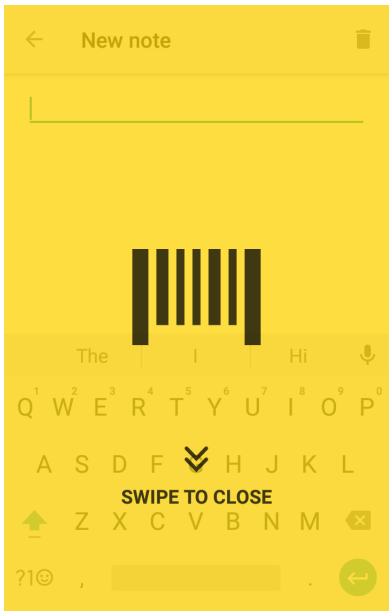

- Enable - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
  - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
  - **Left only** - Places the button on left edge of the screen.
  - **Right 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 129 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.

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

### 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.

For Bluetooth scanners, if the device was not previously paired, a pairing barcode displays prior to automatic connection.

- **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
- Multibarcode params
- Keep enabled on suspend

## Select Scanner to Set Parameters

Select a scanner from the available options to set the parameters for or select **All Scanners**.

## 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 18 Supported Decoders*

| Decoders | Internal Imager SE2100 | Internal Imager SE4710 | DS2278 | LI3678 |
|---|---|---|---|---|
| Australian Postal | O | O | O | -- |
| Aztec | 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 | -- |
| Composite C | O | O | O | -- |
| Discrete 2 of 5 | O | O | O | O |
| Datamatrix | X | X | X | -- |
| Dutch Postal | O | O | O | -- |
| DotCode | O | O | O | O |
| EAN13 | X | X | X | X |
| EAN8 | X | X | X | X |

*Table 18 Supported Decoders (Continued)*

| Decoders | Internal Imager SE2100 | Internal Imager SE4710 | DS2278 | LI3678 |
|---|---|---|---|---|
| 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 |
| Japanese Postal | 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 | -- |
| MicroPDF | O | O | O | -- |
| MicroQR | O | O | O | -- |
| MSI | O | O | O | O |
| PDF417 | X | X | X | -- |
| QR Code | 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 | -- |
| UPCA | X | X | X | X |
| UPCE0 | X | X | X | X |
| UPCE1 | O | O | O | O |
| US4state | O | O | O | -- |

*Table 18 Supported Decoders (Continued)*

| Decoders | Internal Imager SE2100 | Internal Imager SE4710 | DS2278 | LI3678 |
|---|---|---|---|---|
| US4state FICS | O | O | O | -- |
| US Planet | O | O | O | -- |
| US Postnet | 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.

### 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 FCN4** - 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).

**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**

- **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.
- **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).

**Trioptic 39**

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

**UK Postal**

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

**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 is interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
  - **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
  - **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded. (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.
- **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.
- **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.
- **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 **Multibarcode params** 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).
- **Decode Screen Notification** - Select to enable the display of a one second translucent green screen overlay as a notification for each successful decode. Default - disabled.

**NOTE:** For **Decode Screen Notification** to work, **Display over other apps** permission must be granted for the application.

- **Decode Screen Notification Timer** - Set the amount of time (in milliseconds) that the green decode screen stays lit (500 - 1500). (default - 1000).
- **Decode Screen Translucency Level** - Set the level of translucency for the green decode screen (20 - 50). (default - 35).
- **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** - Set the good decode beep to the ringer sound.
- **Music and Media** - Set the good decode beep to the media sound.
- **Alarms** - Set the good decode beep to the alarm sound.
- **Notifications** - Set the good decode beep to the notification sound (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).

### Multibarcode 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).
- **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.

  Editing in the Validation window is not supported if Keystroke Input is enabled in the profile where Voice Input is enabled.
- **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. DataWedge sends captured data via intents, where user applications can consume them in their applications without worrying about the complexities to write code to capture the data.

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, move the focus to the next field.
  - **Line feed** - Line feed character code in a barcode is processed. When DataWedge detects this character code in a barcode, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a barcode is processed. When DataWedge detects this character code in a barcode, move the focus 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 Multbyte characters only to delay only the multibyte characters.
- **Multi byte character display** - Set the amount of time (in milliseconds) of the inter character delay for multi byte characters. (default - 0.)
- **Key event delay** - Set the amount of time (in milliseconds) of the wait time for control characters. (default - 0.)

- **Data formatting and ordering** - Allows formatting and ordering of UDI and Multibarcode 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.
  - **Multibarcode 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.

- **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).
- **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.category.DEFAULT
and the Intent category would be:
android.intent.category.MAIN.

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

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

- String LABEL_TYPE_TAG = "com.symbol.emdk.datawedge.label_type";
  - String contains the label type of the barcode.
- String DATA_STRING_TAG = "com.symbol.emdk.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.emdk.datawedge.decode_data";
  - Decode data is returned as a list of byte arrays. In most cases there will be one byte array per decode. For 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.

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.

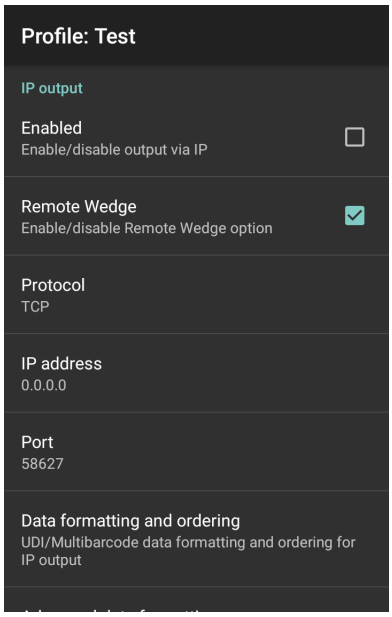
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol 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 Multibarcode 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 130 IP Output Screen




## Using IP Output with IPWedge

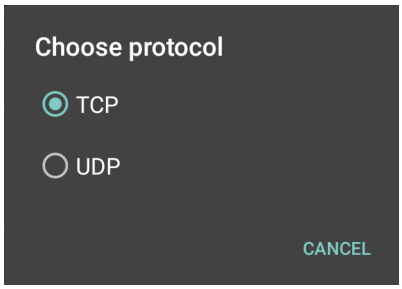
IPWedge is a computer application that can be easily configured to retrieve data sent over network by DataWedge IP Output. Refer to the IPWedge User Manual on how to install and configure in a host computer. To enable IP Output to send captured data to a remote computer that is installed with IPWedge:

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

   A check appears in the checkbox.

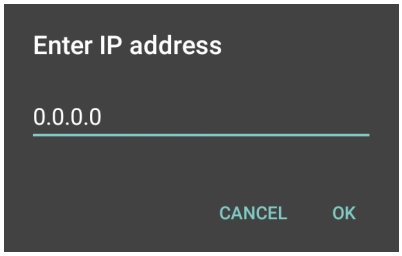
2. Ensure **Remote Wedge** option is enabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).

Figure 131 Protocol Selection



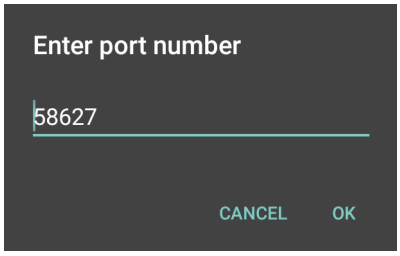

5. Touch **IP Address**.
6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

Figure 132 IP Address Entry




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

Figure 133 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.

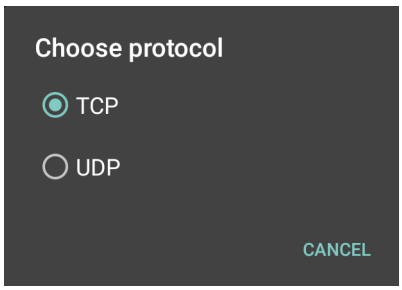
## Using IP Output without IPWedge

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).

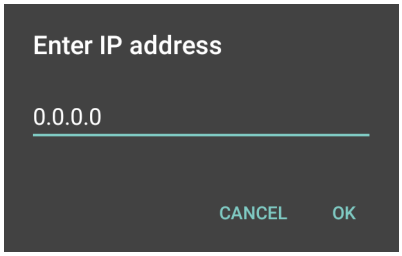
Figure 134 Protocol Selection




5. Touch **IP Address**.

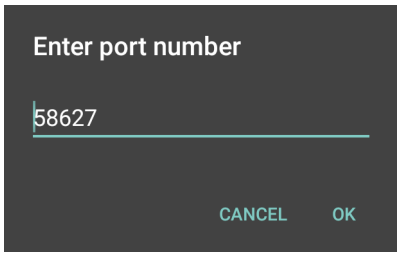
6. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.

Figure 135 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 136 Port Number Entry




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

### Generating Advanced Data Formatting Rules

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

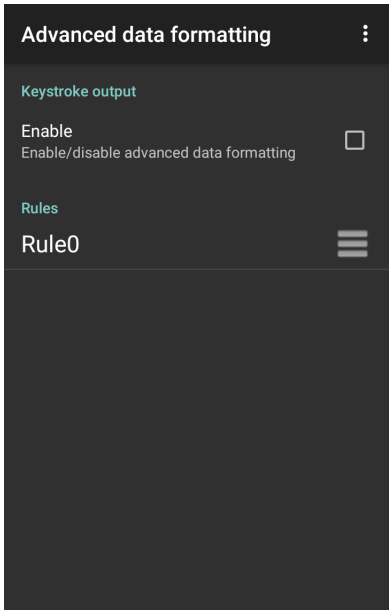
- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.
- Criteria - Criteria can be set according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

## Configuring ADF Plug-in

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

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

Figure 137 Advanced Data Formatting Screen




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

## Creating a Rule

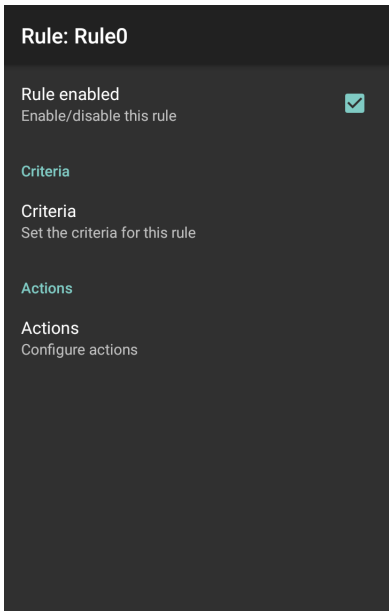
**NOTE:** By default, **Rule0**, is the only rule in the Rules list.

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

### Defining a Rule

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

Figure 138 Rule List Screen

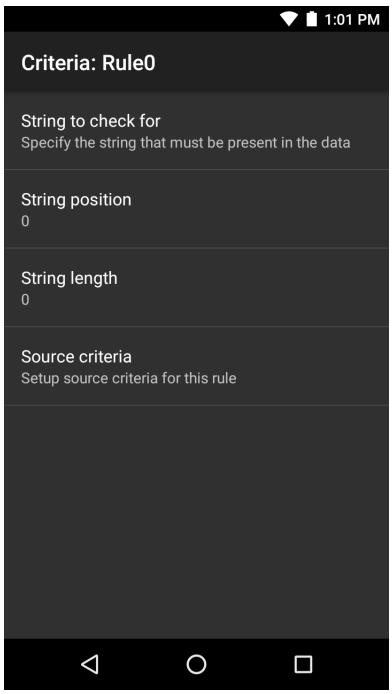



2. Touch the **Rule enabled** check box to enable the current rule.

## Defining Criteria

1. Touch **Criteria**.

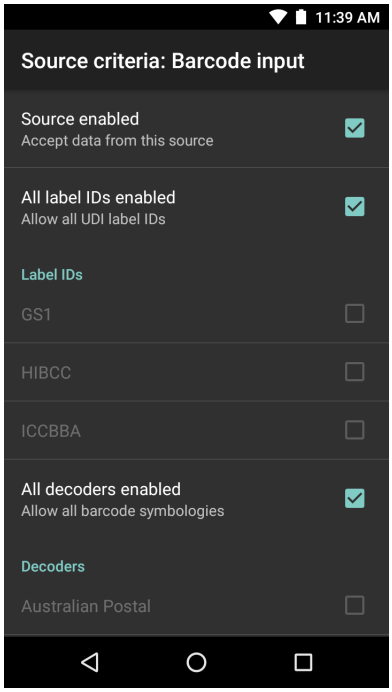
Figure 139 Criteria Screen




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 140 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 19 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 19 ADF Supported Actions (Continued)*

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

## Deleting an Action

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

## ADF Example

The following illustrates an example of creating Advanced Data Formatting:

When a user scans a barcode with the following criteria:

- Code 39 barcode.
- length of 12 characters.

- contains 129 at the start position.

Modify the data as follows:

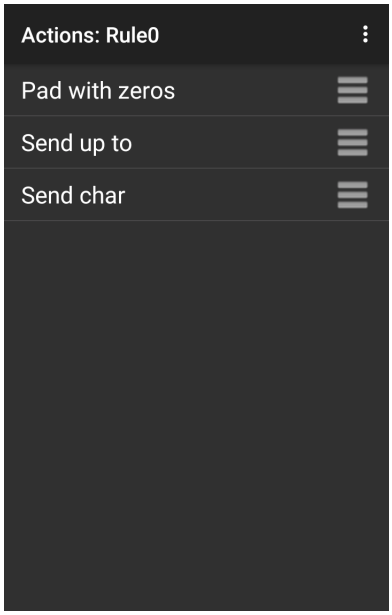
- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

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**.

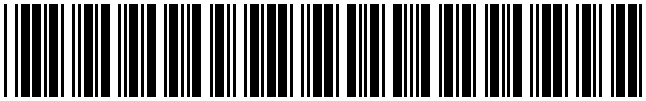
28. Change value to 8 and then touch **OK**.
29. Press ◁.
30. Touch ⋮.
31. Touch **New action**.
32. Select **Send up to**.
33. Touch **Send up to** rule.
34. Touch **String**.
35. In the **Enter a string** text box, enter X.
36. Touch **OK**.
37. Touch ◁.
38. Touch ⋮.
39. Touch **New action**.
40. Select **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 141 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 142 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.

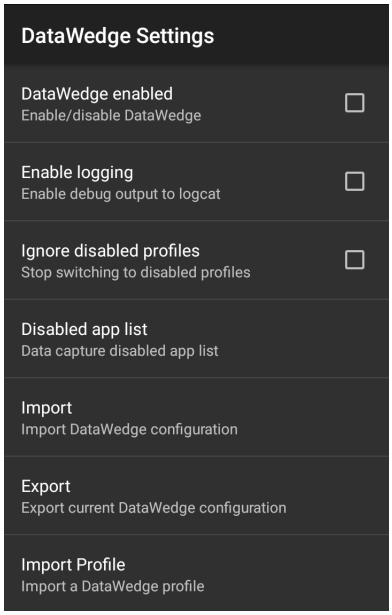
    Scanning a Code 39 barcode of 1299X15598 does not transmit data (rule is ignored) because the barcode data did not meet the length criteria.

Figure 143 Formatted Data


# DataWedge Settings

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

Figure 144 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. Swipe up from the bottom of the screen and touch .
3. Touch .
4. Touch **Settings**.
5. Touch **Import**.
6. Touch **filename to import**.

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

### Exporting a Configuration File

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **Export**.
5. In the **Export to** dialog box, select the location to save the file.
6. Touch **Export**. The configuration file (datawedge.db) is saved to the selected location.

## Importing a Profile File

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

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

## Exporting a Profile

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **Export Profile**.
5. Touch the profile to export.
6. Touch **Export**.
   The profile file (dwprofile_x.db, where x = name of the profile) is saved to the root of the On-device Storage.

## Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Swipe up from the bottom of the screen and touch .
2. Touch .

3. Touch **Settings**.
4. Touch **Restore**.
5. Touch **Yes**.

# Configuration and Profile File Management

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

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

# Enterprise Folder

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

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

## Auto Import

DataWedge supports remote deployment of a configuration to a device, using tools such as 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). When DataWedge launches it checks the folder. If a configuration or profile file is found, it imports the file to replace any existing configuration or profile. Once the file has been imported it is deleted from the folder.

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

**NOTE:** A Factory Reset deletes all files in the **`/enterprise`** folder.

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

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.

## 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.

## Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

## Overriding Trigger Key in an Application

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

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

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

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

## Disable DataWedge on Device and Mass Deploy

To disable DataWedge and deploy onto multiple devices:

1. Swipe up from the bottom of the Home screen and touch **DataWedge**.
2. Touch ⋮.
3. Touch **Settings**.
4. Unselect the **DataWedge enabled** check box.
5. Export the DataWedge configuration. See Exporting a Configuration File on page 195 for instructions. See Configuration and Profile File Management on page 196 for instructions for using the auto import feature.

## 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. For more information, see http://techdocs.zebra.com/datawedge/6-8/guide/api/

## 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.

**IMPORTANT:** To avoid the unnecessary use of enable/disable scanner API calls, Zebra recommends that apps register to be notified of changes in scanner status (using the SCANNER_STATUS parameter of the REGISTER_FOR_NOTIFICATION API). This enables apps to receive scanner status changes immediately rather than having to query and wait for the result. Status-change notifications include the active Profile name, which permits an app to use the enable/disable scanner API calls only when status changes effect a relevant Profile.

### Function Prototype

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

### Parameters

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

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

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

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

## Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, 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.this.sendBroadcast(i);
}
```

## Comments

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

**NOTE:** Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile. The above assumes that ProfileA is not associated with any applications/activities, therefore when focus switches back to activity A, DataWedge will not automatically switch to ProfileA therefore activity A must switch back to ProfileA in its onResume method. Because DataWedge will automatically switch Profile when an activity is paused, it is recommended that this API function be called from the onResume method of the activity.

# Enumerate Scanners

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

## Function Prototype

```
Intent i = new Intent();
i.setAction("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 a broadcast Intent. The broadcast Intent action is "com.symbol.datawedge.api.ACTION_ENUMERATEDSCANNERLIST" and the list of scanners is returned as a string array (see the example below).

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

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

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

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

## 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 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, parameters and failures, for example, Profile not found or associated with an application.

### Example

```
::javascript
// 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 will set the DataWedge Profile accordingly either to the default Profile or to an associated Profile.

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

## Function Prototype

```
Intent i = new Intent();
i.setAction("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 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, 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 will have no effect if the specified Profile does not exist or is already associated with an application.

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

This API function activates such Profiles.

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

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

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

## Notes

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

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

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

DataWedge auto Profile switching works as follows:

Every second…

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

# 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.

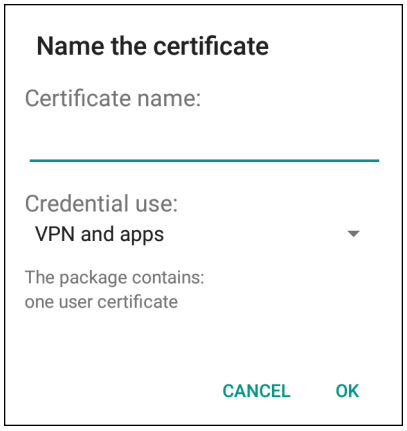
## Installing a Secure Certificate

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** > **Advanced** > **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 145** Name the Certificate Dialog Box




10. Touch **OK**.

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

## Android

Android development tools are available at developer.android.com.

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

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

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

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

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

By default, the Developer Options are hidden. To un-hide the developer options, swipe down 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.

## 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.

### MX Features

The following MX features are available in the Configuration Service Provider (CSP) Settings:

- Enable/Disable On Screen Power Button - available in MX 8.3 and later.
- Enable/Disable Navigation Bar - available in MX 7.1 and later.

**On Screen Power Button** - From StageNow, create a profile using the Xpert mode wizard (with MX 8.3 or later) and select UI Manager CSP Settings. Include the requirements to create a barcode and stage the device.

**Navigation Bar** - From StageNow, create a profile using the Xpert mode wizard (with MX 7.1 or later) and select Power Key Manager CSP Settings. Include the requirements to create a barcode and stage the device.

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

#### GMS Restricted

GMS Restricted mode deactivates Google Mobile Services (GMS). All GMS apps are disabled on the device and communication with Google (analytics data collection and location services) is disabled.

Use StageNow to disable or enable GMS Restricted mode. After a device is in GMS Restricted mode, enable and disable individual GMS apps and services using StageNow. To ensure GMS Restricted mode persists after an Enterprise Reset, use the Persist Manager option in StageNow. For more information on StageNow, refer to techdocs.zebra.com.

## ADB USB Setup

To use the ADB, install the USB driver. This assumes that the development SDK has been installed on the host computer. Go to 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. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

## Enabling USB Debugging

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

1. Swipe down 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`**
    **`XXXXXXXXXXXXXXX device`** (where XXXXXXXXXXXXXXX is the device number).

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

13. Touch ◯.

# Application Installation

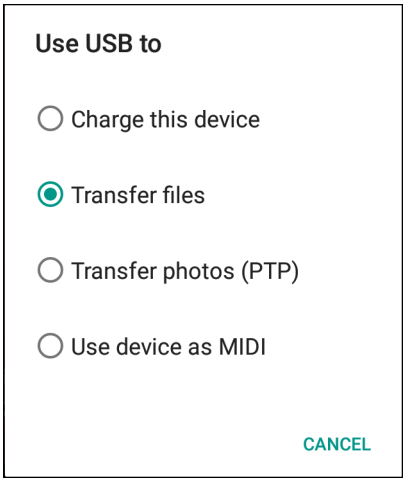
After an application is developed, install the application onto the device using one of the following methods:

- USB connection, see Installing Applications Using the USB Connection.
- 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**.

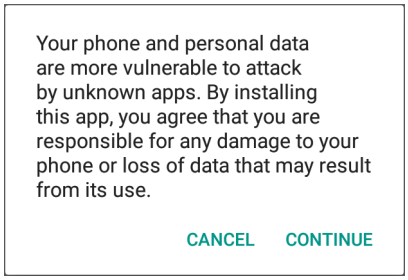
**Figure 146** Use USB Dialog Box




3. Touch **Transfer files**.

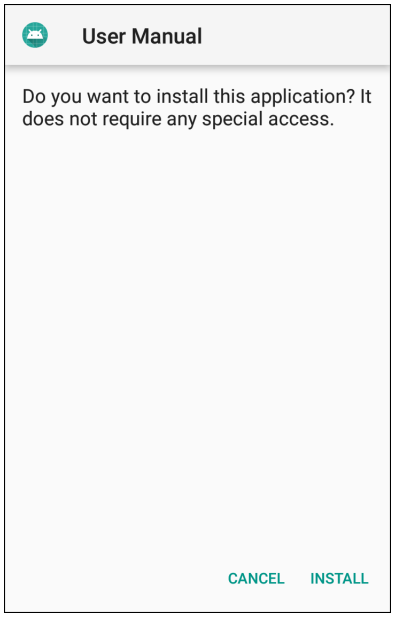
4. On the host computer, open a **Files** application.
5. On the host computer, copy the application .apk file from the host computer to the device.
6. Disconnect the device from the host computer.
7. Swipe the screen up and select to view files on the Internal Storage.
8. Locate the application .apk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

Figure 147 Install App Permission Dialog Box




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

Figure 148 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.

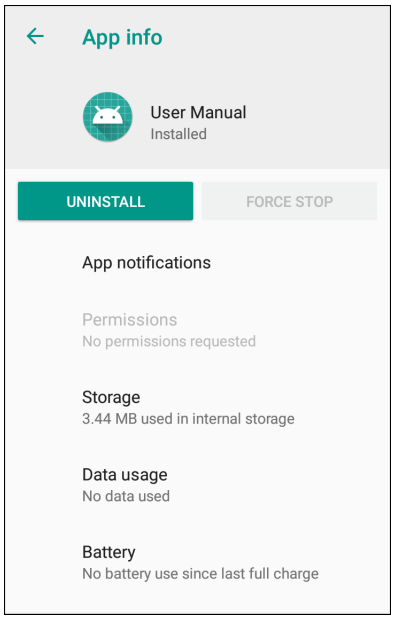
1. Connect the device to a host computer using USB. See USB Communication.
2. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
3. Touch **System** > **Developer options**.
4. Slide the switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check 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 149** 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.
2. Download the appropriate System Update package to a host computer.

## Using ADB

To update the system using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.
2. Connect the cable or cradle to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
4. Touch **System** > **Developer options**.
5. Slide the switch to the **ON** position.
6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and use the adb command:
   `adb devices`
   The following displays:
   `List of devices attached`
   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

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

9. Type:
   `adb reboot recovery`
10. Press Enter. The System Recovery screen appears.
11. Tap the touch panel to advance to the next menu choice and navigate to **apply upgrade from adb**.

**IMPORTANT:** If **Apply downgrade from ADB** is selected, an Enterprise Reset is performed on whatever upgrade or downgrade package is provided.

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.
2. Download the Enterprise Reset file to a host computer.

## Using ADB

To perform an Enterprise Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.
2. Connect the cable or cradle to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
4. Touch **System** > **Developer options**.
5. Slide the switch to the **ON** position.

6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and type:

   `adb devices`.

   The following displays:

   `List of devices attached`

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

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

9. Type:

   `adb reboot recovery`

10. Press Enter. The System Recovery screen appears.
11. Tap the touch panel to advance to the next menu choice and navigate to **apply upgrade from adb**.
12. Press the Scan button.
13. Navigate to **Full OTA Package**.
14. Press the Scan button.
15. On the host computer command prompt window type:

    `adb sideload <file>`

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

16. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.
17. Press the Scan 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.
2. Download the appropriate Factory Reset file to a host computer.

## Using ADB

To perform an Factory Reset using ADB:

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

2. Connect the cable or cradle to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
4. Touch **System** > **Developer options**.
5. Slide the switch to the **ON** position.
6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and use the adb command:
   `adb reboot recovery`
9. Press Enter. The System Recovery screen appears.
10. Tap the touch panel to advance to the next choice and navigate to **apply upgrade from adb**.
11. Press the Scan button.
12. On the host computer, open a command prompt window and use the adb command:
    `adb devices`.
    The following displays:
    `List of devices attached`
    `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

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

13. Type:
    `adb reboot recovery`
14. Press Enter. The System Recovery screen appears.
15. Tap the touch panel to advance to the next choice and navigate to **apply upgrade from adb**.
16. Press the Scan button.
17. Navigate to **Full OTA Package**.
18. Press the Scan button.
19. On the host computer command prompt window type:
    `adb sideload <file>`
    where: <file> = the path and filename of the zip file.
20. Press Enter. The Factory Reset package installs and then the Recovery screen appears.
21. Press the Scan button to reboot the device.Replace the top cover.

# Storage

The device contains four types of file storage:

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

- Enterprise folder.

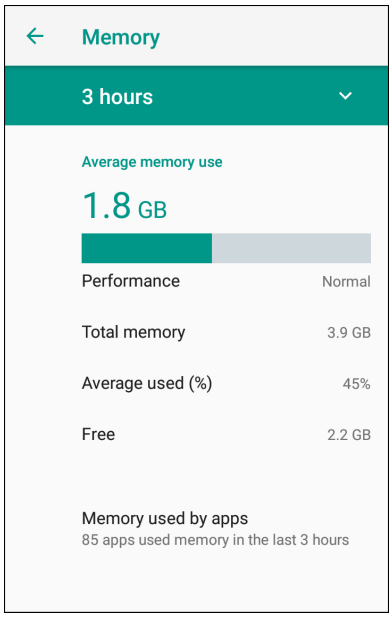
For more information, see Knowledge Articles - Best Practices in Mobile Computing: Flash at zebra.com/ps20-info.

## 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 150** Memory Screen




The screen displays the amount of used and free RAM.

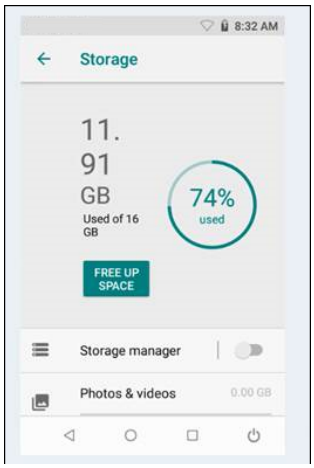
- **Performance** - Indicates memory performance.
- **Total memory** - Indicates the total amount of RAM available.
- **Average used (%)** - Indicates the average amount of memory (as a percentage) used during the period of time selected (default - 3 hours).
- **Free** - Indicates the total amount of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

## On Device Storage

The PS20 has On Device Storage. The On Device Storage content can be viewed and files copied to and from when the PS20 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 On Device Storage, swipe down from the Status bar and then touch ⚙ > **Storage**.

Figure 151 On Device Storage Screen



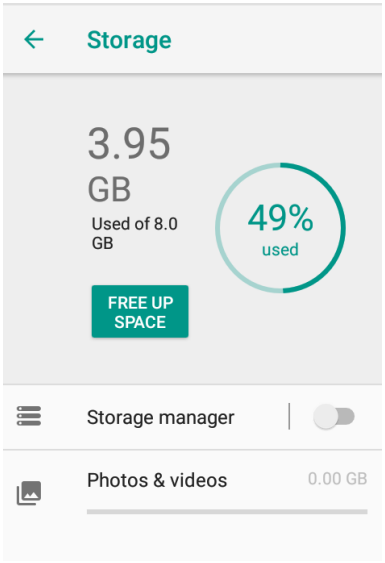

## Internal Storage

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 152 Storage Screen




### Enterprise Folder

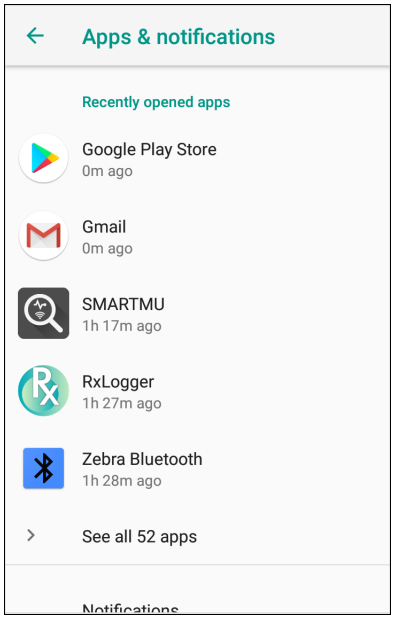
The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128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

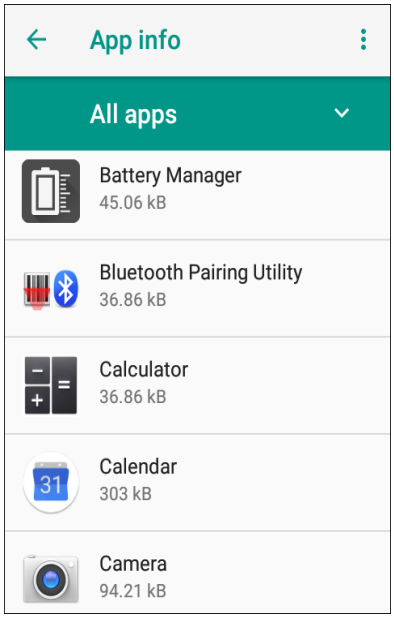
1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Apps & notifications**.

**Figure 153** Apps & Notifications Screen




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

Figure 154 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 with details about it and, depending on the item, to change its settings, permissions, notifications and to force stop or uninstall it.

# Viewing App Details

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

- **Force stop** - stop an app.

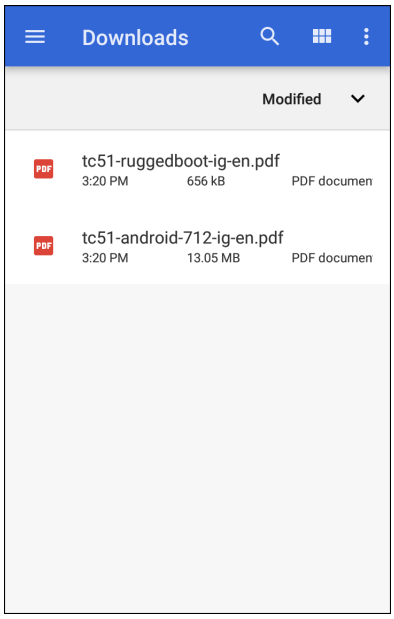
- **Disable** - disable an app.
- **Uninstall** - remove the app and all of its data and settings from the device. See Uninstalling an Application for information about uninstalling apps.
- **Storage** - lists how much information is stored, and includes a button for clearing it.
- **Data usage** - provides information about data (Wifi) 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 155 Files - Downloads Screen




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

# Changing Application Location

Some applications are designed to be stored on On-device Storage, rather than in internal storage. Others are designed so you can change where they are stored. You may find it helpful to move large applications off of

your internal storage, to make more room for other applications that don't offer the option. Many large applications are designed this way for exactly this reason.

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Apps.**
3. Swipe the screen to display the **On Device Storage** tab.

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

   Applications that are stored on On-device Storage card are checked.

   The graph at the bottom shows the amount of memory used and free of On-device Storage: the total includes files and other data, not just the applications in the list.
4. Touch an application in the list.
5. The Storage section of the application's details screen shows details about the memory used by the application. If the application can be moved, the Move button is active.
6. Touch **Move to On-device Storage** to move the bulk of the application from the device's internal storage to the On-device Storage.
7. Touch **Move to device** to move the application back to the device's internal storage.

# Settings

## Introduction

This chapter describes settings available for configuring the device.

## 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.

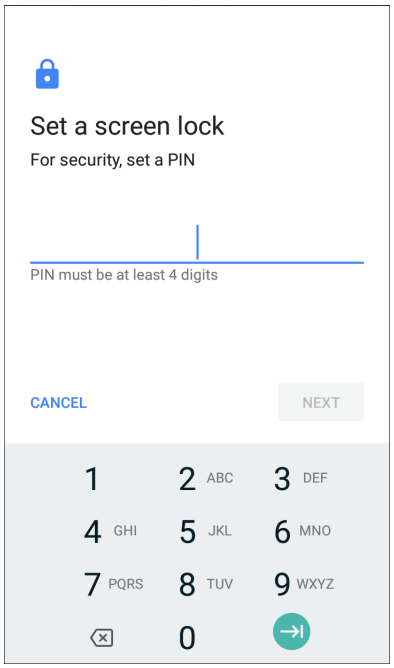
Slide the screen up to unlock. If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.

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 156** PIN Screen



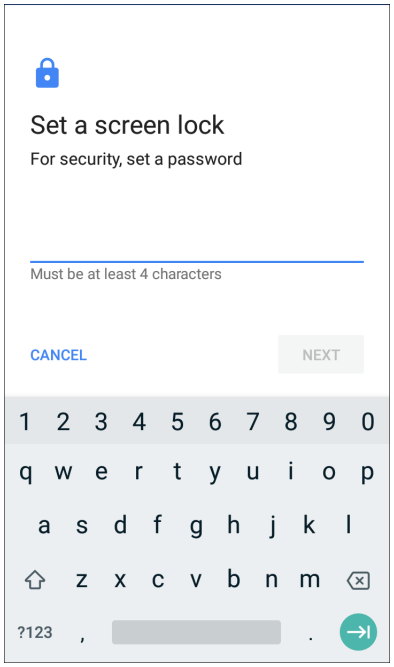

6. Touch in the text field.
7. Enter a PIN (4 numbers) then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch ◯. The next time the device goes into suspend mode a PIN is required upon waking.

# 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) then touch **Next**.

**Figure 157** Password Screen

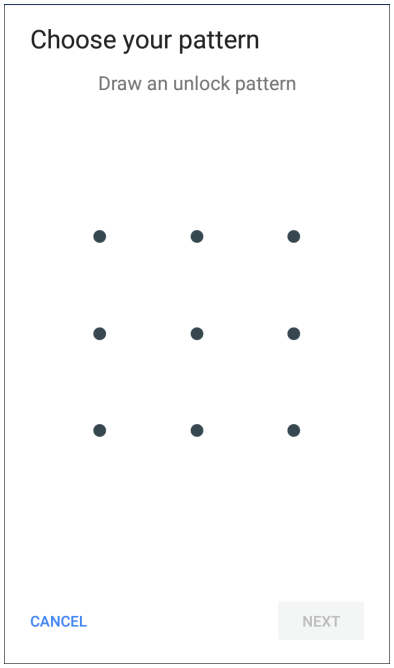



8. Re-enter the password and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch ○. The next time the device goes into suspend mode a password is required upon waking.

## 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 158** 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.

# 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 phase 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:

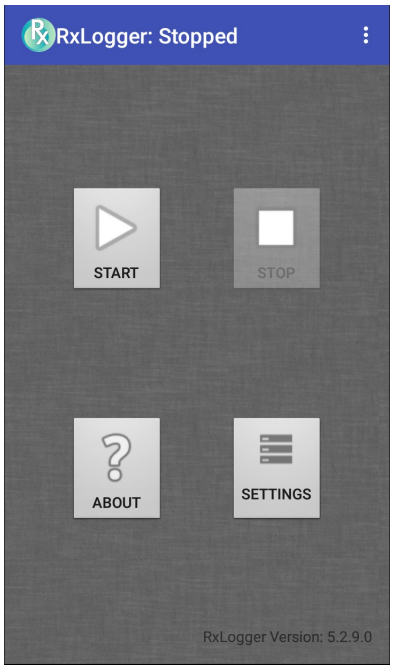
- Android Keyboard - AOSP devices only
- Enterprise Keyboard
- Gboard - GMS devices only.

## 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 159** RxLogger




## RxLogger Settings

The RxLogger Settings module provides additional RxLogger settings.

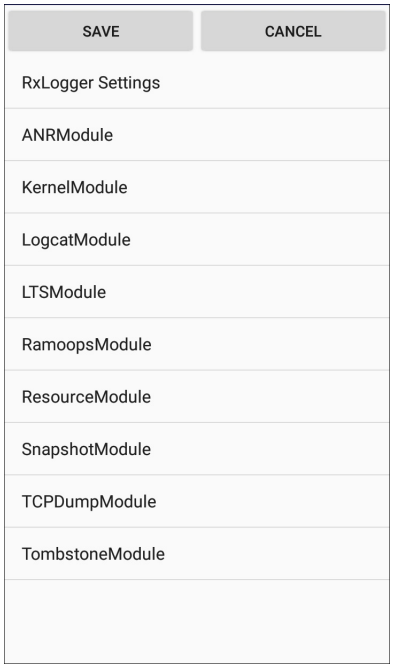
- **Enable notifications** - Select to allow RxLogger notifications in the Status bar and Notification panel.
- **Enable debug logs** - Select to enable debug logs.

## 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 160** RxLogger Configuration Screen




## 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.

## Kernal Module

The Kernel Module captures kmsg from the system.

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

## Qxdm Module

The Ramoops Module captures Qualcomm Modem Logs from the device.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the storage path for Qxdm files.

- **Qxdm Log Size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Qxdm test sets to keep** - Specifies the number of test sets to keep. One test set is a start and stop.
- **Choose Log Filter** - Select which filter Qxdm uses to process logs.
- **Path for User Defined Filter** - Specifies the path to a user-defined configuration file.

## 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 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.

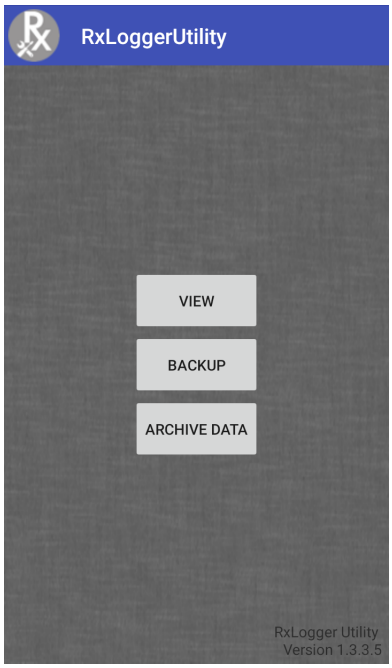
## RxLogger Utility

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 161** App View

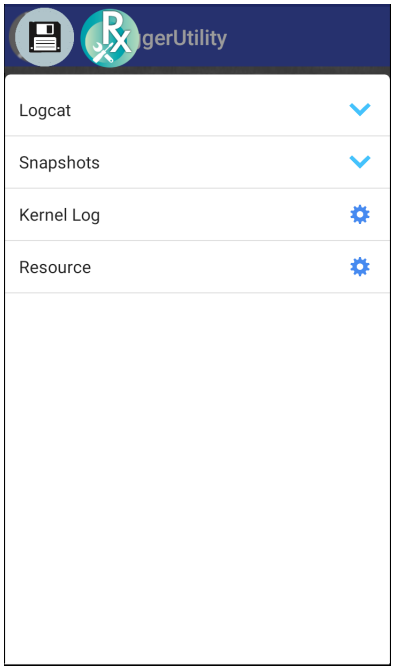



### Viewing Logs

To view logs:

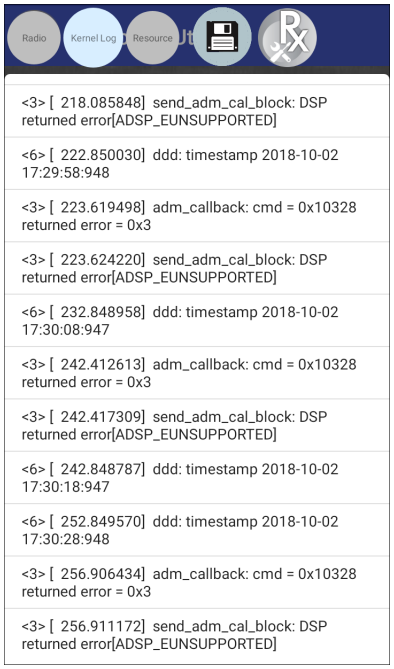
1. Touch the Main Chat Head icon. The Overlay View screen appears.

**Figure 162** 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 163** Log File

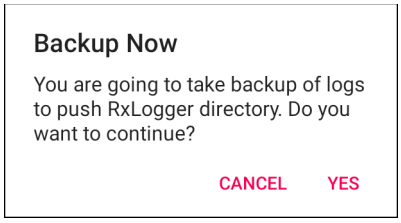


# Backup

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**.

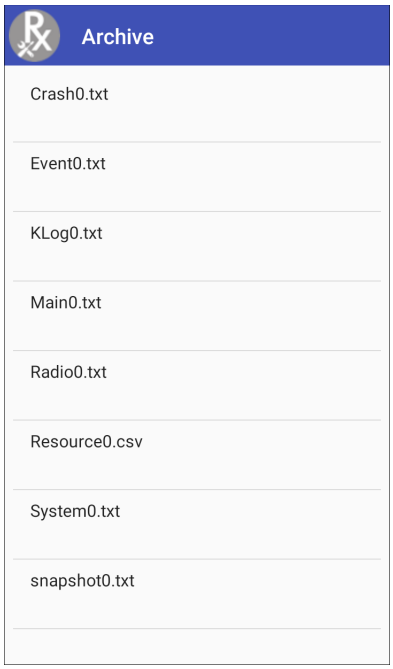
**Figure 164** Backup Message




## Archive Data

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

**Figure 165** 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:

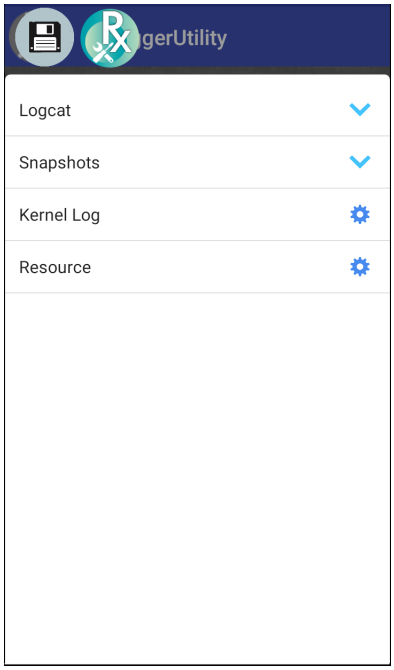
1. Touch and drag the icon. A circle with an X appears.
2. Move the icon over the circle and then release.

## Viewing Logs

To view logs:

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

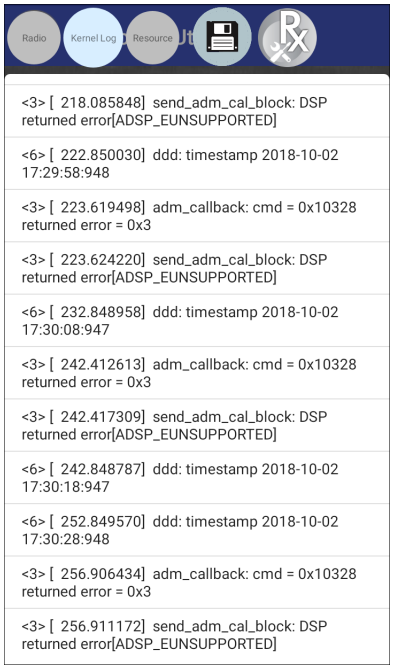
**Figure 166** Overlay View Screen




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 167** 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 Phone

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.
  - **Ethernet MAC address** - Displays the Ethernet driver MAC address.
  - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
  - **Serial number** - Displays the serial number of the device.
  - **MSM serial number** - Displays the serial number of the MSM.
  - **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.

# 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:

- In order to avoid scratching the screen, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the 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 battery and charger temperatures must be between +32ºF and +104ºF (0ºC and +40ºC)
- 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 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.

# Long Term Storage

When storing the device for a long period of time, it is recommended to remove the battery. When returning the device to everyday operation, install a fully charged battery.

# 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[1] **(see important note below)**, ammonium chloride or mild dish soap.

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

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

Due to the powerful oxidizing nature of sodium hypochlorite the metal surfaces on the device are prone to 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.

Approved cleaners include:

- Purell Ethanol Wipes

- 409 Glass Cleaner
- Windex Blue

## 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; acqueous 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.

Cleaners that are not approved include:

- Clorox Disinfecting Wipes
- Hydrogen Peroxide Cleaners
- Bleach Products.

## 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, but gently wipe the unit. Be careful not to let liquid pool around the display window or other places. Allow the unit to air dry before use.

**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 ethanolamine, 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.

For consistency and optimum image capture, it is recommended to clean the camera window periodically especially when used in environments prone to dirt or dust.

## 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.

### Camera and Exit Window

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

## Cleaning Battery Connectors

To clean the battery connectors:

1. Remove the main battery from the mobile computer.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. To remove any grease or dirt, rub the cotton portion of the cotton-tipped applicator back-and-forth across the connectors on the battery and terminal sides. Do not leave any cotton residue on the connectors.
4. Repeat at least three times.
5. Use a dry cotton-tipped applicator and repeat steps 3 and 4. Do not leave any cotton residue on the connectors.
6. Inspect the area for any grease or dirt and repeat the cleaning process if necessary.

**CAUTION:** After cleaning the battery connectors with bleach-based chemicals, follow the Battery Connector Cleaning instructions to remove bleach from the connectors.

## 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

## PS20

*Table 20 Troubleshooting the PS20*

| Problem | Cause | Solution |
|---|---|---|
| PS20 does not turn on. | Battery not charged. | Charge or replace the battery in the PS20. |
| | Battery not installed properly. | Ensure battery is installed properly. See Replacing the Battery on page 28. |
| | System crash. | Perform a soft reset. If the PS20 still does not turn on, perform a hard reset. See Resetting the Device on page 46. |
| Battery did not charge. | Battery failed. | Replace battery. If the PS20 still does not operate, try a soft reset, then a hard reset. See Resetting the Device on page 46. |
| | PS20 removed from cradle before charging completed. | Insert the PS20 into the cradle and begin charging. The battery fully charges in approximately four hours. |
| | Ambient temperature of the cradle is too warm or too cold. | The ambient temperature must be between 0 °C and 40 °C (32 °F and 104 °F). |
| During data communication, no data was transmitted, or transmitted data was incomplete. | PS20 unplugged from host computer during communication. | Reconnect the programming cable to the host computer and re-transmit. |
| | Communication software was incorrectly installed or configured. | See system administrator. |

*Table 20 Troubleshooting the PS20 (Continued)*

| Problem | Cause | Solution |
|---|---|---|
| PS20 turns itself off. | PS20 is inactive. | When the PS20 ships, by default, the Sleep period is **Never**. If the PS20 is running on battery power, this period can be changed to 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or 30 minutes. The PS20 turns off after the set period of inactivity. Change the setting if you need a longer delay before the automatic shutoff feature activates. |
| | Battery is depleted. | Place the PS20 in the cradle to re-charge the battery. |
| | Battery is not inserted properly. | Insert the battery properly (see Replacing the Battery on page 28). |
| | The PS20's battery is low and it powers down to protect memory content. | Place the PS20 in the cradle to re-charge the battery. |
| A message appears stating that the PS20 memory is full. | Too many files stored on the PS20. | Delete unused memos and records. You can save these records on the host computer. |
| | Too many applications installed on the PS20. | If you have installed additional applications on the PS20, remove them to recover memory. See Uninstalling an Application on page 214. |
| The PS20 does not accept scan input. | Scanning application is not loaded. | Verify that the PS20 is loaded with a scanning application. See the System Administrator. |
| | Unreadable bar code. | Ensure the symbol is not defaced. |
| | Distance between imager exit window and bar code is incorrect. | Move the PS20 closer or further from the bar code to the proper scanning range. |
| | PS20 is not programmed for the bar code. | Verify that the PS20 can read the type of bar code being scanned (See Technical Specifications). Ensure that the bar code parameters are set properly for the bar code being scanned. |
| | PS20 is not programmed to generate a beep. | Verify that a beep on a good decode is used. See Barcode Input on page 161 for more information. |
| | Battery is low. | If the scanner is still not reading symbols, contact the distributor or service. |
| During USB data communications, no data was transmitted, or transmitted data was incomplete. | Incorrect cable connection. | See USB Communication. |
| | Communications software is not installed or configured properly. | Perform setup as described in Cradle Installation. |
| | | Ensure that a sync program is installed on the host computer. |
| Cannot sync with Host Computer | Host computer not configured properly. | Ensure that sync program on the host computer is set to allow USB connections. See USB Communication for more information. |

## Cradles

*Table 21 Troubleshooting the Cradles*

| Symptom | Possible Cause | Solution |
|---|---|---|
| PS20 battery is not charging. | PS20 was removed from cradle or cradle was unplugged from AC power. | Ensure cradle is receiving power. Ensure PS20 is seated correctly. Confirm main battery is charging. The battery fully charges in approximately four hours. |
| | Battery is faulty. | Verify that other batteries charge properly. If so, replace the faulty battery (see Replacing the Battery on page 28). |
| | The PS20 is not fully seated in the cradle. | Remove and re-insert the PS20 into the cradle, ensuring it is firmly seated. |
| | Ambient temperature of the cradle is too warm or too cold. | Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F). |
| When the PS20 is placed in the cradle, the cradle LED does not blink. | Cradle is not powered. | Ensure cradle is receiving power. |
| | Cradle firmware is corrupted. | Contact system administrator. |
| | The PS20 is not operational. | Contact system administrator. |
| | Cradle - PS20 communication error. | Contact system administrator. |
| Cradle LED blinks red. | The cradle is issued an unlock command and it fails to unlock. | Contact system administrator. |
| | Cradle is overheating due to continuous lock/unlock or other cradle faults. | Contact system administrator. |

# Specifications

## Technical Specifications

The following tables summarize the PS20's intended operating environment and general technical hardware specifications.

*Table 22 Technical Specifications*

| Item | Description |
|---|---|
| **Physical and Environmental Characteristics** | |
| Dimensions (H x L x W) | 2.95 in. x 8.58 in. x 3.09 in. (7.50 cm x 21.80 cm x 7.86 cm) |
| Weight | 290 g (10.23 oz) with battery |
| Keys | Single Scan key |
| Display | Color LCD, 4",480x800 WVGA resolution, 16 bits/pixel RGB, 450 Nits LED backlight, capacitive touch screen |
| Speaker | 2W speaker |
| Main Battery | PowerPrecision+ rechargeable 3.63 VDC Lithium Ion battery<br>Typical Capacity: 3,500 mAh.<br>Minimum Capacity: 3,350 mAh. |
| **Performance Characteristics** | |
| CPU | Qualcomm Snapdragon ™ 660 octa-core, 2.2 GHz |
| Operating System | Android 8.1 Oreo |
| Memory | Flash - 16 GB, RAM - 4 GB |
| Application Development | Zebra Android EMDK. |
| Data Capture Method | Base: SE2100 1D/2D imager with white LED illumination<br>Plus: SE4710 1D/2D imager + Digimarc support with red LED illumination with LED dot aim pattern |
| Camera (Front Facing) | Plus model only: 5 MP fixed focus |
| **User Environment** | |
| Operating Temperature | -10°C to 50°C (14°F to 122°F) |
| Storage Temperature | -20°C to 70° C (-4°F to 158°F) |
| Battery Charging Temperature | 0°C to +40°C (32°F to 104°F) ambient temperature range. |

*Table 22 Technical Specifications (Continued)*

| Item | Description |
|---|---|
| Humidity | 40°C (RH 5% - 95%) Non-condensing |
| Flammability | UL94V1 |
| Drop Specification | 4 ft.(1.2 m) to concrete, over operating temperature range. |
| Sealing | Liquid penetration per “A4T Casual Spill Test Spec” document number 71-98611-01. Applies ONLY with battery installed. |
| ESD | ± 15k VDC air discharge<br>± 8k VDC contact discharge |
| **Wireless LAN Data Communications** | |
| Radio | IEEE ® 802.11 a/b/g/n/ac/d/h/i/r/k/v/w; Wi-Fi ™ certified; IPv4, IPv6, 2x2 MU-MIMO |
| Data Rates | 5 GHz: 802.11a/n/ac - up to 866.7 Mbps;<br>2.4 GHz: 802.11b/g/n - up to 300 Mbps |
| Operating Channels | Channels 1 - 13 (2412 - 2472 MHz) 1,2,3,4,5,6,7,8,9,10,11,12,13<br>Channels 36 - 165 (5180 - 5825 MHz) 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140, 144,149,153,157,161,165<br>Actual operating channels/frequencies depend on regulatory rules and certification agency |
| Security and Encryption | WEP (40 or 104 bit);<br>WPA/WPA2 Personal (TKIP, and AES);<br>WPA/WPA2 Enterprise (TKIP, and AES) - EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0- MSCHAPv2, PEAPv1-EAP-GTC and LEAP, EAP-PWD |
| Multimedia | Wi-Fi Multimedia ™ (WMM) |
| Certifications | WFA (802.11n, WMM-PS, 801.11ac, PMF) |
| Fast Roam | PMKID Caching, Cisco CCKM, 802.11r, OKC |
| **Wireless PAN Data Communications** | |
| Bluetooth | V5.0 with Low Energy |
| USB | USB 2.0 Client for service and maintenance |
| **Data Capture Specifications** | |
| 2D Imager | SE2100 imager (1D and 2D).<br>SE4710 imager (1D and 2D). |
| Camera | |
| **2D Imager Engine (SE2100) Specifications** | |
| Field of View | Horizontal - 41.5°<br>Vertical - 31.7° |
| Image Resolution | 640 horizontal X 480 vertical pixels |
| Roll | 360° |
| Pitch Angle | ± 60° from normal |

*Table 22 Technical Specifications (Continued)*

| Item | Description |
|---|---|
| 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 | LED: Ultra white<br>Pattern Angle: 42° horizontal, 32.0° vertical at 50% intensity |
| **2D Imager Engine (SE4710) Specifications** | |
| Field of View | Horizontal - 42.0°<br>Vertical - 28° |
| Image Resolution | 1280 horizontal X 800 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: 19.4 cm (7.64 in.) |
| Laser Aiming Element | LED: 610<br>Aiming Dot Brightness Level: 130 fcd nominal |
| Illumination System | LEDs: Hyper Red 660 nm<br>Pattern Angle: 53° horizontal, 32° vertical at 50% intensity |

## Supported Symbologies

*Table 23 Data Capture Supported Symbologies*

| Item | Description |
|---|---|
| ID Barcodes | Code 39, Code 128, Code 93, Codabar, MSI, UPC/EAN, Interleaved 2 of 5, RSS, Composite, TLC-39 |
| 2D Barcodes | PDF-417, Micro PDF-417, Composite, TLC-39, Datamatrix, QR Code, Micro QRCode, Maxicode, Postal codes, Aztec Code, Han Xin |

## Three Slot Cradle

*Table 24 Cradle Specifications*

| Item | Description |
|---|---|
| Operating Temperature | 0° C to +40° C (32° F to 104° F) |
| Storage Temperature | -20° C to 60° C (-4° F to 140° F) |
| Battery Charging Temperature | 0° C to +40° C (32° F to 104° F) ambient temperature |
| Humidity | 10% to 95% non-condensing |

*Table 24 Cradle Specifications*

| Item | Description |
|---|---|
| Size (H x L x W) | 129 mm x 134 mm x 310 mm (5 in x 5.2 in x 12.2 in) |
| Weight | 1550 g (54.67 oz) |
| Power Supply | 12.0 VDC,9.0 A |
| Electrostatic Discharge (ESD) | ±15 k VDC air discharge, ± 8 k VDC contact discharge |

## Single Slot Cradle

*Table 25 Cradle Specifications*

| Item | Description |
|---|---|
| Operating Temperature | 0° C to +40° C (32° F to 104° F) |
| Storage Temperature | -20° C to 60° C (-4° F to 140° F) |
| Battery Charging Temperature | 0° C to +40° C (32° F to 104° F) ambient temperature |
| Humidity | 10% to 95% non-condensing |
| Size (L x W x H) | 98 mm x 127 mm x 272 mm (4 in. x 5 in. x 10.7 in.) |
| Weight | 620 g (21.87 oz) |
| Power Supply | 12.0 VDC,9.0 A |
| Electrostatic Discharge (ESD) | ±15 k VDC air discharge, ± 8 k VDC contact discharge |

# PS20 Interface Connector Pin-Outs

Figure 168 Power Connector Pin-Outs

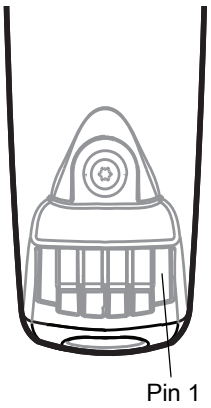



*Table 26 Power Connector Pin-Outs*

| PIN | Signal Name | Function |
|---|---|---|
| 1 | +5V | Input power |
| 2 | TX | Transmit Output to Cradle |
| 3 | RX | Receive Input from Cradle |
| 4 | GND | Ground |

# Cable Specifications

## Power Supply Cable, Y-type

*Table 27 Wire Run List & Specifications*

| Wire Color | AWG | Connector 1 Molex 39-01-2060 housing; 4x, 39-00-0211 contacts | Connector 2 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts | Connector 3 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts | Function |
|---|---|---|---|---|---|
| Red | 16 | 1 | 1 | | (+) term |
| Black | 16 | 6 | 2 | | (-) term |
| Red | 16 | 2 | | 1 | (+) term |
| Black | 16 | 5 | | 2 | (-) term |

The 16 AWG wire should have the following specifications: UL1007, 300 Volt, PVC, -40° C to 80° C operating temperature.

## Cradle Interconnection Cable

*Table 28 Wire Run List & Specifications*

| Wire Color | AWG | Connector 1<br>Molex 39-01-2025 housing; 2x,<br>39-00-0211 contacts | Connector 2<br>Molex 39-01-2025 housing; 2x,<br>39-00-0211 contacts | Function |
|---|---|---|---|---|
| Red | 16 | 1 | 1 | (+) term |
| Black | 16 | 2 | 2 | (-) term |

The 16 AWG wire should have the following specifications: UL1007, 300 Volt, PVC, -40° C to 80° C operating temperature.

# Index

## D



## E

## F



## G



## H



## K



## L



## M



## N



## O



## P

## Q



## R



## S



## T



## U



## V



## W