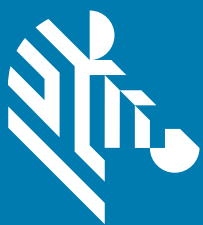


VC8300

8" Vehicle-Mounted Computer



User Guide for Android™ 8.1.0 Oreo



ZEBRA

Copyright

© 2019 ZIH Corp. and/or its affiliates. All rights reserved. ZEBRA and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. Google, Android, Google Play and other marks are trademarks of Google LLC; Oreo is a trademark of Mondelez International, Inc. group. All other trademarks are the property of their respective owners.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

Terms of Use

- Proprietary Statement

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

- Product Improvements

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

- Liability Disclaimer

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

- Limitation of Liability

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

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	4/2019	Initial release

Table of Contents

Copyright	2
Terms of Use	2
Revision History	2
About This Guide	14
Introduction	14
Configurations	14
Software Versions	14
Chapter Descriptions	15
Notational Conventions	15
Related Documents and Software	16
Service Information	16
Provide Documentation Feedback	16
Getting Started	17
Introduction	17
Unpacking	17
Removing the Protective Film from the Display	17
Safety	17
Initial Operation Safety Considerations	18
Power Supply/Cable Safety	18
External Devices Safety	18
Features	19
Front Keys and LED Indicators	21
Front Keys	21
LED Indicators	21
Powering Up the Device	22
Powering Down the Device	22
Setting Up WLAN	22
Device Settings	22

Table of Contents

Heater Status	22
Battery Management	22
Monitoring Battery Usage	22
Low Battery Notification	23
Turning Off the Radios	23
Installation	24
Introduction	24
Overview	24
Mounting Instructions	24
Installing the Device	24
Electrical Installation	24
Wiring Guidelines	25
Wiring Vehicle Power to the VC8300	26
External Antenna Installation	26
Positioning the VC8300 in the Vehicle	27
Overview of the Assembly Steps	27
Cable Dust Cover	27
Strain Relief	28
Installing the VC8300 on a Forklift	28
Forklift Battery Replacement Conditions	29
Starting from Cold Soak	29
Pre-Heat Mode	30
Installing the Power Pre-Regulator	30
Non-Vehicle Installations	31
Screen Blanking Wiring	32
Connecting Switch for Screen Blanking	32
Using the Device	34
Google Mobile Services	34
Home Screen	34
Status Bar	35
Status Icons	36
Notification Icons	37
Managing Notifications	38
Setting App Notifications	38
Viewing Notification Settings for All Apps	39
Controlling Lock Screen Notifications	39
Quick Access Panel	39
Editing Icons on Quick Settings	40
App Shortcuts and Widgets	41

Table of Contents

Adding an App Shortcut to the Home Screen	41
Moving Items on the Home Screen	41
Removing an App Shortcut or Widget from the Home Screen	41
Folders	42
Creating a Folder	42
Naming Folders	42
Removing a Folder	42
Home Screen Wallpaper	42
Using the Touchscreen	43
Integrated Keyboard	43
Soft Input Panel	45
Virtual Keyboards	46
Using the GBoard Keyboard	46
Editing Text	46
Entering Numbers, Symbols and Special Characters	46
Using the Enterprise Keyboard	47
Numeric Tab	47
Alpha Tab	47
Special Character Tab	47
Scan Tab	48
Apps	49
Accessing Apps	51
Switching Between Recent Apps	51
Un-Locking the Screen	52
Resetting the Device	54
Performing a Soft Reset	54
Performing a Hard Reset	54
Suspend Mode	54
Transferring Files	54
Using a USB Drive	55
Disconnecting USB Drive	55
Apps	56
Battery Manager	56
Contacts	59
Adding a Contact	59
Editing Contacts	59
Deleting Contacts	59
DataWedge Demonstration	60
Scanner Selection	61
Device Central	62
Scan and Pair Tab	62

Table of Contents

Scan and Pair	62
Scan to Pair	63
Manually Pairing	63
Peripherals Tab	63
My Device Tab	64
Unpairing a Peripheral	65
Paging an RS6000 Ring Scanner	65
Files	66
Diagnostic Tool	67
Settings	69
Battery Test Information	69
GPS Test Information	69
System Test Information	70
WLAN Test Information	70
WWAN Test Information	70
Bluetooth Test Information	70
Heater Control	71
Temperatures	71
Serial Port Heater	71
USB Port Heater	72
Battery Heater	72
Touch Panel Heater	72
Keyboard Heater	72
Photos	73
PTT Express Voice Client	74
Speaker/Microphone Setup	74
PTT Audible Indicators	74
Notification Icons	75
Enabling PTT Communication	76
Selecting a Talk Group	76
PTT Communication	76
Creating a Group Call	76
Responding with a Private Response	76
Disabling PTT Express Voice Client Communication	77
RxLogger	78
Enabling Logging	78
Disabling Logging	78
RxLogger Configuration	78
ANR Module	79
Kernel Module	79
Logcat Module	79
LTS Module	81
Ramoops Module	81

Table of Contents

Resource Module	81
Snapshot Module	82
TCPDump Module	82
Tombstone Module	82
Enabling Logging	83
Disabling Logging	83
Extracting Log Files	83
RxLogger Utility	84
App View	84
Viewing Logs	84
Backup	85
Archiving	85
Overlay View	86
Removing the Main Chat Head	86
Viewing Logs	86
Removing a Sub Chat Head Icon	87
Backup	87
VC Settings	88
Display	88
Peripheral Power	88
Ignition Detection	89
WIFI Antenna Switching	89
Built-In Speaker	89
Screen Blanking	89
Velocity	90
Data Capture.....	91
Imaging	91
Operational Modes	92
Laser Scanning	92
Scanning Considerations	92
Barcode Capture with RS6000 Bluetooth Ring Scanner	93
Barcode Capture with RS507/RS507x Hands-Free Imager	94
Bar Code Capture with Zebra Scanner	95
Connecting an RS-232 Scanner	96
Connecting a USB Scanner	98
Connecting Using Simple Serial Interface	98
Connecting Using HID Mode	99
Pairing the RS507/RS507x/RS6000 Hands-Free Imager	99
Pairing Using Simple Serial Interface	99
Pairing Using Human Interface Device	100
Pairing a DS3678 Scanner	101

Table of Contents

Pairing Using Simple Serial Interface	101
Pairing a DS3678 Scanner Using Human Interface Device	102
DataWedge	102
Enabling DataWedge	103
Disabling DataWedge	103
Wireless	104
Wireless Local Area Networks	104
Scanning and Connecting to a Wi-Fi Network	104
Remove a Wi-Fi Network	105
Configuring a Wi-Fi Network	106
Manually Adding a Wi-Fi Network	107
Configuring for a Proxy Server	108
Configuring the Device to Use a Static IP Address	109
Wi-Fi Preferences	110
Additional Wi-Fi Settings	111
Wi-Fi Direct	112
WPS Pin Entry	113
WPS Push Button	113
Wi-Fi Advanced Features	114
Zebra Mobility Extensions	115
Bluetooth	115
Adaptive Frequency Hopping	115
Security	116
Bluetooth Profiles	116
Bluetooth Power States	117
Bluetooth Radio Power	117
Enabling Bluetooth	117
Disabling Bluetooth	118
Discovering Bluetooth Device(s)	118
Changing the Bluetooth Name	118
Connecting to a Bluetooth Device	119
Selecting Profiles on the Bluetooth Device	119
Unpairing a Bluetooth Device	119
Accessories and Mounting	120
Introduction	120
Accessories	120
VC8300 Antenna Options	121
VC8300 Mounting Accessories	123
MT43XX RAM Mount	124

Table of Contents

Optional Mounts	124
Plate Bases for MT35XX Mounts	125
MT4200 Quick Release Mount	126
Assembling MT4200	126
Attaching MT4200 to VC8300	127
MT4210 Adapter Bracket	128
DataWedge	129
Introduction	129
Profiles	129
Profile0	129
Plug-ins	130
Input Plug-ins	130
Process Plug-ins	130
Output Plug-ins	130
Profiles Screen	131
Profile Context Menu	131
Options Menu	132
Disabling DataWedge	132
Creating a New Profile	132
Profile Configuration	133
Associating Applications	133
Data Capture Plus	135
Barcode Input	137
Enabled	137
Scanner Selection	137
Auto Switch to Default on Event	137
Decoders	138
Decoder Params	139
UPC EAN Params	145
Reader Params	147
Scan Params	150
UDI Params	151
Multibarcodes	151
Serial Port Input from Serial Port 1	151
Serial Port Input from Serial Port 2	151
Voice Input	152
Keystroke Output	153
Intent Output	154
Intent Overview	155
IP Output	156
Usage	157
Using IP Output with IPWedge	157

Using IP Output without IPWedge	158
Generating Advanced Data Formatting Rules	159
Configuring ADF Plug-in	160
Creating a Rule	160
Defining a Rule	160
Defining Criteria	161
Defining an Action	162
Deleting a Rule	162
Order Rules List	163
Deleting an Action	164
ADF Example	164
DataWedge Settings	167
Importing a Configuration File	168
Exporting a Configuration File	168
Importing a Profile File	168
Exporting a Profile	168
Restoring DataWedge	169
Reporting	169
Configuration and Profile File Management	169
Enterprise Folder	170
Auto Import	170
Programming Notes	170
Overriding Trigger Key in an Application	170
Capture Data and Taking a Photo in the Same Application	170
Disabling DataWedge	171
Soft Scan Trigger	171
Function Prototype	171
Scanner Input Plugin	171
Function Prototype	171
Parameters	171
Return Values	172
Example	172
Comments	172
Enumerate Scanners	173
Function Prototype	173
Parameters	173
Return Values	173
Example	174
Comments	174
Set Default Profile	175
Default Profile Recap	175
Usage Scenario	175
Function Prototype	175
Parameters	175

Return Values	175
Example	176
Comments	176
Reset Default Profile	176
Function Prototype	177
Parameters	177
Return Values	177
Example	177
Comments	177
Switch To Profile	178
Profiles Recap	178
Usage Scenario	178
Function Prototype	178
Parameters	178
Return Values	179
Example	179
Comments	179
Notes	180
Settings.....	181
Introduction	181
Setting the Date and Time	181
Display Setting	182
Setting the Screen Brightness	182
Setting Screen Timeout	182
Setting Font Size	183
Setting Screen Rotation	183
The Keyboard Backlight	184
General Sound Setting	184
Do Not Disturb Feature	186
Limit Sounds and Vibrations	186
Total Silence	186
Alarms Only	186
Automatically Block Sounds and Vibrations	187
Silence Sounds During Certain Times	187
Silence Sounds During Events and Meetings	187
Turn Sounds Back On	188
Setting Screen Lock	188
Setting Screen Lock Using PIN	189
Setting Screen Unlock Using Password	189
Setting Screen Unlock Using Pattern	190
Passwords	191
System Language Usage	191

Table of Contents

Adding Languages	191
Selecting a Language	191
Removing a Language	191
Adding Words to the Dictionary	192
Virtual Keyboard Settings	192
Enterprise Keyboard Configuration	192
Enabling Keyboards	192
Configuring the GBoard Keyboard	193
Configuring the Enterprise Keyboard	193
Key Programmer	193
Remapping a Button	193
About Phone	195
Application Deployment.....	196
Introduction	196
Security	196
Secure Certificates	196
Installing a Secure Certificate	196
Configuring Credential Storage Settings	197
Development Tools	197
Android	197
EMDK for Android	198
StageNow	198
ADB USB Setup	199
Enabling USB Debugging	199
Application Installation	200
Installing Applications Using a USB Drive	200
Installing Applications Using the Android Debug Bridge	201
Uninstalling an Application	203
Performing a System Update	204
Downloading the System Update Package	204
Using USB Drive	204
Using ADB	204
Verify System Update Installation	205
Performing an Enterprise Reset	206
Downloading the Enterprise Reset Package	206
Using a USB Drive	206
Using ADB	206
Performing a Factory Reset	207
Downloading the Factory Reset Package	207
Using a USB Drive	208

Table of Contents

Using ADB	208
Storage	209
Random Access Memory	209
Internal Storage	210
External Storage	211
Formatting a USB Drive	212
Enterprise Folder	212
App Management	213
Viewing App Details	213
Managing Downloads	214
Maintenance and Troubleshooting	215
Introduction	215
Cleaning	215
Housing Cleaning	215
Touchscreen Cleaning	215
Touchscreen	215
Troubleshooting	216
Specifications.....	219
Introduction	219
Technical Specifications	219
Drill Hole Dimensions	222

About This Guide

Introduction

This guide provides instructions for setting up, operating, configuring, and maintaining the VC8300 8" vehicle-mount computer.



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



WARNING: Before transporting, assembling, and starting the computer, please read this manual carefully and follow all the safety guidelines and requirements.

Configurations

The VC8300 offers different configurations to suit various work requirements. Some of the configuration options include:

- Qualcomm Snapdragon 660 octa-core 2.2 GHz
- 4 GB RAM/ 32 GB Flash
- Sunlight Readable Display
- Internal and External Antenna
- Freezer Condensing
- Android 8.1.0 Oreo Google™ Mobile Services (GMS)
- Basic I/O.



NOTE: For detailed configuration and part number information, contact your Zebra representative.

Software Versions

To determine the current software versions:

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

4. Scroll to view the following information:

- **Model**
- **Android version**
- **Android security patch level**
- **Kernel version**
- **Build number.**

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

- **Serial number**

Chapter Descriptions

Topics covered in this guide are as follows:

- [Getting Started](#) provides information on safety guidelines and initial VC8300 setup.
- [Installation](#) provides instructions on installing the VC8300.
- [Using the Device](#) provides information for operating the VC8300.
- [Apps](#) provides information on using applications installed on the VC8300.
- [Data Capture](#) explains how to capture data using the optional scanners.
- [Wireless](#) provides information on the various wireless options.
- [Accessories and Mounting](#) describes the accessories and mounting options available for the VC8300.
- [DataWedge](#) describes how to use and configure the DataWedge application.
- [Settings](#) provides the settings for configuring the VC8300.
- [Application Deployment](#) provides information for developing and managing applications.
- [Maintenance and Troubleshooting](#) includes instructions on cleaning the VC8300 and provides troubleshooting solutions for potential problems during device operations.
- [Specifications](#) summarizes the device's intended operating environment and technical specifications.

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.
 - Chapters and sections in this guide
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents and Software

The following document provides more information about the VC8300 vehicle-mount computer.

- VC8300-8 Quick Reference Guide, p/n MN-003394-xx - includes setup information and regulatory information.
- U-Mount Bracket Installation Guide, p/n MN-002931-xx - includes the instructions to install the U-Mount Bracket Kit (KT-U-MOUNT-VC80-R) and dimensions.
- Adapter Bracket Kit for VC50 U-Mount Installation Guide, p/n MN-002932-xx - provides instruction on installing the Adapter Bracket Kit (MNT-VC80-ADPA1-1) to attach the VC8300 to the VC5090 U-Mount.
- Adapter Bracket Kit for Honeywell U-Mount Installation Guide, p/n MN-002934-xx - provides instruction on installing the Adapter Bracket Kit (MNT-VC80-ADPB1-1) to attach the VC8300 to the Honeywell U-Mount Bracket.

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

Service Information

If you have a problem with your equipment, contact Zebra Customer Support for your region. Contact information is available at: <http://www.zebra.com/support>.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number.

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

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

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

Provide Documentation Feedback

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

Getting Started

Introduction

The VC8300 is a rugged, vehicle mounted computer running Android 8.1.0 Oreo operating systems. Wireless communications are supported over a 802.11 WLAN network. The Bluetooth module supports Bluetooth printers and scanners. The VC8300-8 contains an integrated keyboard in either QWERTY or AZERTY alphanumeric keyboard layout. It features 54 keys, 12 direct function keys, and a power button.

The VC8300 is intended for use in commercial and industrial applications with a focus on real time wireless data transactions with options suiting materials handling applications in warehouses, manufacturing facilities, ports, yards, and freezers.

Unpacking



WARNING: Before operating the unit for the first time, carefully read Safety on page 17.



NOTE: Configure the VC8300 before fastening it to machines or vehicles.

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

Inspect the equipment for damage. If any equipment is missing or damaged, contact the Zebra Support Center immediately. See Service Information on page 16 for contact information.

Removing the Protective Film from the Display

The front display of the VC8300 is protected during transport by a transparent film. This film should remain on the front display during assembly to avoid damage to the front display surface. Only remove the film once all of the assembly work has been completed.

Safety

In order to prevent injury and damage, observe the following safety guidelines prior to assembly and commissioning. The VC8300 is a multifunction vehicle computer for stationary and mobile use in commercial environments such as, warehouses, manufacturing, yard/ports, and freezers. Different or extraordinary usage is not permitted. For resulting damage, the user/operator of the VC8300 is solely responsible. This also applies to any changes that you make to the device. Compliance with the safety

guidelines is particularly important for the proper use of this device. The manufacturer assumes no liability for any and all damages that can be attributed to non-compliance with these guidelines.

Initial Operation Safety Considerations

- Installation/Initial Operation - Perform VC8300 installation in accordance with [Installation on page 24](#). Specifically, pay special attention to the various electrical potentials of the vehicle. Some vehicles have a chassis that is connected to one of the battery supply lines (DC+ or DC-), while most electrically-driven forklift vehicles have floating chassis, connected to neither DC+ or DC-. See Wiring Vehicle Power to the VC8300 on page 26 for required wiring of vehicle power and fusing for the VC8300.
- Risk of injury during transit or installation - The unit can fall during transit or installation and cause injury. Always ensure that there are two persons available when installing or removing the device.
- Ensure that no persons are injured in case the mounting bracket breaks - The VC8300 may not be installed in such a way that persons can be injured during a breaking of the mounting bracket (e.g. fatigue break). If the device is mounted in a place where people can be injured if the bracket breaks, apply appropriate safety measures (e.g. install a security cable in addition to the device bracket).

Power Supply/Cable Safety

The main power cord shall comply with the national safety regulations of the country where the equipment is to be used.

- Operation in an emergency - In case of an emergency (such as damage to the power cable or housing, or ingress of liquid or other foreign bodies), disconnect the device immediately from the power supply. Contact technical support staff at once.
- Protection of the power supplies - If, after replacement, the fuse fed by the internal power supply blows, send the device for servicing immediately.
- Danger of electrocution when cleaning/servicing the device - In order to avoid electrocution, always disconnect the VC8300 from the power supply before cleaning or servicing the device.
- Do not exceed maximum voltage when charging the vehicle battery - While charging the vehicle battery, disconnect the VC8300 from the battery or ensure that the maximum allowed input voltage of the VC8300 is not exceeded.
- Do not switch on devices with damaged cables or plugs - Do not use the VC8300 if a cable or plug is damaged. Replace damage parts immediately.
- Do not connect or disconnect cables during storms - Cables must never be connected or disconnected during an electrical storm.

External Devices Safety

The use of additional wiring and other peripheral devices, which are not recommended or sold by the manufacturer, can result in fire, electrocution or personal injury.

- If a power supply is used, only use the power supply recommended by the manufacturer.
- Before connecting or disconnecting peripheral devices (exception: USB devices), disconnect the VC8300 from the power supply to avoid serious damage to both the VC8300 and the connected devices.

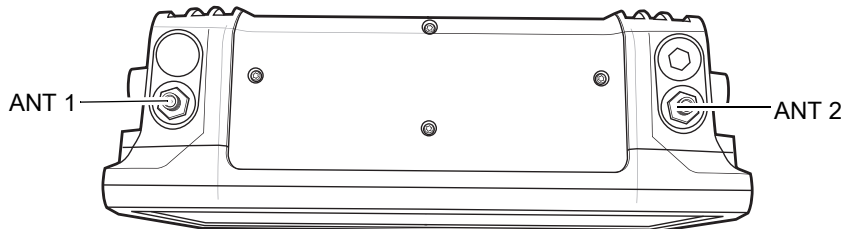
Features

Figure 1 VC8300 8" Front View



Figure 2 VC8300 8" Top View

802.11 a/b/g/n/ac Radio External Antenna Connectors



ANT 1 - Reverse Polarity SMA Jack (WLAN & BT) / External Main Antenna

ANT 2 - Reverse Polarity SMA Jack (WLAN) / External Aux Antenna



NOTE: Optional external Wi-Fi antennas are not shipped with the device and must be ordered as a separate accessory. The device can be switched between internal and external antenna. For a complete list of configurations see [Table 14 on page 120](#).

Figure 3 VC8300 Back View with Dust Cover

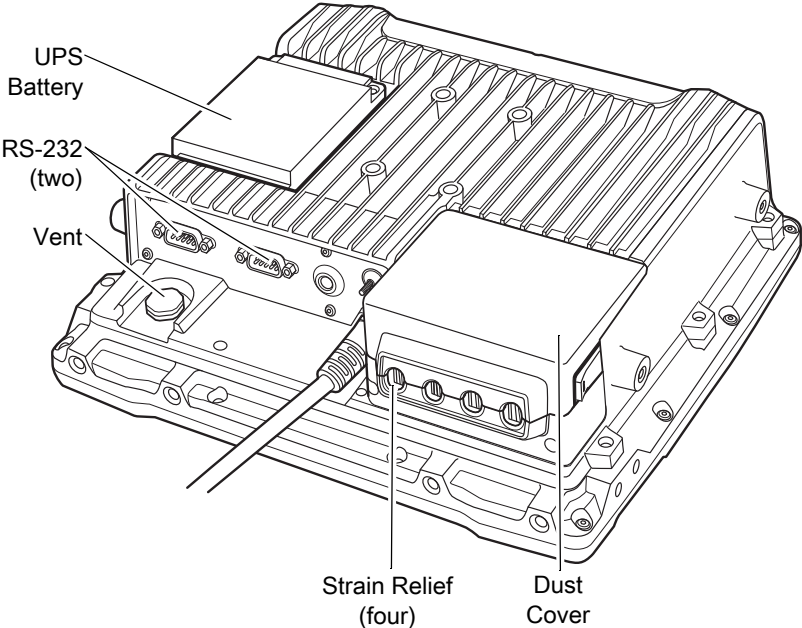
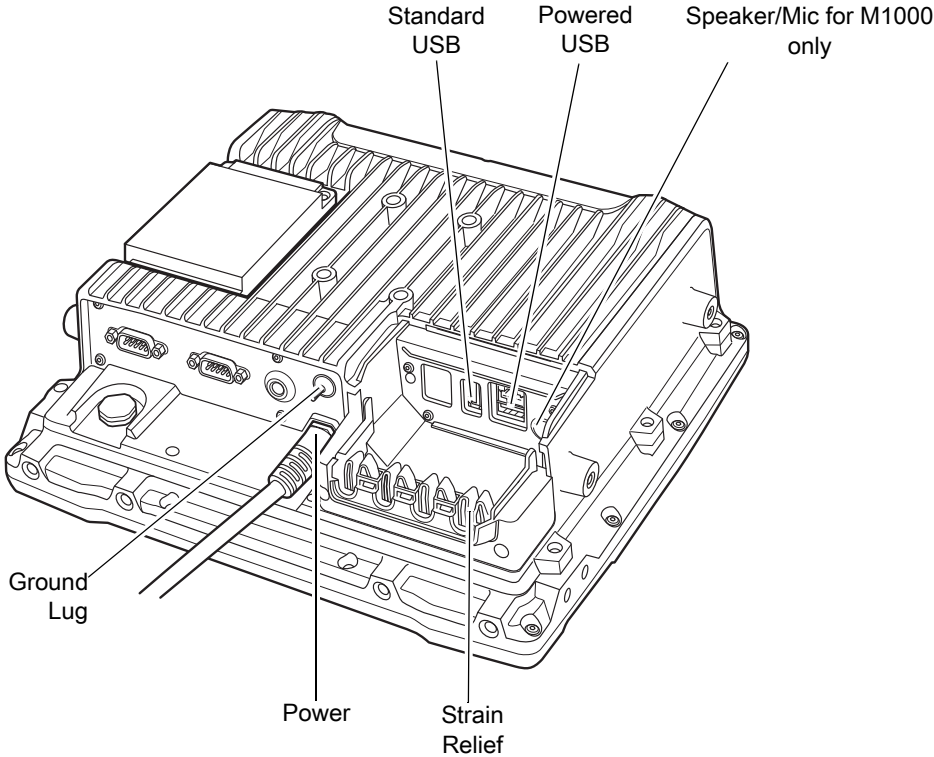


Figure 4 VC8300 Back View without Dust Cover



Front Keys and LED Indicators

The device has the following front bezel keys and LEDs:

Front Keys

Table 1 VC8300 8" Front Keys

Front	Function
Power	Powers the device on or off. Use to reset the device. See Resetting the Device on page 54.
Diamond Key	Opens the special character SIP.
Blue Modifier Key	Modifies programmable macro keys allowing for an additional six programmable keys. Press the Blue Modifier key twice to lock the key on and to unlock, press the key once again.
Function Keys	Function keys perform special, custom-defined functions within an application. These keys are accessed by pressing one of the dedicated function keys on the keyboard, or through the appropriate [Blue] key sequence.
Keyboard	Use to enter text.
Bar Codes	
Pairing Bar Code	Pair peripheral Bluetooth scanners to the VC8300.
Unpairing Bar Code	Un-pair peripheral Bluetooth scanners to the VC8300.
Speaker	
Front Speaker	Located on front bezel.

LED Indicators

Table 2 LED Indicators

Indicator	State	Description
Power	Off	The device has no power and cannot be turned on.
	Amber	The device has power and can be turned on.
	Flashing Amber	The unit is pre-heating.
	Solid Green	The unit is ON, operating from external power.
	Slow Flashing Green	The device is running with UPS/Internal Battery power, no external power available.
	Fast Flashing Green	The device is in Sleep mode. Press Power button to wake the device.
Warning	Off	No battery or charger faults.
	Solid Red	Battery temperature is out of range for charging.
	Blinking Red	Any other battery/charging fault, e.g. communication fault, charge timeout, or defective battery pack.

Powering Up the Device

Power up the device after connecting all of the devices.

To power up the device, connect to an appropriate power supply and press the Power button (see [Figure 1](#)) or the ignition signal.



CAUTION: Make sure there is a suitable disconnecting device such as a power switch or circuit breaker in the power supply circuit. See [Installing the Device on page 24](#) for more information.

Powering Down the Device

Always shut down the device as follows:

1. Press the Power button until the menu appears on the screen.
2. Touch **Power off**.

Setting Up WLAN

To connect to a WLAN, see [Scanning and Connecting to a Wi-Fi Network on page 104](#).

Device Settings

The user can configure the device setting:

- Date and Time settings. See [Display Setting on page 182](#).
- Display settings, see [Display Setting on page 182](#).
- Sound settings, see [General Sound Setting on page 184](#).

Heater Status

The device offers a unique heater system that enables continuous operations in freezer environments. See [Heater Control on page 71](#) for information about the heater settings.

Battery Management

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

Battery status indicates that the battery is discharging and **Battery level** lists the battery charge (as a percentage of fully charged).

Monitoring Battery Usage

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


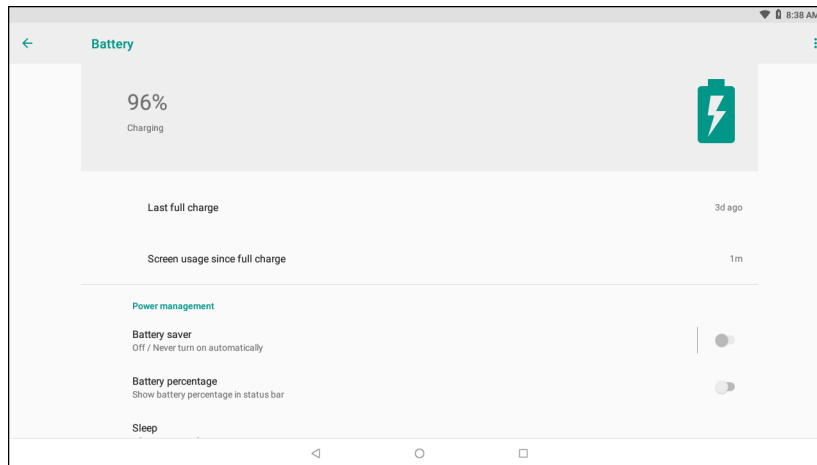
1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **Battery**.

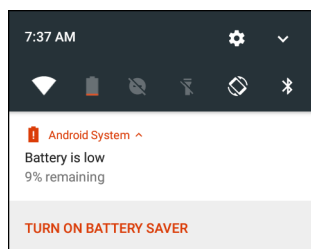
Figure 5 Battery Screen

The **Battery** screen lists the applications using the battery. The discharge graph at the top of the screen shows the rate of the battery discharge since last charged (short periods of time when connected to a charger are shown as thin green lines at the bottom of the chart), and how long it has been running on battery power.

Touch an application in the **Battery** screen to display details about its power consumption. Different applications display different information. Some applications include buttons that open screens with settings to adjust power use.

Low Battery Notification

When the battery charge level drops below 30%, the device displays a notice to connect the device to power. The user must connect the device to external power.

Figure 6 Low Battery Notification

When the battery charge drops below 15%, the device displays a notice to connect the device to power. The user must connect the device to external power.

When the battery charge drops below 7%, the device turns off.

The user must connect the device to external power.

Turning Off the Radios

To turn off all the radios:

1. Press the Power button until the menu appears.
2. Touch **Airplane mode**. The airplane icon ✈ appears in the Status bar indicating that all the radios are off.

Installation

Introduction

This chapter provides instructions on installing the device.

Overview

The device can be installed in a variety of ways:

- Position the device horizontally on a desk or mounted on a vehicle console.
- Wall mount the device using the optional wall mount (see [VC8300 Mounting Accessories on page 123](#)).
- Overhead mount on a lift truck cage using mounting hardware.

Depending on the vibration resistance and pivoting demands, mounting brackets, clamp feet or RAM mount elements can also be used to attach the device. Contact your Zebra sales office to find out more about the range of available installation options.



WARNING: The unit could fall during transit or installation/mounting and cause injury. Always ensure that there are two people available when installing or removing the device.

Mounting Instructions

Follow and retain the mounting instructions included with assembly kit when installing the device. See Safety on page 17 for safety instructions.

Installing the Device

Electrical Installation

There are various electrical potentials when installing the unit on a vehicle such as a forklift.

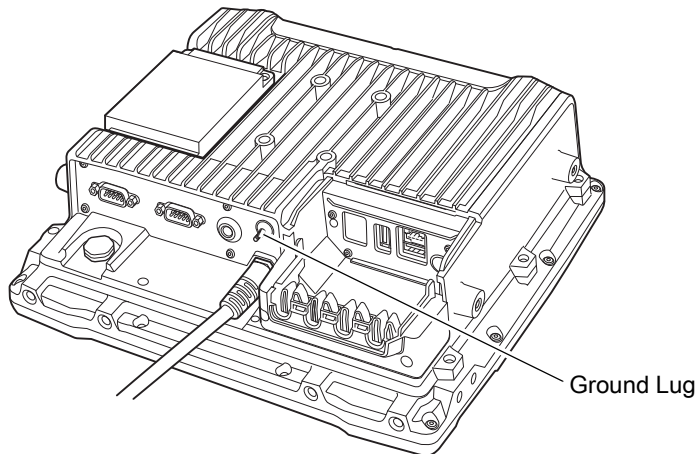


WARNING: Most electrically driven forklift vehicles have floating chassis connected to neither DC+ or DC-. However, electrical faults can cause the battery + or - to be connected to the chassis via low resistance paths. All connected peripherals must be completely isolated.

The device accepts DC power sources with a minimum of 10 VDC nominal and 48 VDC nominal. A Power Pre-regulator is required for voltages above 48 VDC nominal.

Applying a voltage above 48 VDC nominal without the pre-regulator or reversing polarity may result in permanent damage to the device and voids the product warranty.

Figure 7 Ground Lug



CAUTION: Attach the device connecting cable as close to the battery as possible. Connecting the device to large electrical loads, such as converters for the forklift motor may result in random restarts, malfunctions and/or irreparable damage to the device.

To connect devices fed by other power sources to the device, such as printers, power up the peripheral devices at the same time or after the device to avoid start-up problems, malfunctions or irreparable damage to the device.

Wiring Guidelines

The metal chassis of the device is equipped with a ground lug (located on the underside adjacent to the power cable) to provide additional ground to the vehicle. It is strongly recommended that a grounding strap is used to connect the ground stud on the vehicle-mount to a solid, reliable contact point on the main portion of the vehicle chassis. It must not be connected to battery negative or terminal block.

As with other vehicle cables, carefully consider the routing of the ground strap to ensure it does not pose a hazard to the operator or the safe operation of the vehicle. If necessary, secure the ground strap with cable ties or some other mechanical means to prevent loops or loose lengths of wire from catching on stationary items when the vehicle is in motion.

Before installing the cables between the mount and other devices, consider the following:

- Ensure that drilling holes do not damage the vehicle or its wiring.
- Protect cable runs from pinching, overheating and physical damage.
- Use grommets to protect cables that pass through metal.
- Use plastic straps and tie-downs to secure cables and connectors in their desired location, away from areas where they may get snagged or pulled.
- Keep cables away from heat sources, grease, battery acid and other potential hazards.
- Keep cables away from control pedals and other moving parts that may damage the cables or interfere with the operation of the vehicle.



IMPORTANT: Make sure the cables run inside the roll cage of the vehicle.

If the device is installed in an environment where earth ground is present such as a vehicle with metal wheels running on a metal track, or is powered by the AC/DC adapter in a permanent installation, the ground lug must be connected to the ground structure.

Wiring Vehicle Power to the VC8300



WARNING: Applying voltage above the input voltage rating or reversing polarity may result in permanent damage to the VC8300 and void the product warranty.

An extension power cable is used to wire the VC8300 to the truck battery (order cable separately, see [Accessories on page 120](#)). Wire this cable to a filtered, fused (15A max) accessory supply on the vehicle. Follow the installation instructions supplied with the extension cable.

Additional wiring (minimum 14 gauge), connectors or disconnects used should be rated for at least 300 VDC, 15A.

When connecting the extension power cable:

- If a power extension cable with ignition sense is used, ensure that the ignition sense wires (18AWG wires in red and black leads) and the power wires (14AWG in red and black leads) are reliably secured away from each other, or are separated with reliably secured certified insulation. Minimum 2.8 mm distance, or 0.4 mm distance through insulation is required for the separation.
- The red lead of the 14AWG power cables attach to the vehicles battery positive terminal. The 14AWG black lead connects to the vehicle's battery negative terminal. This should be connected to a proper terminal block and not to the vehicle body. An optional grounding strap wire (sourced separately) may be connected to the ground lug of the VC8300 terminal connector bay and to the vehicle chassis.
- You may have the option to connect power before or after the key switch. Though the VC8300 is equipped with a UPS, a proper shut down is recommended using the Power Off procedure. If it is wired after the key switch, the operator must shut down the VC8300 using the Power Off procedure before turning off the vehicle. If it is wired before the key switch, then to avoid excessive drain on the vehicle battery, either the operator should shut it down when the vehicle is to be left off for an extended period, or the ignition cable shut down wire should be connected and the VC8300 configured to shut down automatically.
- An appropriate fuse type must be used with the power extension cable according to the installation instructions. For main power cable, use 3AB, 15A, 250V, slow blow fuse. For ignition sense input, use 3AB, 0.3A, 250V, slow blow fuse.



NOTE: The VC8300 supports the ignition sense feature that detects when the ignition switch or key switch is On or Off to allow automatic computer start up or shut down (with delay as needed).

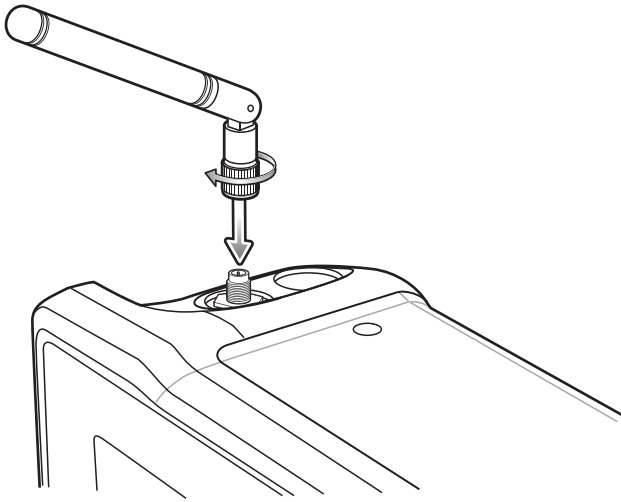
When wiring the ignition sense wires (18AWG in red and black), the red 18AWG wire is connected to a positive DC voltage source switched on by the ignition. The black 18AWG wire is connected to ground reference of this switched ignition source.



External Antenna Installation

To install an external antenna:

1. Align the antenna connector with the connector on top of the VC8300.
2. Insert the antenna connector onto the VC8300 connector.
3. Tighten the antenna connector.

Figure 8 Installing External Antenna



4. Swipe up from the bottom of the Home screen and touch **VC Setting** .
5. Touch **Choose Antenna**.
6. Touch **External Antenna**.
7. Touch .

Positioning the VC8300 in the Vehicle

When positioning the VC8300 on the vehicle:

- The driver's field of view must be kept free.
- Plan for sufficient space if a keyboard and scanner are installed with the VC8300.
- No part of the VC8300 system may project beyond the vehicle.

Overview of the Assembly Steps

Before fastening the VC8300 to the vehicle:

- Configure shut down automation.
- Prepare the forklift such as ignition connection and correct voltage.
- It is recommended to fasten the bracket to the vehicle and then install the VC8300 to the bracket.

Cable Dust Cover

For the dust cover location, see [VC8300 Back View with Dust Cover on page 20](#).



CAUTION: Turn on external peripheral devices with their own power supply at the same time or after the VC8300. If this is not possible, ensure that the VC8300 is adequately protected from power leakage caused by an external device.

Strain Relief



CAUTION: For safety reasons, install the supplied cable cover for the external ports prior to using the VC8300.

After the VC8300 and bracket are fastened, prepare the strain relief as follows:

1. Install the cables loosely on the strain relief rail (see [Figure 4 on page 20](#)).
2. As far as possible, route cables leading to or away from the unit next to one another without crossing.
3. Fasten the cables into the strain relief rail precisely at the positions at which the cable openings in the cable cover are located.

Installing the VC8300 on a Forklift

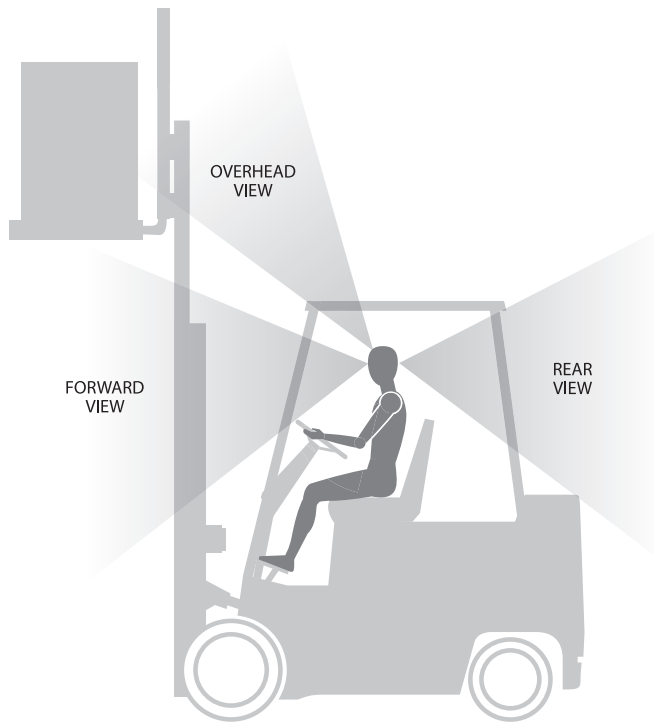


CAUTION: Tighten peripherals with thumbscrews by hand only. Do not use tools for tightening thumbscrews.



NOTE: If installing peripherals, allow enough space when selecting a mounting location.

1. Attach the desired mount to the VC8300. See VC8300 Mounting Accessories on page 123 for detailed mounting options and instructions.
2. Attach the mounted VC8300 to the vehicle and position in a location that does not obstruct the operator's view.
3. If using an external antenna, connect antenna in a vertical position to the VC8300.
4. Connect peripherals to the VC8300. Place the cables in the strain relief brackets inside the dust cover and replace the dust cover (see [Figure 3 on page 20](#)).
5. Connect the VC8300 to the vehicle DC supply.
6. Press the **Power** button to turn the device On or Off (see [Figure 2 on page 19](#)).

Figure 9 View Obstruction Considerations

Forklift Battery Replacement Conditions

The VC8300 maintains normal function of applications and connections during and after forklift battery replacement.

Replace the forklift battery at any point during a shift and/or while the VC8300 is fully running.

The forklift battery may be replaced under following condition: VC8300 external temperature range: -30°C to $+50^{\circ}\text{C}$ (-22°F to 122°F).

During forklift battery replacement (VC8300 is running on UPS battery), both Android and the VC8300 are monitoring remaining UPS battery capacity. The default Low Battery notification threshold is set to 30%. The Critical Battery threshold is set to 7%. If UPS battery is discharged below 7%, the VC8300 automatically shuts down.

Starting from Cold Soak

The VC8300 can start up from a saturated cold soak at -30°C (or above) internal VC8300 temperature when a valid external DC power source is present.

The VC8300 design minimizes wait time from -30°C cold soak to load the OS and have internal heaters to assist system warm up.

From a -30°C cold soak condition, the VC8300 battery heater may be activated to warm the UPS battery to an acceptable charging temperature if charging is needed. The conditions and time to heat the battery are managed by the system. The OS load time and VC8300 ready for use time is independent of warming the battery.

Pre-Heat Mode

When the device is powered down or suspended and the system temperature is below -25°C (-13°F), the device enters pre-heat mode when the user presses the power key. This warms up critical internal components with the heater elements prior to boot up.

When in Pre-heat mode the Power LED blinks amber.

The pre-heat mode lasts no longer than 15 minutes. The freezer configuration spends less time in Pre-heat mode due to the additional Touch Panel heater.

The device remains powered down or suspended during Pre-heat mode. Once the system reaches the adequate temperature, the device automatically boots up. The user is not required to press the power button.

The device does not enter Pre-heat mode if it is outside the operating temperature range (-30°C to 50°C (-22°F to 122°F)).

Installing the Power Pre-Regulator



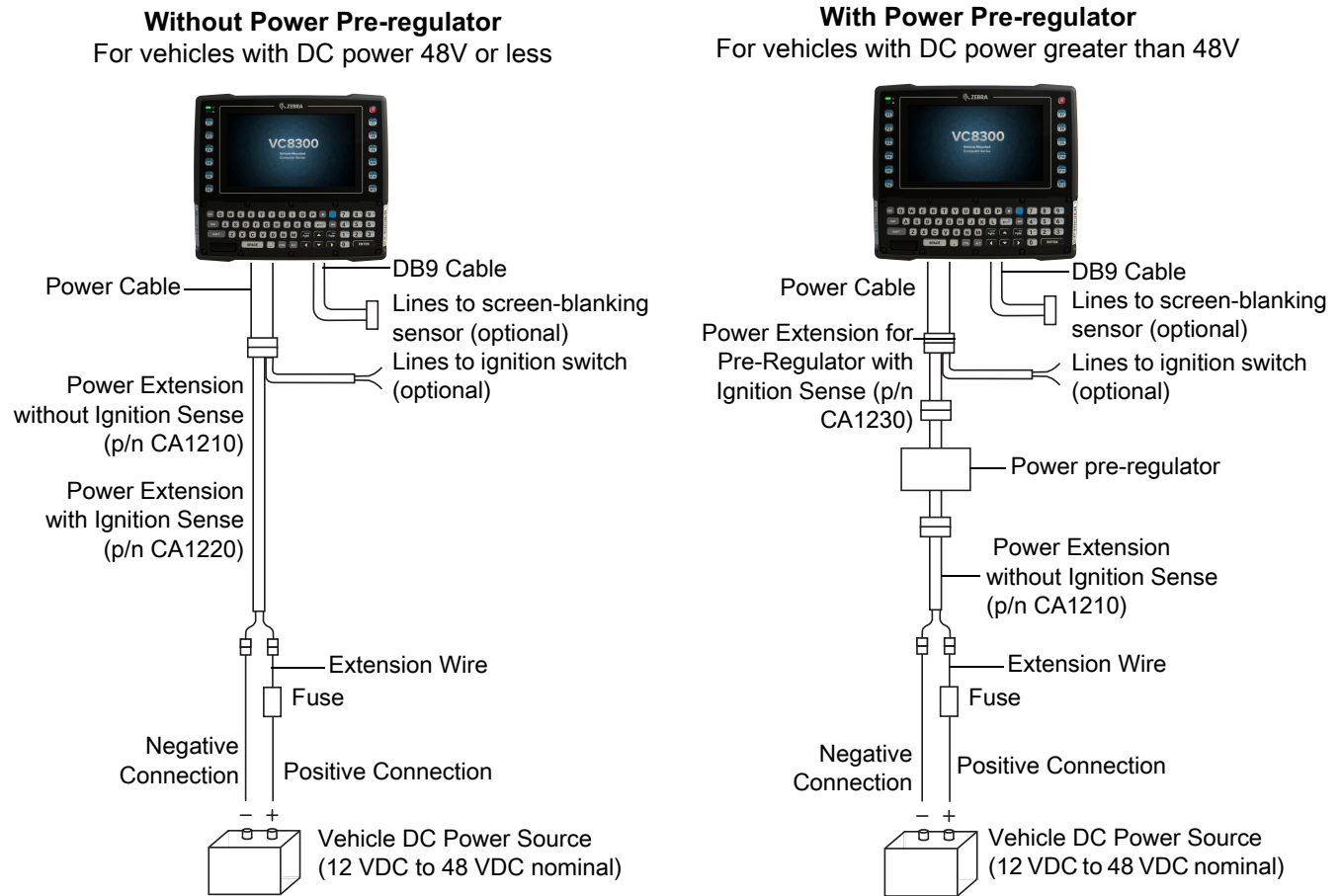
IMPORTANT: The Zebra power extension cable positive lead is red and the negative lead is black.

It is recommended that all connections be secured with electrical tape or heat shrink to prevent contaminants from degrading the connection.

To install the power pre-regulator:

1. Attach the pre-regulator cable male connector to the Zebra power extension cable which is installed on the vehicle.
2. Connect the pre-regulator cable female connector either directly to the VC8300 power cable, or to the power extension cable. See [Figure 10](#).

Figure 10 Connections To Vehicle DC Supply



Non-Vehicle Installations

Using AC power, the VC8300 Vehicle-Mount Computer can be mounted at fixed locations adjacent to cross-dock doors, manufacturing stations, or in offices.

Use the 100/240 VAC Power Supply (p/n PS1450) to power the computer from an AC source.

IMPORTANT: The AC/DC power supply is only intended for use at room temperature condition such as an office environment. Power On/Off with Ignition

The VC8300 is equipped with an ignition sense feature which shuts down the VC8300 when the vehicle ignition is turned off and can power on the VC8300 when the ignition is switched on. To use this feature, a power extension cable with ignition sense wires must be used and installed properly on the vehicle.

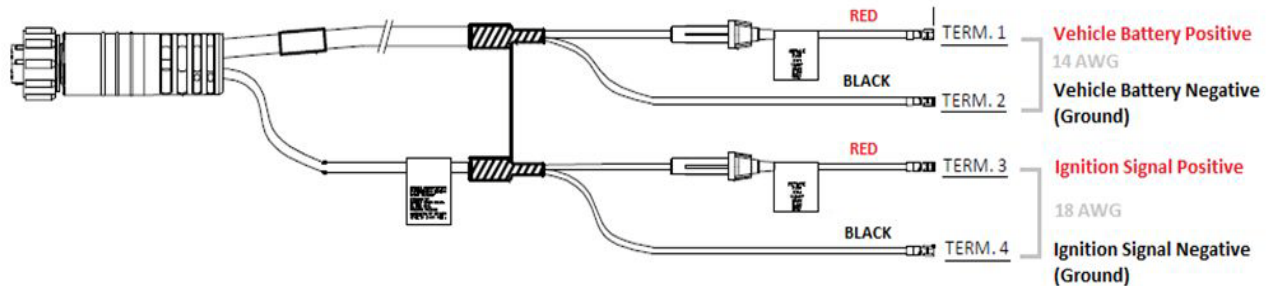
The cable in [Figure 11](#) is the power extension cable (p/n CA1220) with two wires used to connect to vehicle ignition. The red and black leads of the two 18AWG wires that connect to the key switch of the ignition and ground, respectively. Once the wires are connected, the VC8300 may switch on or off depending on the state of the vehicle ignition key. See [VC Settings on page 88](#) to select power settings.

IMPORTANT: When connecting to an ignition switch using the power extension cable with ignition sense wires, ensure that the wires of different polarities are reliably secured away from each other, or are separated with reliably secured certified insulation. A minimum distance of 2.8mm (or 0.4mm distance through insulation) is required for the separation.

The thinner wires (18 AWG) are used for Ignition Sense wires while the thicker wires (14AWG) are used for Vehicle Power and Ground. Identify them carefully and **Do Not** confuse them.

An appropriate fuse type must be used with the power extension cable according to the installation instructions. For the main power cable, use 3AB, 15A, 250V, slow blow fuse. For ignition sense input, use 3AB, 0.3A, 250V, slow blow fuse.

Figure 11 Power Extension Cable Kit with Optional Ignition Sense Wires (p/n CA1220)

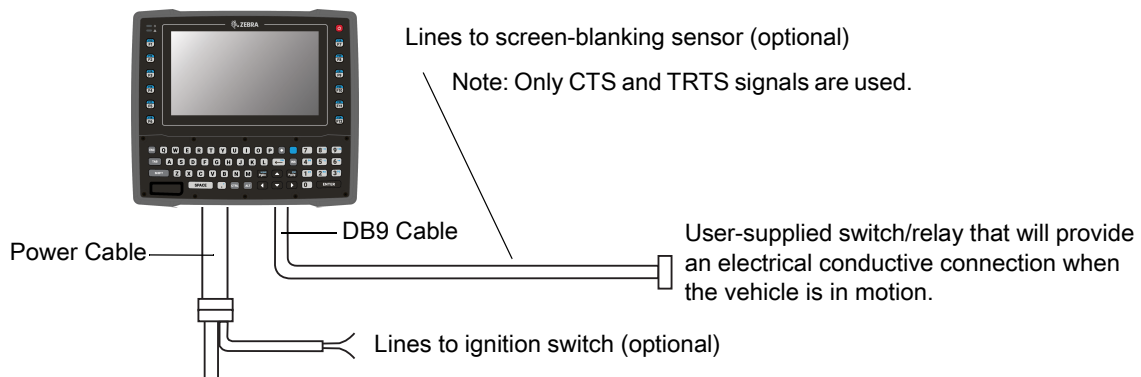


Screen Blanking Wiring

Connecting Switch for Screen Blanking

To use Screen Blanking, connect one of the two DB9 serial ports (using CA1300 Screen Blanking cable) on the VC8300 to a switch. Activate this switch electrically (e.g. motion sensor) or mechanically (e.g. pedal switch) when the vehicle is in motion.

Figure 12 Connecting the Switch to the DB9 Cable



IMPORTANT: For customers migrating to the VC8300 from a 8515, 8525, 8535 vehicle mount computer or a 753x hand-held computer cradle:

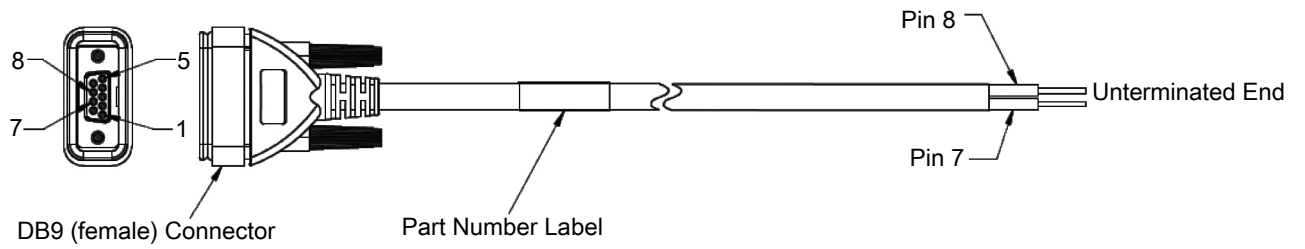
If the screen blanking feature was used previously, ensure that you are no longer feeding the screen blanking signals to the VC8300 main DC power cable. Rewire the screen blanking inputs to the VC8300 DB-9 serial port through the DB-9 screen blanking cable. In previous generations of vehicle-mount computers, the screen blanking signals were fed in to the terminal through 2 of the 4 wires in the CPC connector of the DC power cable. This no longer applies for the VC830000.

The screen blanking feature makes use of either one of the DB-9 ports to monitor electrical relay closure. When enabled, the CTS/RTS pins of the DB9 port are continuously monitored by the screen blanking application. See [Figure 13](#) for pin configuration.

When the vehicle is in motion, the switch closes the circuit, allowing data packets to be sent or received through the RTS and CTS pins. The computer detects that the circuit is closed and turns off the screen.

When the vehicle is not in motion, the switch opens the circuit, preventing data packets from being sent or received. The computer detects that the circuit is open and turns on the screen.

Figure 13 Screen Blanking DB9 Pin Configuration



Using the Device

This chapter explains the buttons, status icons, and controls on the device, and provides basic instructions for using the device including resetting the device and entering data.

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 > Location access**.
 - 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

The Home screen displays when the device turns on. Depending upon the configuration, the Home screen might appear different. Contact your system administrator for more information.

After a suspend or screen time-out, the Home screen displays with the lock sliders. Touch the screen and slide up to unlock. For screen locking information see [Un-Locking the Screen on page 52](#).

Figure 14 Home Screen

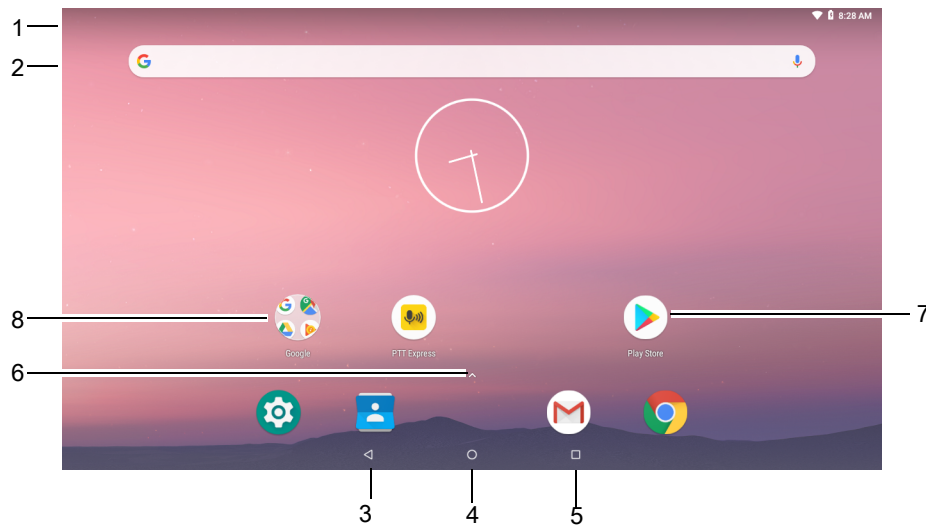


Table 3 Home Screen Items

Item	Description
1 — Status Bar	Displays the time, status icons (right side), and notification icons (left side). For more information see Status Bar on page 35 and Managing Notifications on page 38 .
2 — Widgets	Launches stand-alone applications that run on the Home screen. See App Shortcuts and Widgets on page 41 for more information.
3 — Back	Displays the previous screen.
4 — Home	Displays the Home screen.
5 — Recent Button	Displays recently used applications.
6 — All Apps	Opens the APPS window.
7 — Shortcut Icons	Opens applications installed on the device. See App Shortcuts and Widgets on page 41 for more information.
8 — Folder	Contains apps.

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

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 15 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 4 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.
	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.
	Indicates that the Blue key is pressed.
	Indicates that the Blue key is locked.
	Indicates that the ALT key is pressed.

Table 4 Status Icons (Continued)

Icon	Description
	Indicates that the ALT key is locked.
	Indicates that the CTRL key is pressed.
	Indicates that the CTRL key is locked.
	Indicates that the Shift key is pressed.
	Indicates that the Shift key is locked.

Notification Icons

Table 5 Notification Icons



















Icon	Description
	Main battery is low.
	More notifications are available for viewing.
	Data is syncing.
	Indicates an upcoming event.
	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 via USB cable.
	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.
	Headset is connected to the device.
	PTT Express Voice client status. See the PTT Express PTT Notification Icons for a complete list.

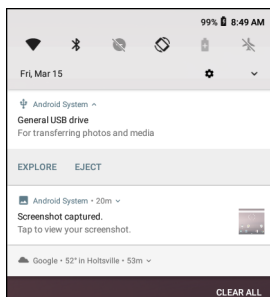
Table 5 Notification Icons (Continued)

Icon	Description
	Indicates that RxLogger app is running.
	Indicates the RS6000 is connected to the device.
	Indicates the RS507 or 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 16 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, 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**.

Quick Access Panel

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

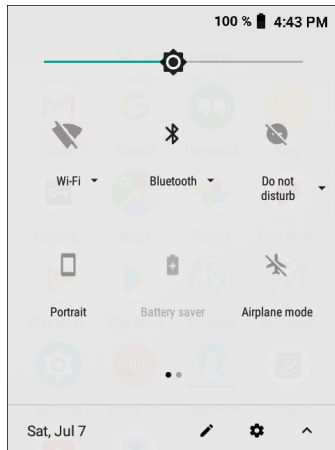
Figure 17 Quick Settings Bar



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 18 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 saver - Turn Battery saver mode on or off. When Battery saver mode is on the performance of the device is reduced to preserve battery power.
- Invert colors - Invert the display colors.
- 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.
- Night Light - Tint the screen amber to make it easier to look at the screen in dim light. Set Night Light to turn on automatically from sunset to sunrise, or at other times.
- Nearby - Helps find and interact with services and devices close to the device.
- 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.



Editing Icons on Quick Settings

The first several setting tiles from the Quick Access panel become the Quick Settings bar.



To move a setting tile:

1. Open the Quick Access panel.
2. Touch .
3. Touch and drag a setting tile to another location.
4. Release the tile.
5. Touch  to save tiles and return to the Quick Access panel.

To add a setting tile:

1. Open the Quick Access panel.
2. Touch .
3. Slide the Quick Settings panel up to reveal additional tiles.
4. Touch and drag a setting tile from the **Drag to add tiles** area to the main area.
5. Release the tile.
6. Touch  to save tiles and return to Quick Access panel.

To remove a setting tile:

1. Open the Quick Access panel.
2. Touch .
3. Touch and drag a setting tile to the **Drag here to remove** area.
4. Release the tile.
5. Touch  to save tiles and return to Quick Access panel.

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.

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:

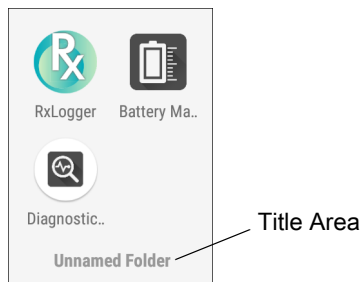
1. Go to the desired Home screen.
2. Touch and hold one app icon.
3. Drag the icon and stack on top of another icon.
4. Lift and release.


Naming Folders

To name a folder:

1. Touch the folder.

Figure 19 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. Touchscreen usage includes Glover and Finger (with or without screen protector, or Finger Only modes.

- 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).

Integrated Keyboard

The device is available with an integrated keyboard in either QWERTY or AZERTY alphanumeric keyboard layout. It features 54 keys, 12 direct function keys, and a power button.

Most of the keys on the keyboard operate much like a desktop computer. Where a key or key function is not consistent with the keyboard, those differences are described in the following sections.

There are a number of modifier keys that provide access to additional keys and system functions.

See [The Keyboard Backlight on page 184](#) for information on adjusting the keyboard backlight.

Figure 20 Integrated Keyboard



Table 6 Key Descriptions

Key	Function
Regular Keys	
The Arrow Keys	The arrow keys are located near the bottom of the keyboard, and are represented on the keyboard as triangles pointing in different directions. The keys move the cursor around the screen in the direction of the arrow: up, down, left, and right. The left arrow key should not be confused with the backspace DEL key which is depicted as a left arrow. The cursor is the flashing box or underline character that indicates where the next character you type will appear.
The DEL Key	The DEL key (represented on the keyboard as an arrow pointing left) is the backspace key that moves the cursor one character to the left, erasing the previous key stroke. The [Blue] + DEL keys erase the character at the current cursor position.
The SHIFT Key	The SHIFT key is used to display uppercase alpha characters. ↑ appears in the status bar. Pressing the SHIFT key a second time locks the keys that all alpha characters are uppercase. ↓ appears in the status bar. Press the SHIFT key again to return to the default keypad functions.

Table 6 Key Descriptions (Continued)

Key	Function
The CTRL and ALT Keys	The CTRL and ALT keys modify the function of the next key pressed and are application dependent. C or A appears in the status bar. Pressing the CTRL or ALT key a second time locks the keys. C or A appears in the status bar. Press the key again to return to the default keypad functions.
The TAB Key	Typically, the TAB key moves the cursor to the next field to the right or downward.
The ESC Key	Generally, this key is used as a keyboard shortcut to close the current menu, dialog box, or activity.
The SPACE Key	Pressing this key inserts a blank space between characters. In a dialog box, pressing the SPACE key enables or disables a check box.
The INS Key	The INS key inserts a character at the cursor position.
Function Keys	
F1 - F12	Function keys perform special, custom-defined functions within an application. These keys are accessed by pressing one of the dedicated function keys on the keyboard, or through the appropriate [Blue] key sequence. To access the blue function keys, first press the [Blue] key followed by the appropriate function key. Function keys can be used with the operating system or another application.
Programmable Keys	
P1 - P5	The device keyboard is equipped with a series of programmable keys that can be programmed to replace frequently used keystrokes, along with the function of executable keys like the ENTER key, the [BACKSPACE] key, any function key, arrow key, etc.
Special Keys	
Diamond Key	The Diamond key provides access to commonly used symbolic characters. Pressing the key brings up the soft input panel (SIP) on-screen keyboard, with symbols mapped to each key.
Blue Key	The [Blue] key provides access to additional keys. These functions are color coded in blue print on the key caps.

Soft Input Panel

The SIP provides additional commonly used symbolic characters that do not appear on the integrated keyboard. Press the Diamond key to show the SIP. Press the Diamond key a second time to lock the SIP in place. Press the Diamond key a third time to hide the SIP. Press and hold up arrow/down arrow key and slide up and down to re-position the SIP on the screen.

Figure 21 Soft Input Panel

=	+	-	×	÷	()	\	/	~	&	£
[]		{	}	€	?	;	:	#	`	'
↑↓	<	>	_	"	*	^	%	\$	#	!	↑↓


Virtual Keyboards

The device comes with the following virtual keyboards that can display on the screen:


- Gboard Keyboard
- Enterprise Keyboard.



By default, the virtual keyboard do not appear when the cursor is placed in a text field.

To use a virtual keyboard:

1. Touch in a text field.
2. Touch  to enable virtual keyboards.
3. In the **Change keyboard** dialog box, touch the **Show virtual keyboard** switch. The selected keyboard displays.

To switch a virtual keyboard:

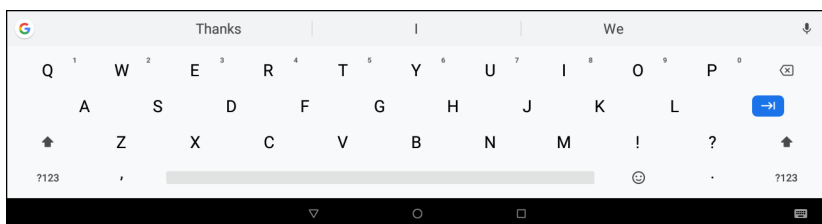
1. Touch in a text field.
2. Touch  to switch virtual keyboards.
3. In the **Change keyboard** dialog box, touch a virtual keyboard radio button. The selected keyboard displays.

When there are multiple virtual keyboards and language keyboards, use the  (GBoard keyboard) or  (Enterprise keyboard) to cycle through the available keyboards.

Using the GBoard Keyboard

The GBoard keyboard is a default keyboard that is supplied with the device. The keyboard can support multiple languages. See [Configuring the GBoard Keyboard on page 193](#) for information on adding and enabling language keyboards.

Figure 22 GBoard Keyboard





Editing Text

Edit entered text and use menu commands to cut, copy, and paste text within or across applications. Some applications 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.

- Double tap the Shift key to lock the keyboard into Shift mode, touch one or more capital letters or symbols to enter them, and then touch the Shift key to return to the lowercase keyboard.
- Touch  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.

Using the Enterprise Keyboard

The Enterprise Keyboard contains the following keyboards:

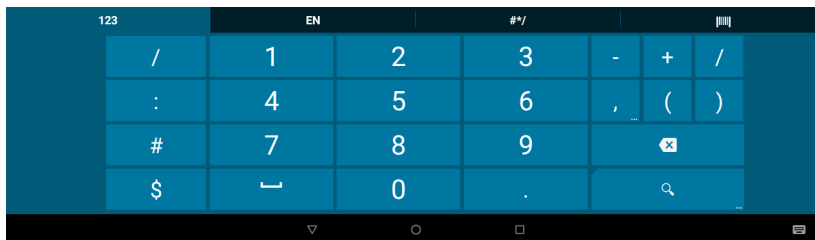
- Numeric
- Alpha
- Special characters
- Data capture.

See [Configuring the Enterprise Keyboard on page 193](#) for information on configuring the Enterprise Keyboard.

Numeric Tab

To access the numeric keyboard, touch the **123** tab. The keys displayed vary on the app being used. For example, an arrow displays in **Contacts**, however **Done** displays in **Email** account setup.

Figure 23 Numeric Keyboard



Alpha Tab

To access the alpha keyboard, touch the **EN** tab.



IMPORTANT: The tab displays the language code for the current keyboard language.

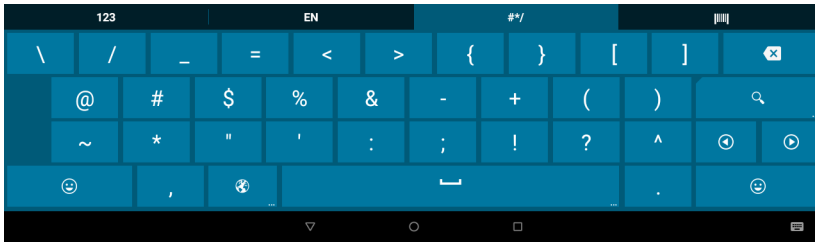
Figure 24 Alpha Keyboard



Special Character Tab

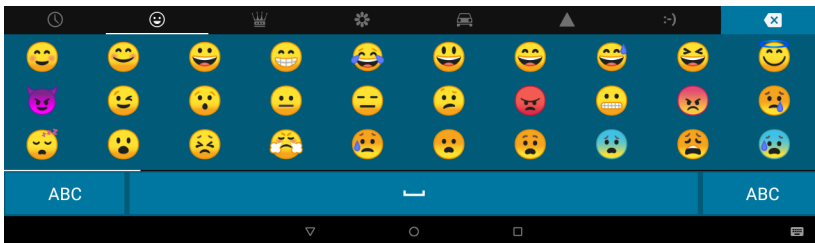
To access additional characters, touch the **#*/** tab.

Figure 25 Symbols Keyboard



Touch 😊 to enter emoji icons in a text message.

Figure 26 Emoji Keyboard

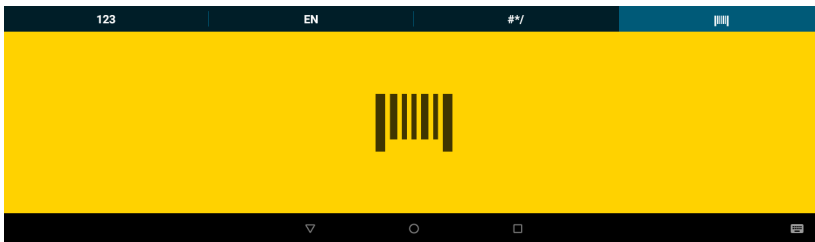


Touch **ABC** to return to the Symbols keyboard.

Scan Tab

The Scan tab provides an easy data capture feature for scanning barcodes.

Figure 27 Scan 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 7 Apps














Icon	Description
	Battery Manager - Displays battery information, including charge level, status, health and wear level.
	Bluetooth Pairing Utility – Use to pair a Bluetooth scanner with the device by scanning a barcode.
	Calculator - Provides the basic and scientific arithmetic functions.
	Calendar - Use to manage events and appointments. GMS/GMS-Restricted only.
	Chrome - Use to access the Internet or intranet. GMS/GMS-Restricted only.
	Clock - Use to schedule alarms for appointments or as a wake-up.
	Contacts - Use to manage contact information. See Contacts for more information.
	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.
	Gmail - Use to send and receive email using a Google email account. GMS/GMS-Restricted only.

Table 7 Apps (Continued)





















Icon	Description
	Google - Launches Google™ search app. GMS/GMS-Restricted only.
	Hangouts - Use to communicate with friends using text messages and photos. GMS/GMS-Restricted only.
	Heater Control - Use to enable heaters when using the device in cold environments. See Heater Control.
	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.
	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.
	Play Store - Download music, movies, books, and Android apps and games from the Google Play Store. GMS/GMS-Restricted only.
	PTT Express - Use to launch PTT Express client for VoIP communication.
	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.
	Settings - Use to configure the device.

Table 7 Apps (Continued)

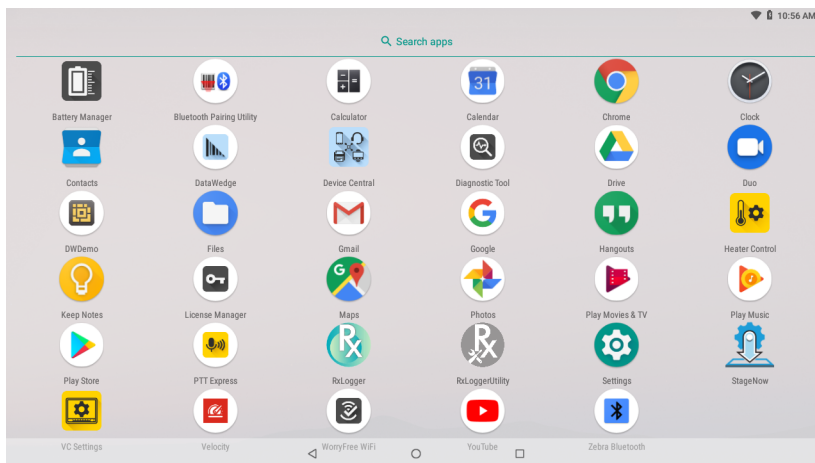
Icon	Description
	StageNow - Allows the device to stage a device for initial use by initiating the deployment of settings, firmware, and software.
	VC Settings - Use to control settings for the device. See VC Settings.
	Velocity - Opens the Ivanti (formerly Wavelink) terminal emulation app.
	Worry Free 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 devices 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 28 APPS Window Example



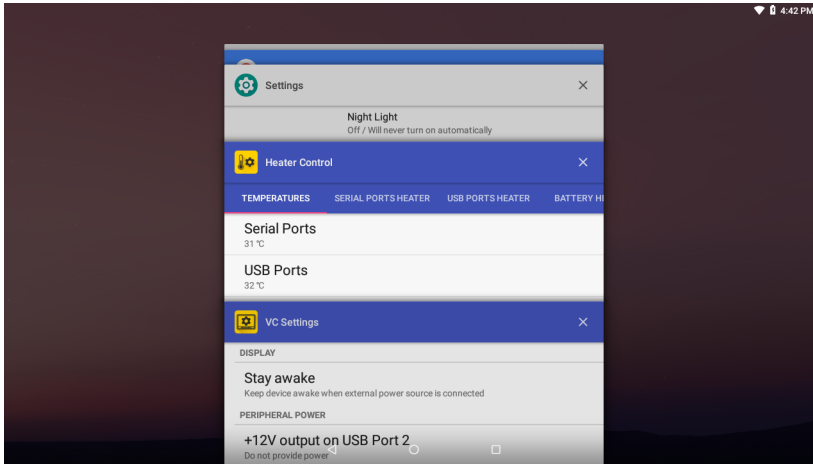
Slide the **APPS** window up or down to view more app icons. Touch an icon to open the app.

Switching Between Recent Apps

To switch between recent apps:

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

Figure 29 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 30 Lock Screen

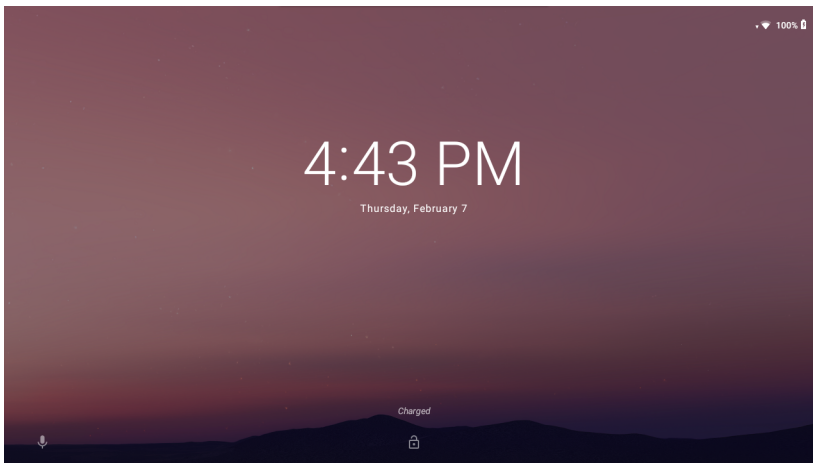


Figure 31 PIN Screen

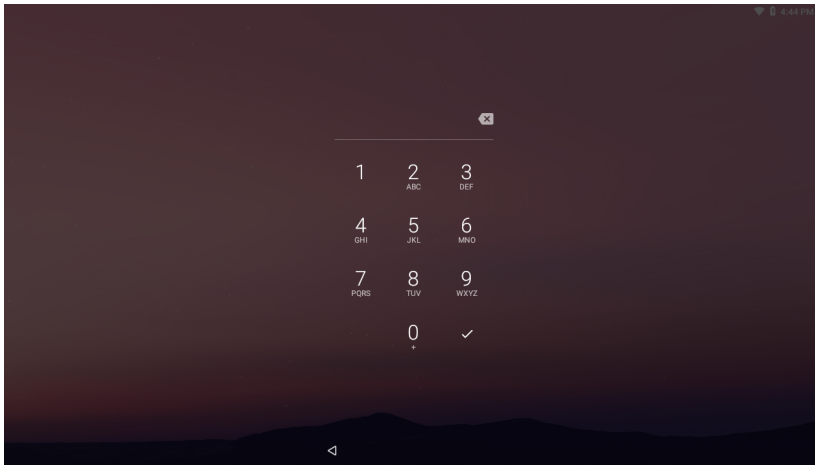


Figure 32 Pattern Screen

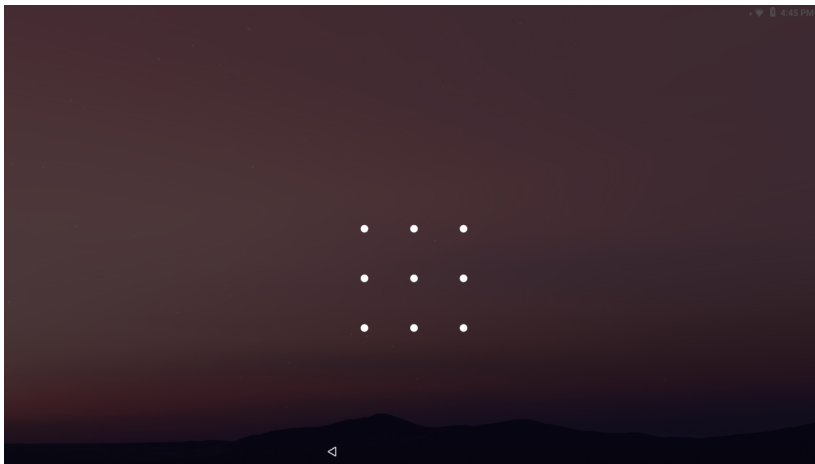
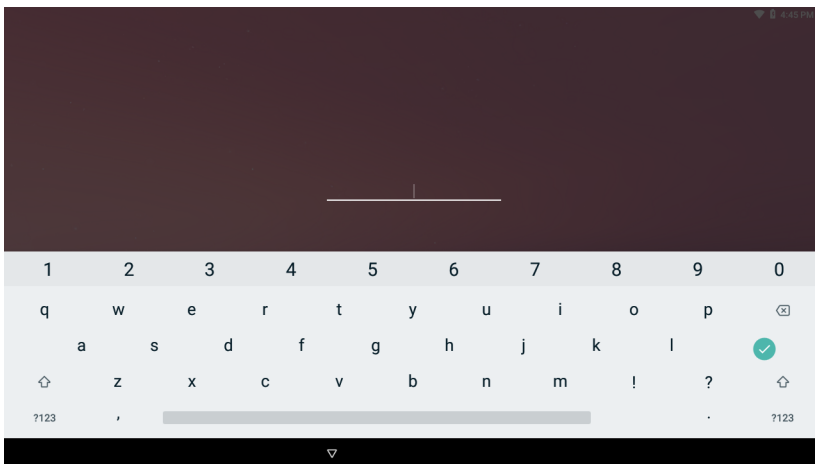


Figure 33 Password Screen



Resetting the Device

There are four reset functions:

- Soft reset
- Hard reset
- Enterprise reset. See [Performing an Enterprise Reset on page 206](#).
- Factory reset. See [Performing a Factory Reset on page 207](#).

Performing a Soft Reset

Perform a soft reset if applications stop responding.

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

Performing a Hard Reset



CAUTION: Performing a hard reset with a USB drive installed in the device may cause damage or data corruption to the USB drive.

Perform a hard reset if the device stops responding.

1. Press and hold the Power button for at least 16 seconds.
2. Release the Power button when the Zebra logo appears.
3. The device reboots.

Suspend Mode

The device goes into suspend mode when you press the Power button or after a period of inactivity (set in the Display settings window).

To wake the device from Suspend mode, press the Power 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.

Transferring Files

To transfer files to the device use a USB drive.

Using a USB Drive



NOTE: Use Media Transfer Protocol (MTP) to copy files between the device (internal memory) and a USB drive.

1. Remove the dust cover on the back of the device.
2. Plug the USB drive into the USB port on the bottom of the device. A notification appears indicating that the device detected the USB drive.

NOTE: Alternately, the **General USB drive** notification touch the down arrow next to **Android System** and then touch **Explore** to open **Files** app.

3. Open **Files**.
4. Touch **General USB Drive** on the left menu to display the contents of the USB drive.
5. Use **Files** to copy files between the drive and the device.

Disconnecting USB Drive

To remove the USB drive:

1. Swipe down from the status bar.
2. In the **General USB drive** notification, touch the down arrow next to **Android System** and then touch **EJECT**.
3. Remove the USB drive from the device.
4. Replace the dust cover.

Apps

This section describes the applications 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 34 Battery Manager Screen

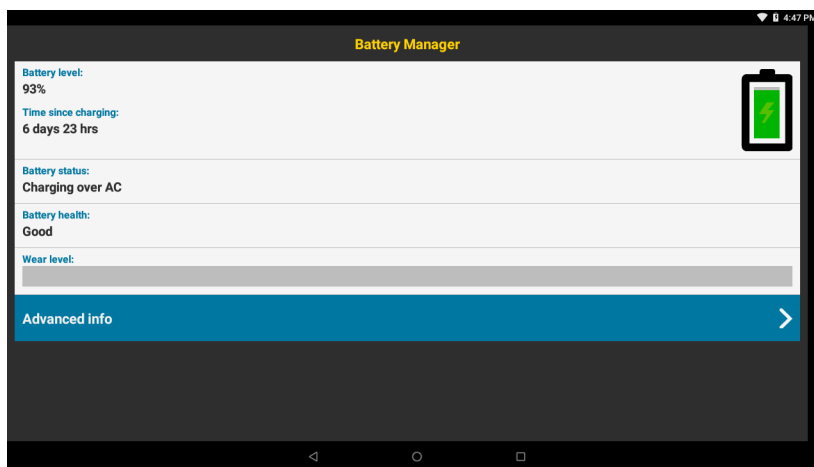






Table 8 Battery Icon Description

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 since charging** - The amount of time since the device began charging.
- **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.
- **Battery present capacity** - Maximum amount of charge that could be pulled from the battery under the present discharge conditions if the battery were fully charged.
- **Battery health percentage** - With a range from **0** to **100**, this is the ratio of “present_capacity” to “design_capacity” at a discharge rate of “design_capacity”.
- **% decommission threshold** - The default % decommission threshold for a gifted battery as 80%.
- **Battery present charge** - Amount of usable charge remaining in the battery at present under the current discharge conditions.
- **Battery total cumulative charge** - The total accumulated charge in all chargers.
- **Battery time since first use** - The time passed since the battery was placed in a Zebra terminal for the first time.
- **Battery error status** - The error status of the battery.
- **Battery usage number** - The health of the battery as a result of charging and discharging. A high number indicates low battery health.
- **Usage decommission threshold** - When the Battery usage number is greater than or equal to the Usage decommission threshold, the battery is past its useful life and should be replaced.
- **App version** - The application version number.

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.

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 35 DataWedge Demonstration Window

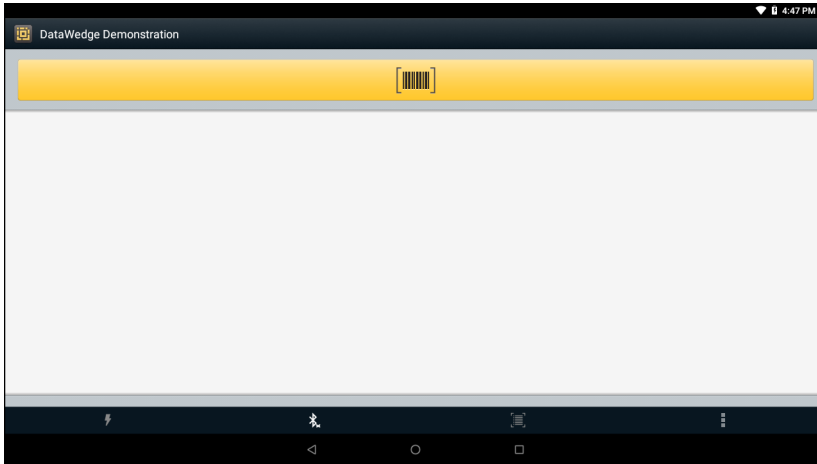


Table 9 DataWedge Demonstration Icons

	Icon	Description
Illumination		Imager illumination is on. Touch to turn illumination off.
		Imager illumination is off. Touch to turn illumination on.
Data Capture		Indicates a USB scanner is connected to the device.
		Indicates a USB scanner is not connected to the device.
		A Bluetooth scanner is connected.
		A Bluetooth scanner is not connected.
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.



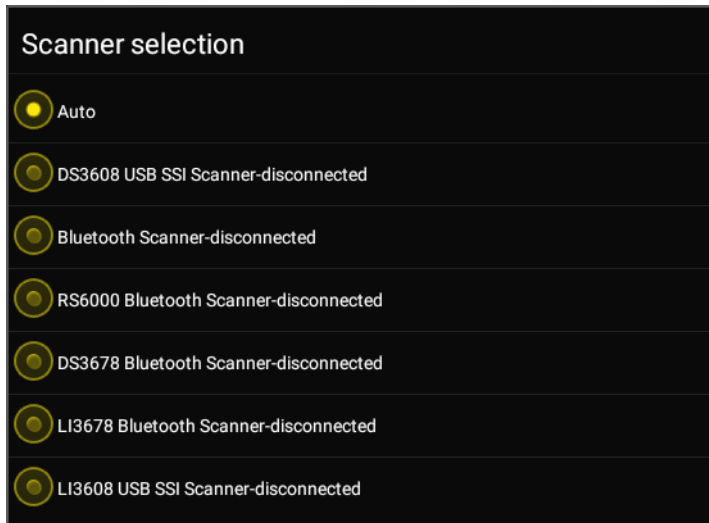
NOTE: See [DataWedge on page 129](#) for more information.

Scanner Selection

Ensure a scanner is connected to the device. See [Data Capture on page 91](#) for more information.

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

Figure 36 Data Capture Options Menu



Select a scanner.

Press the scanner trigger button or touch the on-screen yellow scan button to capture data. The data appears in the text field below the yellow button.

Device Central

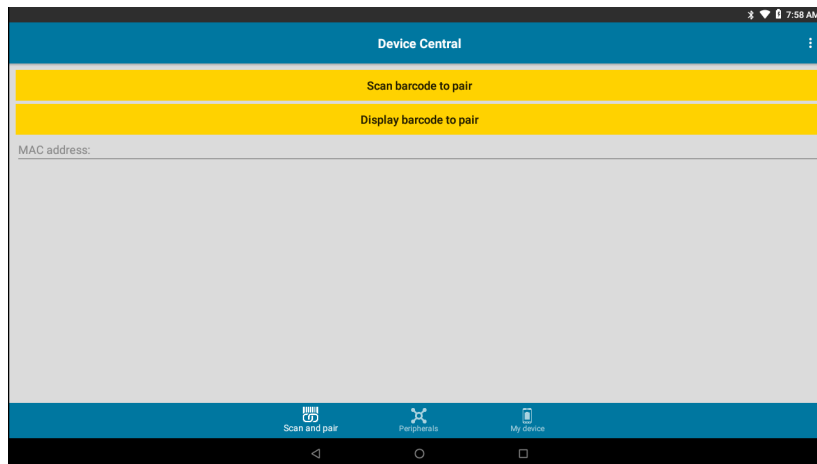
Device Central displays detailed information about the device and connected peripherals, and supports the following Zebra devices:

- RS6000 Bluetooth Ring Scanner
- HS3100 Bluetooth Headset.

Device Central features include:

- Discovering and pairing with supported peripherals via Bluetooth or corded connection.
- Paging a connected RS6000 Ring Scanner.
- Updating the firmware of supported ring scanners. For information on updating ring scanner firmware using Device Central, refer to the RS6000 User Guide.
- Displaying the connection status of peripherals.
- Displaying information for a connected peripheral in the notification bar.

Figure 37 Device Central Screen



Scan and Pair Tab

Pairing to a Bluetooth peripheral is accomplished by one of the following methods:

- Scan and Pair
- Scan to Pair
- Manually Pairing.

Scan and Pair

To scan the peripheral Bluetooth barcode to pair:

1. In the **Scan and Pair** tab, touch **Scan barcode to pair**.
2. The peripheral's scan beam illuminates. Scan the Bluetooth MAC address barcode label on the desired peripheral to pair.

Ensure that Bluetooth is enabled on the peripheral and is set to discoverable mode. Refer to the peripheral user guide for instructions.

- When pairing is successful, the peripheral displays in the list indicating that it is paired. A green dot next to a Bluetooth scanner indicates that the device is connected, and may be in use. Other peripherals such as a Bluetooth headset or printer displays a red dot until the respective application is using these Bluetooth peripherals.

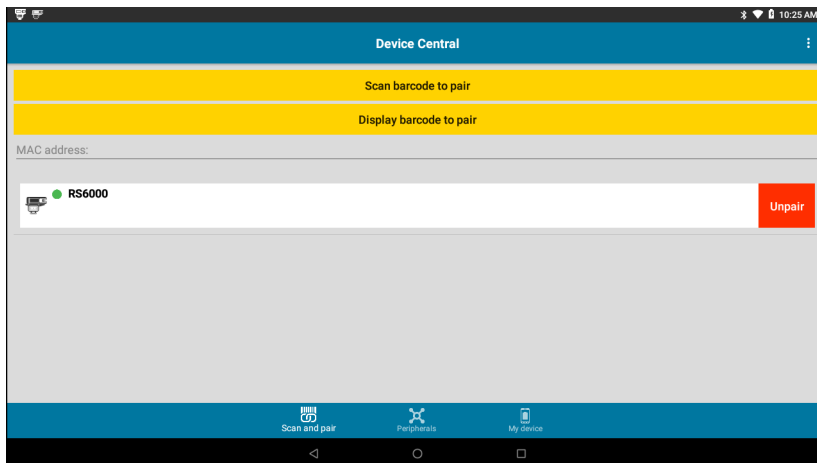
Scan to Pair

Use **Scan and Pair** to pair by scanning the displayed barcode on the display. This applies to peripherals that have scanning capability, such as Bluetooth handheld scanners and ring scanners:

- In the **Scan and Pair** tab, touch **Display barcode to pair**. A barcode displays.
- Using the peripheral, scan the barcode on the screen or scan the barcode on the right side of the device. When the pairing is successful, the peripheral displays in the list with a green dot indicating that it is paired.
- When pairing is successful, the peripheral displays in the list indicating that it is paired. A green dot next to a Bluetooth scanner indicates that the device is connected, and may be in use. Other peripherals such as a Bluetooth headset or printer displays a red dot until the respective application is using these Bluetooth peripherals.

To unpair the scanner, touch the unpair button on the screen or scan the barcode on the left side of the device.

Figure 38 Device Central with Peripheral



Manually Pairing

To pair a peripheral manually if unable to pair via Bluetooth:

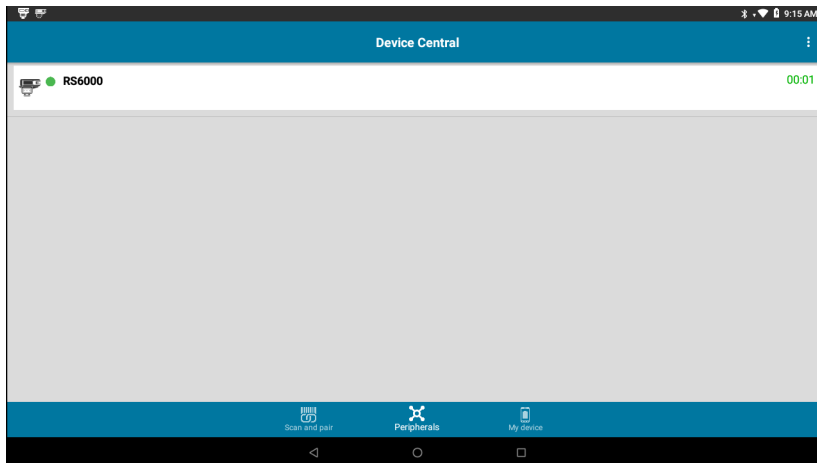
- In the **Scan and Pair** tab, touch the **MAC address** field.
- Enter the Bluetooth MAC address for the peripheral to pair to.
- Touch **Pair**.

When pairing is successful, the peripheral displays in the list. A green dot next to a Bluetooth scanner indicates that the device is connected, and may be in use. Other peripherals such as a Bluetooth headset or printer displays a red dot until the respective application is using these Bluetooth peripherals.

Peripherals Tab

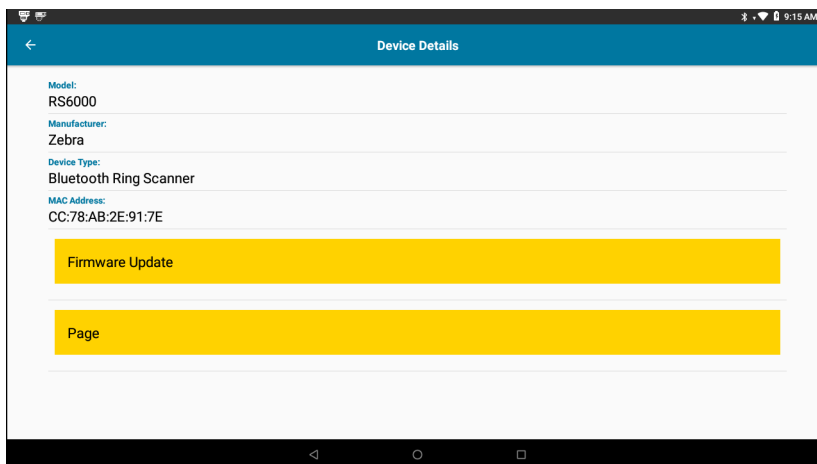
The **Peripherals** tab displays all currently connected and previously connected peripherals. Connected peripherals display the length of time (in minutes) that they have been connected.

Figure 39 Connected Peripherals



Touch the connected device icon to display details about the peripheral. The **Device Details** screen appears. When an RS6000 is connected the **Page** button displays. See [Paging an RS6000 Ring Scanner on page 65](#).

Figure 40 Device Details



My Device Tab

The **My Device** tab displays information about the VC8300.

- **Device Model** - Displays the name assigned to the VC8300.
- **Device Serial Number**- Displays the serial number of the device.
- **OS Version** - Displays the operating system version.
- **Build Number** - Displays the software build number.
- **Battery Level** - The current battery charge level as a percentage.
- **Battery Part Number** - The battery part number.
- **Battery Serial Number** - The battery serial number. The number matches the serial number printed on the battery label.
- **Battery Manufactured Date** - The date of manufacture.


Unpairing a Peripheral

To unpair a Bluetooth peripheral:

1. In the **Scan and Pair** tab, touch **Unpair** for the desired peripheral to unpair.
A confirmation pop-up message appears.
2. Touch **OK**.
3. Once unpaired, a message appears indicating the peripheral has been disconnected, and the peripheral is removed from the list.

Paging an RS6000 Ring Scanner

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

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



NOTE: The RS6000 Ring Scanner must be within 10 m (32 ft) of the VC8300.

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

To stop paging, press the scan trigger of the RS6000. On a triggerless RS6000, stop paging by resetting the RS6000.

Files

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


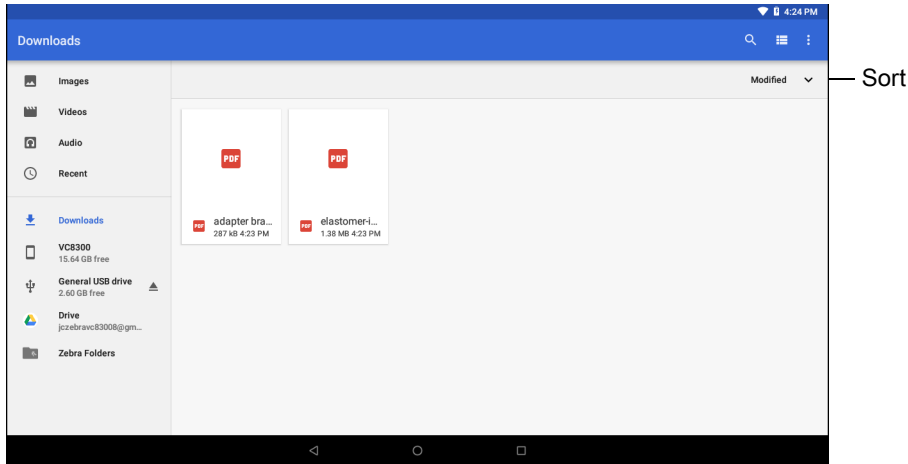








To open **Files**, swipe up from the bottom of the screen and touch .

Figure 41 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.

Diagnostic Tool

The **Diagnostic Tool** is a utility that determines the health of the VC8300. Use the Diagnostic Tool to troubleshooting the device and determine issues.


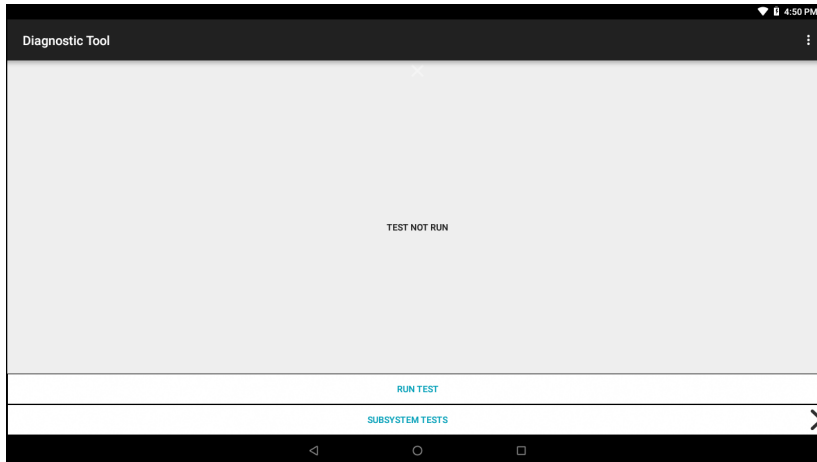
1. Swipe up from the bottom of the Home screen and touch .

Figure 42 Diagnostic Tool



2. Touch **Run Test**. The app tests all enabled subsystems (by default only the Battery and System tests are enabled). See Settings on page 69 to enable subsystem tests.

Figure 43 Test Passed Screen

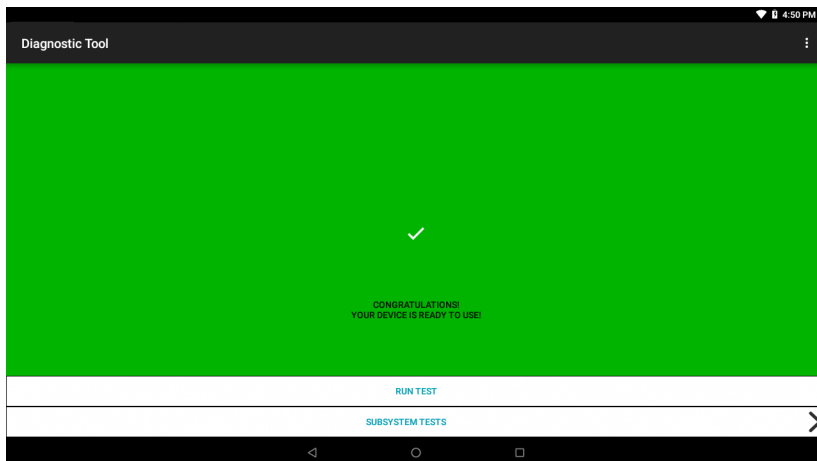
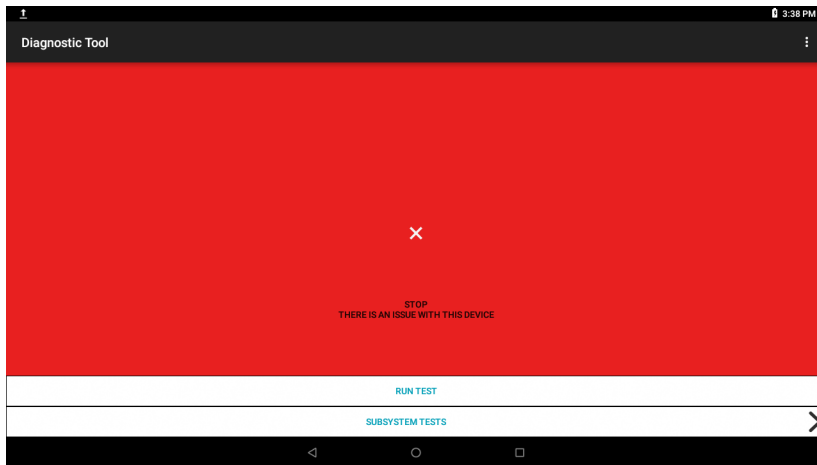


Figure 44 Test Failed Screen



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

Figure 45 Subsystem Screen

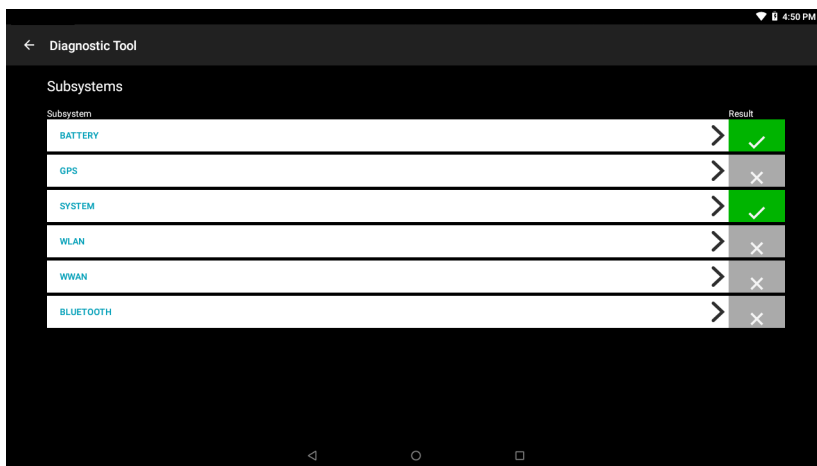


Table 10 *Subsystem Test Result Indicators*

Status Icon	Description
	Indicates test passed.
	Indicates test failed.
	Indicates test not supported or not enabled.



4. Touch one of the subsystems to view details.

Figure 46 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.

GPS Test Information

Not supported on the VC8300.

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 that storage on the device is almost full. The System Test obtains the following information:

- **CPU Load** - Indicates the amount of CPU being used.
- **Free Physical Memory** - Indicates the amount of RAM available.
- **Free Storage** - Indicates the amount of internal Flash memory available.
- **Process Count** - Indicates the number of processes currently running.

WLAN Test Information

If the WiFi radio is not present or disabled the test may be skipped. Use this information to determine 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** - Indicates if the WLAN radio is enabled or disabled.
- **WLAN Status** - Indicates the current status of association with the access point.
- **ESSID** - Displays the name of the wireless network.
- **BSSID** - Displays the MAC address of the connected access point.
- **MAC Address** - Displays the device's MAC address.
- **Signal** - Indicates the strength of the Wi-Fi signal (in dBm).
- **IP Address** - Displays the IP address of the device.

WWAN Test Information

Not supported on the VC8300.

Bluetooth Test Information

The Bluetooth Test obtains the following information:

- **Enabled** - Indicates if the Bluetooth radio is enabled or disabled.
- **Status** - Indicates if the device is paired to another Bluetooth device.
- **Connectable/Discoverable** - Indicates if the device is discoverable or connectable.
- **Address** - Displays the Bluetooth radio MAC address.
- **Name** - Displays the Bluetooth name for the device.

Heater Control

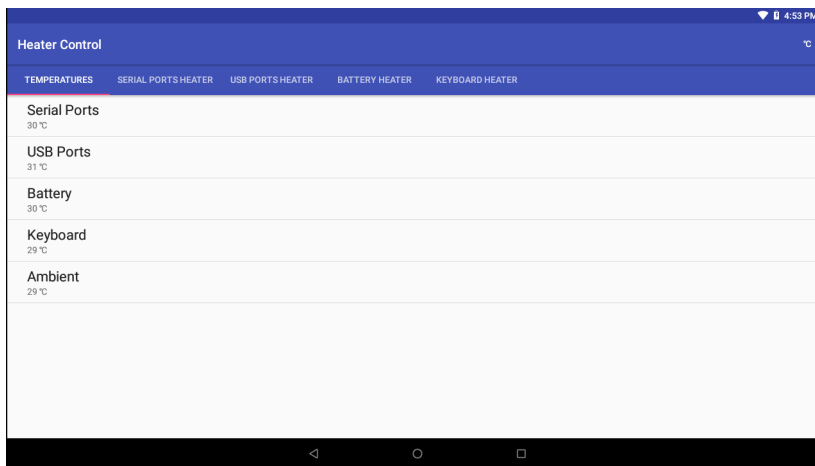


IMPORTANT: Heater Control app is only applicable to freezer configurations.

The device heater ensures optimum performance in freezers. The heater benefits include:

- Touch screen heater clears condensation on the display.
- Port heater prevents condensation on contacts.
- UPS Battery requires a heater to operate below freezing temperatures.
- The user interface displays current temperatures.

Figure 47 Heater Control Screen



Temperatures

The **Temperature** tab displays the current temperature for the following:

- Serial Ports
- USB Ports
- Battery
- Keyboard
- Touch Panel (Freeze configurations only)
- Ambient.

Serial Port Heater

Use the **Serial Ports Heater** tab to enable and set the heater for the serial ports.

- **Enable Heater** - Turns on or off the serial port heater. When on, the switch turn red.
- **Heater on threshold** - Set the temperature at which the heater turns on (default - 5°C/41°F).
- **Heater off threshold** - Set the temperature at which the heater turns off (default - 15°C/59°F).

USB Port Heater

Use the **USB Ports Heater** tab to enable and set the heater for the USB ports.

- **Enable Heater** - Turns on or off the USB port heater. When on, the switch turn red.
- **Heater on threshold** - Set the temperature at which the heater turns on (default - 5°C/41°F).
- **Heater off threshold** - Set the temperature at which the heater turns off (default - 15°C/59°F).

Battery Heater

Use the **Battery Heater** tab to enable and set the heater for the battery.

- **Enable Heater** - Turns on or off the battery heater. When on, the switch turn red.
- **Heater on threshold** - Set the temperature at which the heater turns on (default - 15°C/59°F).
- **Heater off threshold** - Set the temperature at which the heater turns off (default - 20°C/68°F).

Touch Panel Heater



NOTE: Touch Panel Heater tab is available on Freezer configurations only.

Use the **Touch Panel Heater** tab to enable and set the heater for the touch panel.

- **Enable Heater** - Turns on or off the touch panel heater. When on, the switch turn red.
- **Heater on threshold** - Set the temperature at which the heater turns on (default - 15°C/59°F).
- **Heater off threshold** - Set the temperature at which the heater turns off (default - 22°C/72°F).

Keyboard Heater

Use the **Keyboard Heater** tab to enable and set the heater for the keyboard.

- **Enable Heater** - Turns on or off the keyboard heater. When on, the switch turn red.
- **Heater on threshold** - Set the temperature at which the heater turns on (default - 15°C/59°F).
- **Heater off threshold** - Set the temperature at which the heater turns off (default - 22°C/72°F).

Photos




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.

Use Photos to:

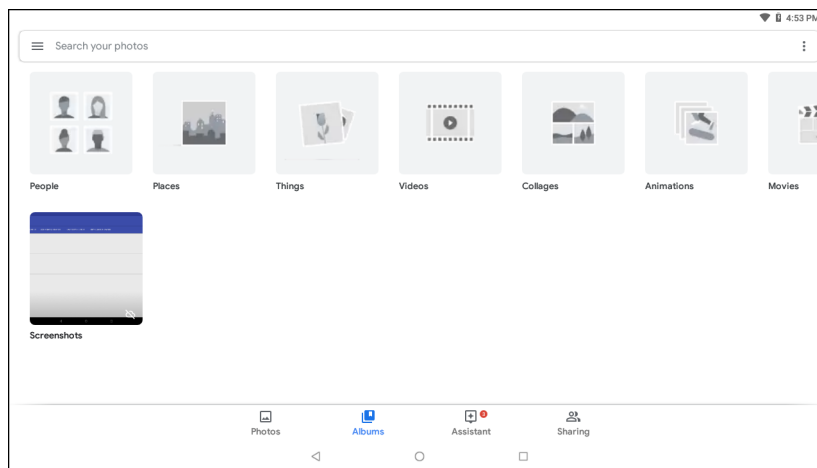
- view photos
- play videos
- perform basic editing of photos
- set photos as wallpaper
- set photos as a contact photo
- share photos and videos.

Photos presents all photos and videos stored on internal memory.

To open the **Photos** application, swipe up from the bottom of the Home screen and touch .

By default, Photos open to the Photos view.

Figure 48 Photos View



Touch **Albums** to view photos sorted by albums.

PTT Express Voice Client



IMPORTANT: The optional M1000 Speaker/Microphone is required to use PTT Express on the VC8300.

PTT Express Voice Client creates Push-To-Talk (PTT) communication capability between disparate enterprise devices. Leveraging existing Wireless Local Area Network (WLAN) infrastructure, PTT Express delivers simple PTT communication without the need of a voice communication server.

- **Group Call:** Press and hold the Talk button to start communicating with other voice client users.
- **Private Response:** Double-press and the Talk button to respond to the originator of the last broadcast or to make a Private Response.

Refer to the PTT Express User Guide at www.zebra.com/support for information on configuring the PTT Express Client application.

Speaker/Microphone Setup

Use the optional M1000 Speaker/Microphone to use PTT Express:

1. Remove the dust cover on the back of the VC8300.
2. Plug the Speaker/microphone audio plug into the Speaker/Mic jack.
3. Replace the audio cable into the cable strain relief.
4. Replace the dust cover.

PTT Audible Indicators

The following tones provide helpful cues when using the voice client.

- **Talk Tone:** Double chirp. Plays when the Talk button is depressed. This is a prompt for the user to start talking.
- **Access Tone:** Single beep. Plays when another user just finished a broadcast or response. The user is now able to initiate a Group Broadcast or Private Response.
- **Busy Tone:** Continuous tone. Plays when the Talk button is depressed and another user is already communicating on the same talkgroup. Plays after the maximum allowed talk time is reached (60 seconds).
- **Network Tone:**
 - Three increasing pitch beeps. Plays when PTT Express has acquired the WLAN connection and the service is enabled.
 - Three decreasing pitch beeps. Plays when PTT Express has lost the WLAN connection or the service is disabled.

Figure 49 PTT Express Default User Interface

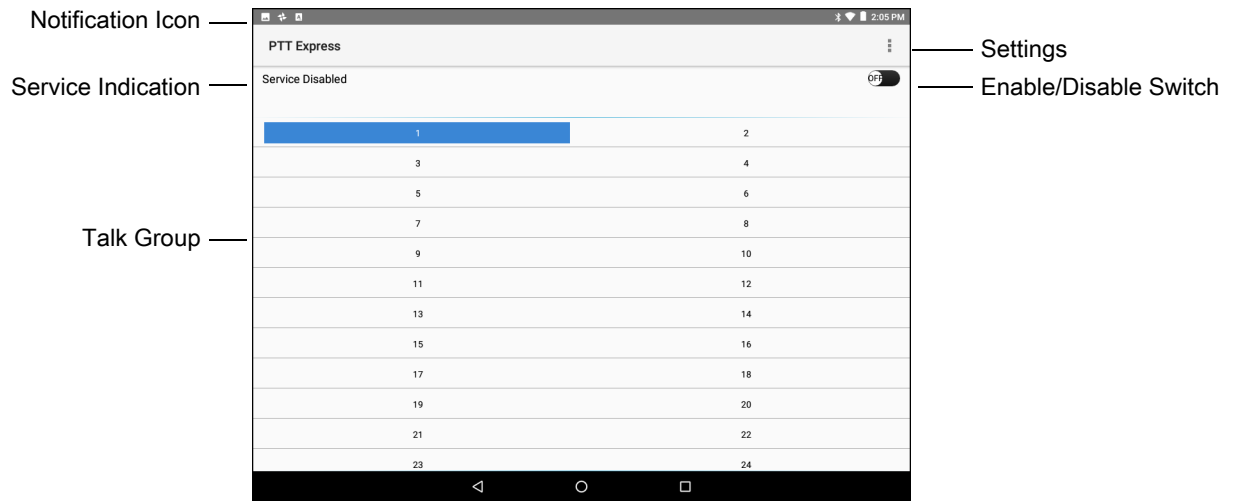


Table 11 PTT Express Default User Interface Descriptions

Item	Description
Notification Icon	Indicates the current state of the PTT Express client.
Service Indication	Indicates the status of the PTT Express client. Options: Service Enabled , Service Disabled or Service Unavailable .
Talk Groups	Lists all 32 Talk Groups available for PTT communication.
Settings	Opens the PTT Express Settings screen.
Enable/Disable Switch	Turns the PTT service on and off.




Notification Icons

Indicates the current state of the PTT Express Voice client.


Table 12 PTT Express Default User Interface Descriptions

Status Icon	Description
	Indicates that PTT Express Voice client is disabled.
	Indicates that PTT Express Voice client is enabled but not connected to a WLAN.
	Indicates that PTT Express Voice client is enabled, connected to a WLAN and listening on the Talk Group indicated by the number next to the icon.
	Indicates that PTT Express Voice client is enabled, connected to a WLAN and communicating on the Talk Group indicated by the number next to the icon.

Table 12 PTT Express Default User Interface Descriptions (Continued)

Status Icon	Description
	Indicates that PTT Express Voice client is enabled, connected to a WLAN and in a private response.
	Indicates that PTT Express Voice client is enabled and muted.
	Indicates that the PTT Express Voice client is enabled but it is not able to communicate due to a VoIP telephony call is in progress.

Enabling PTT Communication

1. Swipe up from the bottom of the Home screen and touch .
2. Slide the **Enable/Disable Switch** to the **ON** position. The button changes to an **ON** button.

Selecting a Talk Group

One of 32 Talk Groups can be selected by PTT Express users. However, only one talk group may be enabled at a time on the device. Touch one of the 32 Talk Groups. The selected Talk Group is highlighted.

PTT Communication



NOTE: This section describes the default PTT Express client configuration. See the PTT Express V1.2 User Guide for detailed information on using the client.

All calls are initiated using the Talk button.

Creating a Group Call

1. Press and hold the Talk button and listen for the talk tone to play.
If a busy tone is heard, release the button and wait a moment before making another attempt. Ensure that PTT Express and the WLAN are enabled.
2. Start talking after the talk tone is heard.



NOTE: If the user holds the button for more than 60 seconds (default), the call is dropped allowing others to make Group calls. The user should release the button when finished talking to allow others to make calls.

3. Release the button when finished talking.



Responding with a Private Response

The Private Response can only be initiated once a Group Call has been established. The initial Private Response is made to the originator of the Group Call.

1. Wait until an access tone is heard.
2. Within 10 seconds, double-press the Talk button, and listen for the talk tone to play.

3. If a busy tone is heard, release the button and wait a moment before making another attempt. Ensure that PTT Express and the WLAN are enabled.
4. Start talking after the talk tone plays.
5. Release the button when finished talking.

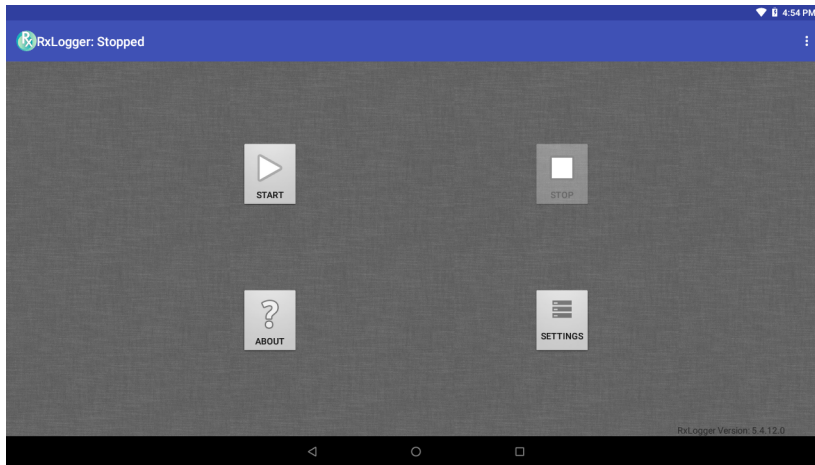
Disabling PTT Express Voice Client Communication

1. Swipe up from the bottom of the Home screen and touch .
2. Slide the **Enable/Disable Switch** to the **OFF** position. The button changes to **OFF**.
3. Touch .

RxLogger



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

Figure 50 RxLogger





Enabling Logging

To enable RxLogger:

1. Swipe up from the bottom of the Home screen and touch .
2. Touch **START**. RxLogger begins collecting data.
3. Touch .

Disabling Logging

To disable RxLogger:

1. Swipe up from the bottom of the Home screen and touch .
2. Touch **STOP**. RxLogger stops collecting data.
3. Touch .

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. Touch **Settings** to open the configuration screen.

Figure 51 RxLogger Settings 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 will also be 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** - Enable to save all previously stored logs.

Kernel Module

The Kernel Module captures kmsg from the system.

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

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 has the ability to collect data from multiple logcat buffers provided by the system. Currently these are the main, event, radio, and system buffers. Each of the settings are available for each buffer independently unless otherwise noted.

- **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** - 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 Max log file size** - 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** - Sets the interval, in milliseconds, 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 Max log file size** - 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** - Sets the interval, in milliseconds, 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** - 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** - Sets the interval, in milliseconds, 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** - 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** - Sets the interval, in milliseconds, 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** - Specifies the maximum size, in kilobytes, 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.
 - **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** - Specifies the maximum size, in kilobytes, 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 to, LTS will then GZ the file and save it in an organize 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

Ramoops Module captures last kmsg from the device.

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

Resource Module

The Resource Module captures devices information on an interval. The data collected contains system statistics to see the health of 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** - Enables or disables the collection of heater temperature data.

Snapshot Module

The Snapshot Module collects detailed device statistics on 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. This file number will be appended to this base filename when saving the snapshot.
- **Log interval** - Specifies the interval, in milliseconds, on which to invoke a detailed snapshot.
- **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.
- **Filesystems** - 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 will be appended to this filename.
- **Tcpdump file size** - 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** - Enable to save all previously stored logs.


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

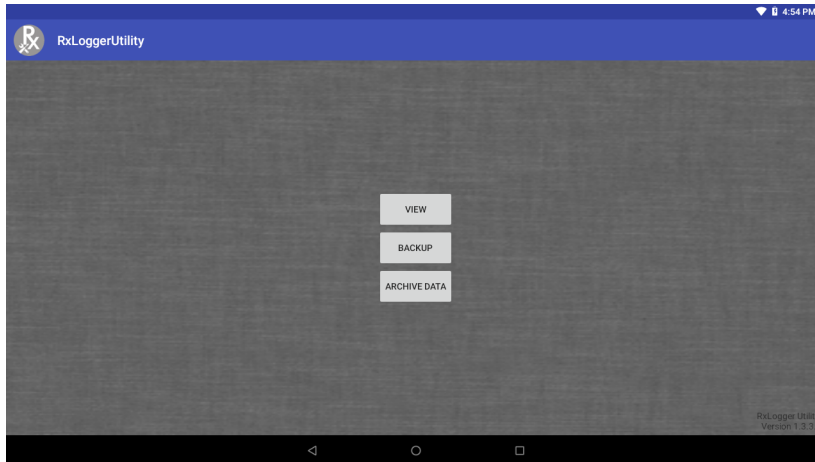
1. Connect the device to a host computer using an USB connection.
2. Using a file explorer, navigate to the **RxLogger** folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

RxLogger Utility

RxLogger Utility is a data monitoring application for viewing logs in the VC8300 while RxLogger is running. The user can access the logs and RxLogger Utility features in the App View or the Overlay View.

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

Figure 52 RxLogger Utility App View

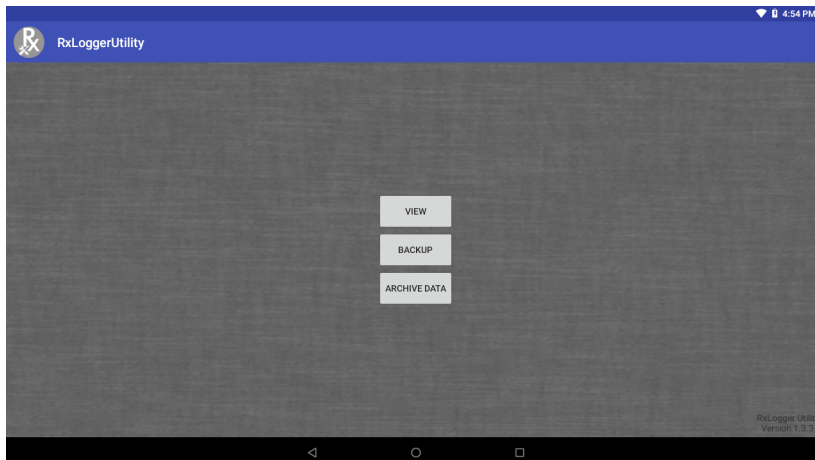


RxLogger Utility is a data monitoring application for viewing logs in the VC8300 while RxLogger is running. The user can access the logs and RxLogger Utility features in the App View or the Overlay View.

App View

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

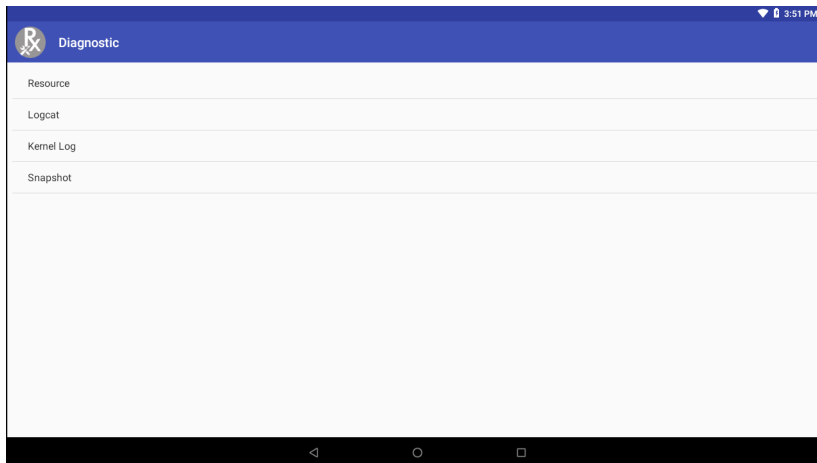
Figure 53 App View



Viewing Logs

Touch **View**. The **Diagnostic** window appears.

Figure 54 Diagnostic Window

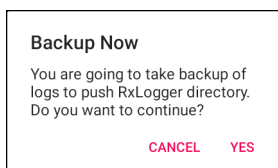


- **Resource** - View all resources.
- **Logcat** - View all the Logcat files. Messages are colored according to flags. Verbose messages is orange text, Assert messages are in brown text, Fail messages are in purple text, Warning messages are in yellow text, information messages are in blue text, debug messages are in green text, and error messages are in red.
- **Kernel Log** - View all the Kernel Logs.
- **Snapshot** - View all the Snapshot.

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.

Figure 55 Backup Message



Touch **Yes** to save the backup data.

Archiving


The user can view all the RxLogger logs stored in the RxLogger directory by default. These is not for live-viewing logs.

Figure 56 Archive

Touch any of the options to view the log files.

Overlay View

To initiate Overlay view:

1. Open **RxLogger**.
2. Touch  > **Toggle Chat Head**. The Chat Head icon appears on 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:

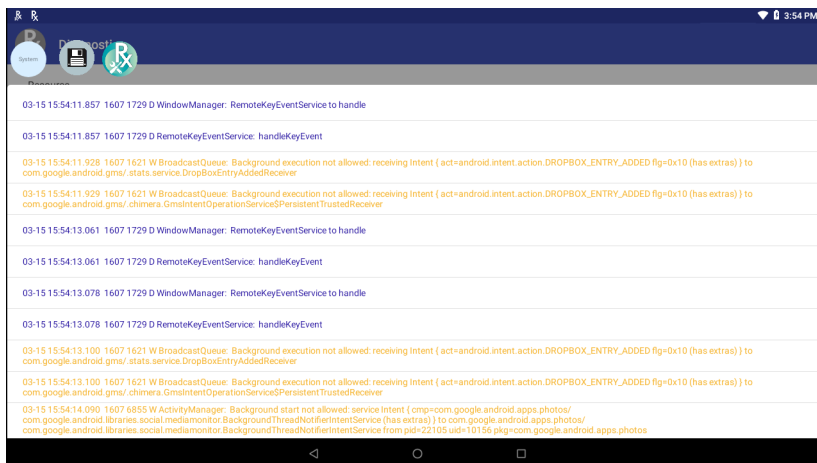
1. Touch the Main Chat head icon. The In View screen appears.

Figure 57 In View Screen



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

Figure 58 Log File



Removing a Sub Chat Head Icon

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

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.

Backup Now icon is always available in the Overlay View.

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

VC Settings



NOTE: Ignition detect requires a CA1220 power extension cable.

Figure 59 VC Settings Screen

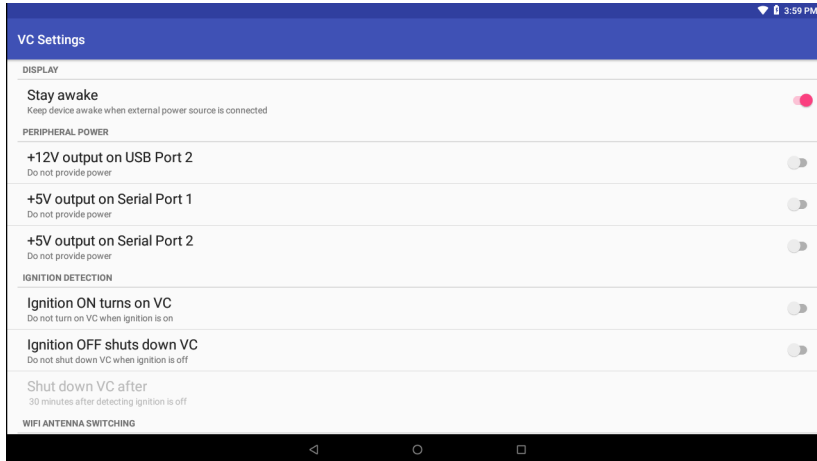
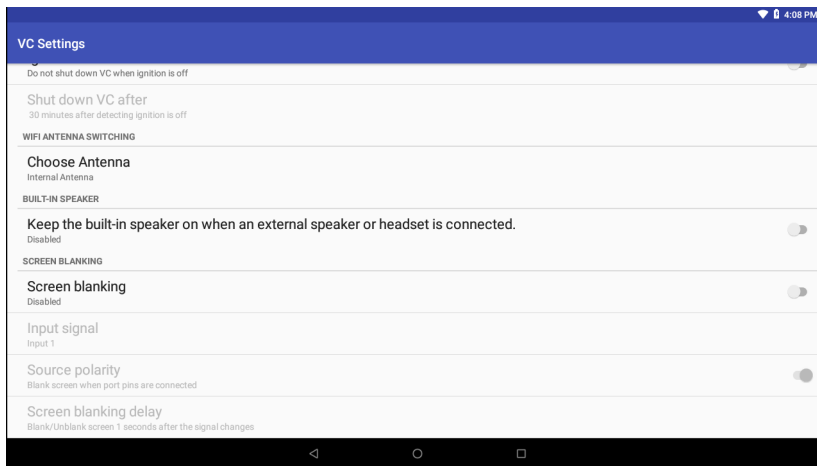


Figure 60 VC Settings Screen (Continued)



Display

Enable/disable **Stay awake** to keep the device awake when the external power source is connected.

Peripheral Power

To provide power to an optional peripheral, turn on power to the appropriate port.

- **+5V output on Serial Port 1** - Enable/disable power for serial port 1.
- **+5V output on Serial Port 2** - Enable/disable power for serial port 2.
- **+12V output on USB** - Enable/disable additional power for the powered USB port.

Ignition Detection

Use Ignition Detection settings to control if the device turns on or off when the user turns on the ignition.



NOTE: Ignition detect requires a CA1220 power extension cable.

- **Ignition ON Turns on VC** - Enable/disable the device to turn on when the user turns the ignition on.
- **Ignition OFF shuts down VC** - Enable/disable the device to turn off when the user turns the ignition off.
- **Shut down VC after** - Select the number of minutes that the device turns off after the user turns off the ignition.

WiFi Antenna Switching

Use to select which Wi-Fi antenna to use.

- Choose Antenna - Select antenna. Options: **Internal Antenna** (default) or **External Antenna**.

Built-In Speaker

Enable/disable to keep the built-in speaker on when the optional M1000 Speaker/Microphone is connected.

Screen Blanking

The optional Screen Blanking setting turns the screen off when the vehicle is moving and back on when the vehicle stops.



NOTE: To use Screen Blanking, first connect one of the two DB9 serial ports on the device to a user-supplied switch or relay. See [Connecting Switch for Screen Blanking on page 32](#).

- **Screen Blanking** - Enable/disable screen blanking feature.
- **Input signal** - Select the port that the screen blank cable is connected to. Options: **Input 1** or **Input 2**.
- **Source polarity** - Select blank screen option. De-select to disconnect the blank screen option.
- **Blank screen delay** - Set the amount of time after the device receives the signal to blank the screen. Options 1 to 30 seconds (default - 1).

Velocity

Velocity transforms the traditional green screen telnet application into a modern smart device application. It accomplishes all of this without modifying the host application, offering workers a familiar experience optimized for today's touch screen mobile computers.


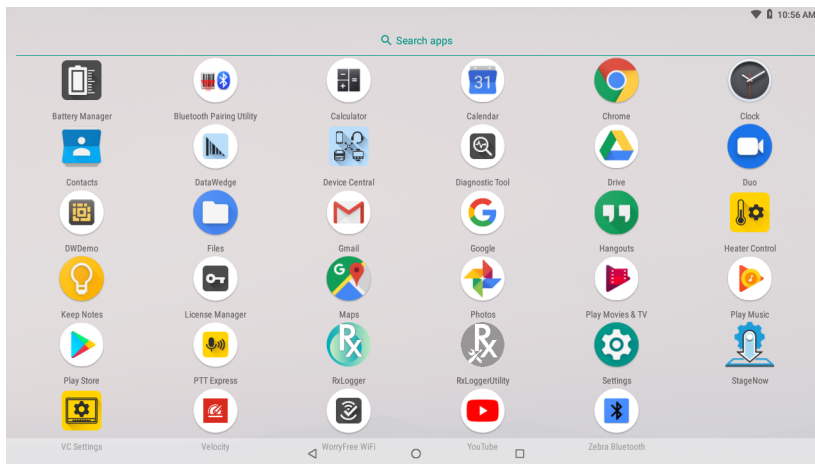
To open Velocity, swipe up from the Home screen and touch .

Figure 61 Velocity Icon



- Access the context menu for quick access to function or control keys.
- Access the Velocity menu for starting new sessions or switching between green and reformatted screens.

Refer to the Velocity user guide for more information. Goto <http://download.wavelink.com/Files/Velocity-qsg-28042016.pdf>

Data Capture

The VC8300 supports scanners that use the Human Interface Device (HID) and Simple Serial Interface (SSI) protocols. In HID mode, the scanner sends data to the VC8300 like entering characters on a keyboard. In SSI mode, the scanner sends data to the VC8300 in packets which can be ASCII data or as part of a larger message.

The VC8300 supports data capture using:

- Tethered scanner connected to COM1 or COM2 port:
 - DS3508-ER, HD, SR
 - DS3608-SR, ER, HP, HD
 - LI3608-SR
 - LS3408-ER, FZ
 - Other tethered serial scanners.
- Tethered scanner connected to a USB host port:
 - DS3508-ER, HD, SR (HID mode only)
 - DS3608-SR, ER, HP, HD (HID and SSI modes)
 - LI3608-SR (HID mode only)
 - LS3408-ER, FZ (HID mode only)
 - Other USB scanners (HID mode only).
- Wireless scanner connected via Bluetooth:
 - DS3678-SR, ER, HP, HD (HID and SSI modes)
 - LI3678-SR (HID mode only)
 - LS3578-ER, SR, HD, FZ (HID mode only)
 - DS3578-SR, ER, HD (HID mode only)
 - RS507/RS507x (HID and SSI modes)
 - RS6000 (HID and SSI modes)
 - Other Bluetooth scanners (HID mode only).

Imaging

The scanner with 2D imager has the following features:

- Omnidirectional reading of a variety of barcode symbologies, including the most popular linear, postal, PDF417, and 2D matrix code types.
- The ability to capture and download images to a host for a variety of imaging applications.

- Advanced intuitive laser aiming cross-hair and dot aiming for easy point-and-shoot operation.

The imager uses imaging technology to take a picture of a barcode, stores the resulting image in its memory, and executes state-of-the-art software decoding algorithms to extract the barcode data from the image.

Operational Modes

The imager supports two modes of operation, listed below. Activate each mode by pressing the Scan button.

- **Decode Mode:** In this mode, the scanner attempts to locate and decode enabled barcodes within its field of view. The imager remains in this mode as long as the user holds the scan button, or until it decodes a barcode.



NOTE: To enable Pick List Mode, configure in DataWedge or set in an application using a API command.

Picklist mode is dependent upon the scanner. Refer to the scanner user guide for more information.

- **Pick List Mode:** This mode allows the user to selectively decode a barcode when more than one barcode is in the scanner's field of view. To accomplish this, move the aiming crosshair or dot over the required barcode to decode only this barcode. This feature is ideal for pick lists containing multiple barcodes and manufacturing or transport labels containing more than one barcode type (either 1D or 2D).

Laser Scanning

Scanner with lasers has the following features:

- Reading of a variety of bar code symbologies, including the most popular linear, postal, and 1-D code types.
- Intuitive aiming for easy point-and-shoot operation.

Scanning Considerations

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

- **Range:** Any scanning device decodes well over a particular working range — minimum and maximum distances from the barcode. This range varies according to barcode density and scanning device optics. Scanning within range brings 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 promoting quick decodes. When laser beams reflect directly back into the scanner from the barcode, this specular reflection can “blind” the scanner. To avoid this, scan the barcode so that the beam does not bounce directly back. But don't 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 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 VC8300 configuration. An application may use different scanning procedures from the one listed above.

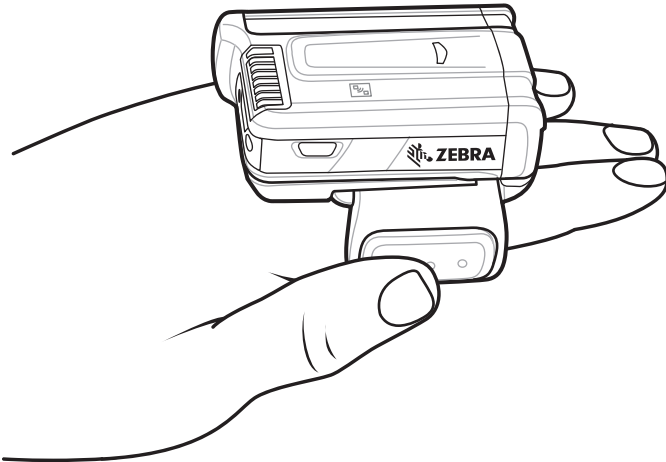
Barcode Capture with RS6000 Bluetooth Ring Scanner

To read a barcode, a scan-enabled application is required. The VC8300 contains the **DataWedge** application that allows the user to enable the scanner to decode barcode data and display the barcode content. See [DataWedge Demonstration on page 60](#) for more information on launching DataWedge.

Pair the RS6000 with the VC8300. See [Pairing Using Simple Serial Interface on page 99](#) or [Pairing Using Human Interface Device on page 100](#) for more information.

1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Point the RS6000 at a barcode.

Figure 62 Barcode Scanning with RS6000



3. Press and hold the trigger.

The red laser aiming pattern turns on to assist in aiming. Ensure the barcode is within the area formed by the cross-hairs in the aiming pattern. The aiming dot is used for increased visibility in bright lighting conditions.

The RS6000 LEDs light green, a beep sounds to indicate the barcode was decoded successfully. Note that when the RS6000 is in Pick List Mode, the RS6000 does not decode the barcode until the center of the crosshair touches the barcode.

Figure 63 Aiming Pattern

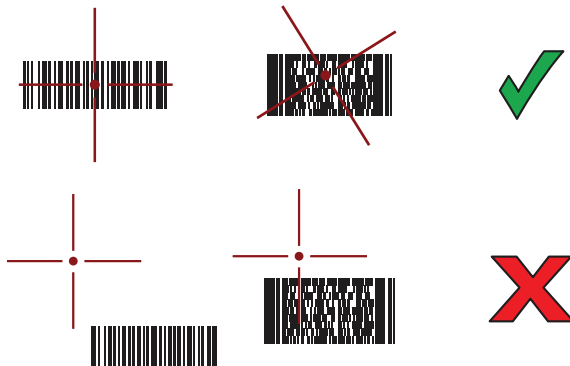


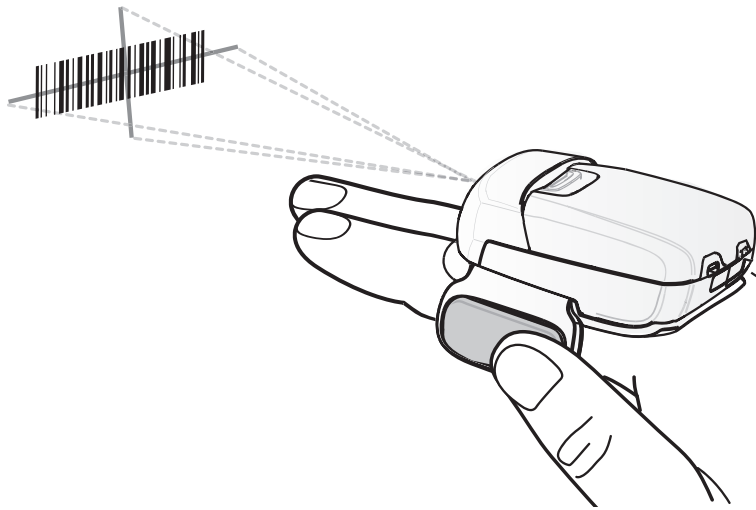
Figure 64 Pick List Mode with Multiple barcodes in Aiming Pattern

4. The captured data appears in the text field.

Barcode Capture with RS507/RS507x Hands-Free Imager

Pair the RS507/RS507x with the VC8300. See Pairing the RS507/RS507x/RS6000 Hands-Free Imager on page 99 for more information.

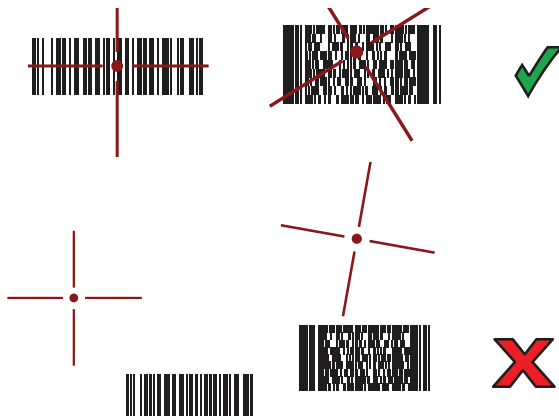
1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Point the RS507/RS507x at a barcode.

Figure 65 barcode Scanning with RS507/RS507x

3. Press and hold the trigger.

The red laser aiming pattern turns on to assist in aiming. Ensure the barcode is within the area formed by the cross-hairs in the aiming pattern. The aiming dot is used for increased visibility in bright lighting conditions.

The RS507/RS507x LEDs light green, a beep sounds to indicate the barcode was decoded successfully. Note that when the RS507/RS507x is in Pick List Mode, the RS507/RS507x does not decode the barcode until the center of the crosshair touches the barcode.

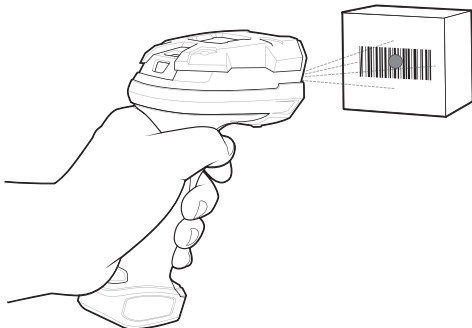
Figure 66 Aiming Pattern**Figure 67** Pick List Mode with Multiple barcodes in Aiming Pattern

4. The captured data appears in the text field.

Bar Code Capture with Zebra Scanner

To capture barcodes data:

1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Point the scanner at a bar code.

Figure 68 Bar Code Scanning (DS3678-SR shown)

3. Press and hold the trigger.

Ensure the bar code is within the area formed by the aiming pattern. The aiming dot is used for increased visibility in bright lighting conditions. The aiming dot is used for increased visibility in bright lighting conditions.

Figure 69 DS3678-SR Aiming Pattern

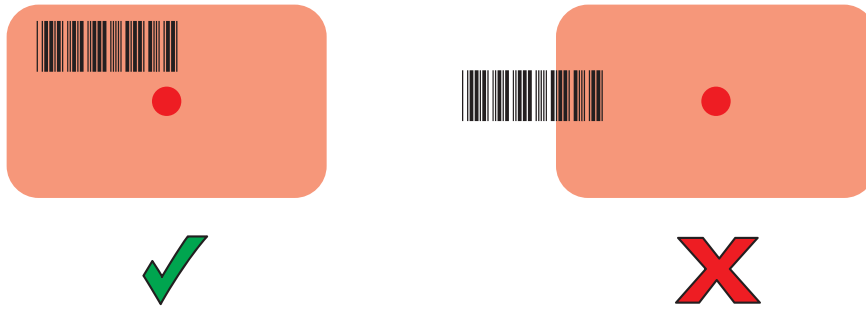
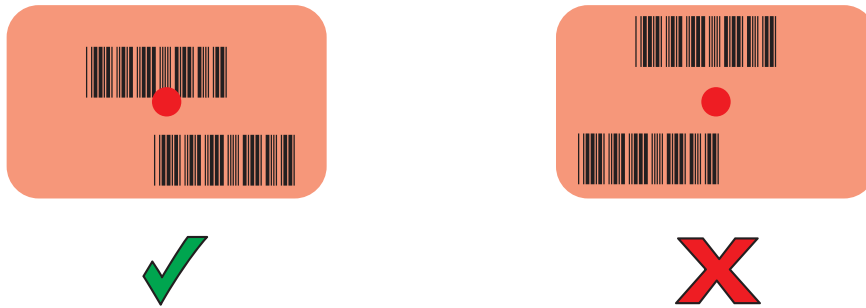


Figure 70 DS3678-SR Pick List Mode with Multiple Bar Codes in Aiming Pattern



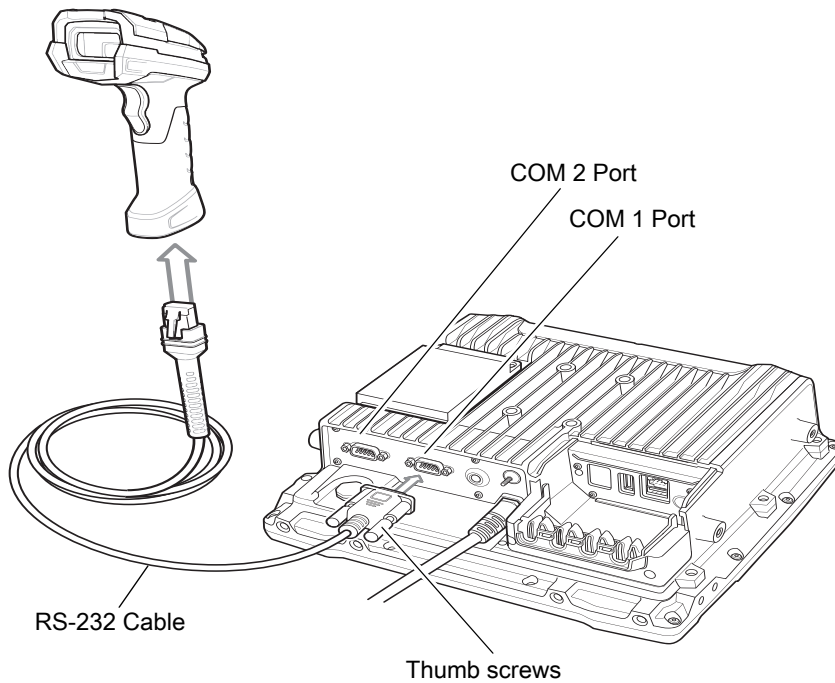
4. The captured data appears in the text field.




Connecting an RS-232 Scanner

To connect an RS-232 scanner:

1. On the bottom of the VC8300, remove the connector cover from either the COM1 or COM2 port.
2. Connect the scanner cable RS-232 connector to either the COM1 or COM2 port and to the scanner.

Figure 71 Connect RS-232 Scanner



3. Tighten the RS-232 connect thumb screws.
4. On the VC8300 home screen, swipe up from the bottom of the Home screen and touch .
5. Touch **+5V output on Serial Port 1** if the RS-232 scanner is connected to the COM1 port or **+5V output on Serial Port 2** if the scanner is connected to the COM 2 port. The scanner beeps.
6. Touch .
7. Swipe up from the bottom of the Home screen and touch .
8. Select a profile.
9. Scroll down to **Serial port input from Serial port 1** or **Serial port input from Serial port 2**.
10. Touch **Enabled**. A check appears in the checkbox to the right.



IMPORTANT: By default, serial settings are set for all Zebra scanners. Other non-Zebra scanner may need configuration. Refer to the scanner user guide for more information.

11. Touch **Serial port configuration**.
12. Touch **Baud rate**.
13. Select one of the available baud rates.
14. Touch **Data bits**.
15. Select **7** or **8**.
16. Touch **Parity**.
17. Select a parity value.
18. Touch **Stop bits**.

19. Select **1** or **2**.

20. Touch ◀.

21. Touch ○.

Connecting a USB Scanner

To connect a USB scanner, use one of the following methods:

- Simple Serial Interface (SSI) mode
- Human Interface Device (HID) mode.

Connecting Using Simple Serial Interface

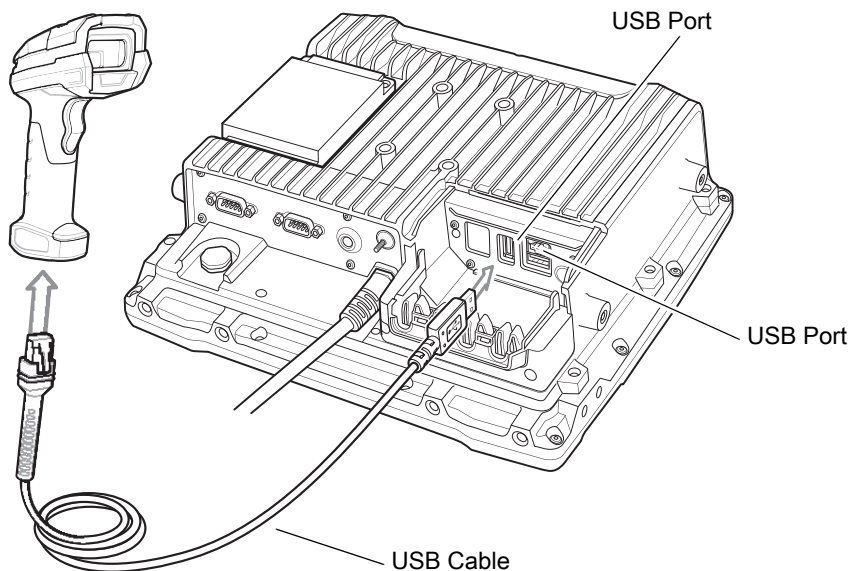


IMPORTANT: Make sure that DS3608 scanner has firmware version CAACJS00-004-R00D0.DAT or higher.

To connect a USB scanner using SSI mode:

1. On the back of the VC8300, remove the dust cover.
2. Connect the scanner cable USB connector to either USB port. The scanner beeps.

Figure 72 Connect USB Scanner



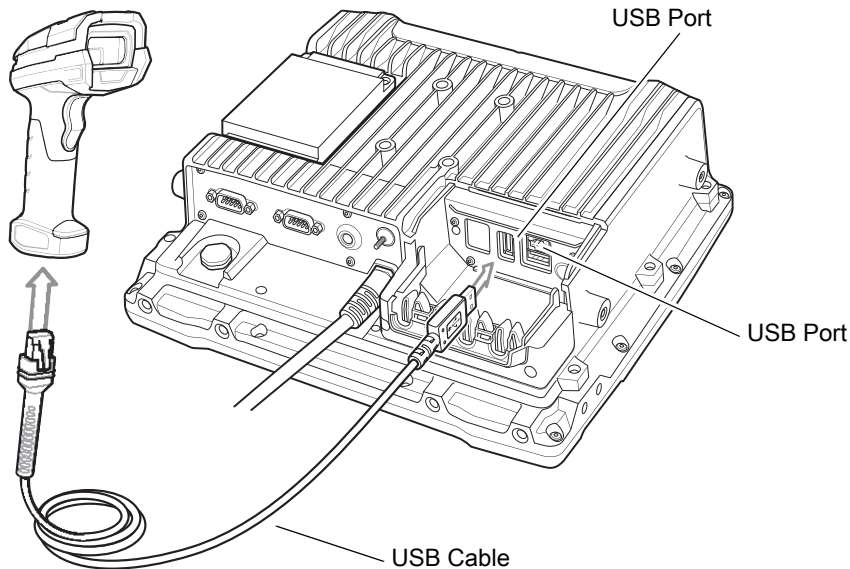
3. Place cable into strain relief.
4. Replace the dust cover.
5. Ensure that the scanner is in SSI mode. Refer to the scanner Product Reference Guide and scan the SSI Over USB CDC barcode.
6. On the VC8300 home screen, swipe up from the bottom of the Home screen and touch .
7. Select a profile.
8. Configure additional settings.

Connecting Using HID Mode

To connect a USB scanner using HID mode:

1. On the back of the VC8300, remove the dust cover.
2. Connect the scanner cable USB connector to either USB port. The scanner beeps.

Figure 73 Connect USB Scanner



3. Place the cable into the strain relief.
4. Replace the dust cover.
5. Ensure that the scanner is in HID mode. Refer to the Product Reference Guide and scan the HID Keyboard barcode or perform a factory reset.

Pairing the RS507/RS507x/RS6000 Hands-Free Imager

To connect an RS507/RS507x/RS6000 Hands-Free Imager to the VC8300, use one of the following methods:

- Simple Serial Interface (SSI) mode
- Bluetooth Human Interface Device (HID) mode.

Pairing Using Simple Serial Interface

To pair the RS507/RS507x/RS6000 with the VC8300 using SSI:

1. Ensure that the scanner is in SSI mode. If the RS507/RS507x/RS6000 is already in SSI mode, skip to step 2.
 - a. Remove the battery from the RS507/RS507x/RS6000.
 - b. Press and hold the Restore key.
 - c. Install the battery onto the RS507/RS507x/RS6000.
 - d. Keep holding the Restore key for about five seconds until a chirp is heard and the Scan LEDs flash green.


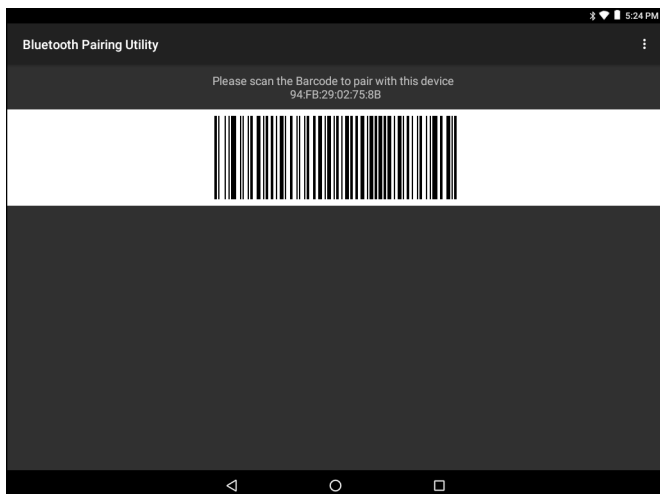

2. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
3. On the VC8300, swipe up from the bottom of the Home screen and touch .

Figure 74 Bluetooth Pairing Utility



4. Using the RS507/RS507x/RS6000, scan the barcode on the screen or scan the barcode on the right side of the VC8300.

The RS507/RS507x/RS6000 emits a high/low/high/low beeps. The Scan LED flashes green indicating that the scanner is attempting to establish connection with the VC8300. When connection is established, the Scan LED turns off and the scanner emits one string of low/high beeps.

5. On the VC8300, touch .

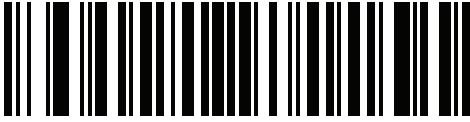
Pairing Using Human Interface Device


To pair the RS507/RS507x/RS6000 with the VC8300 using HID:

1. Place the RS507/RS507x/RS6000 in Human Interface Device (HID) mode. If the scanner is already in HID mode, skip to step 2.
 - a. Remove the battery from the RS507/RS507x/RS6000.
 - b. Press and hold the Restore key.
 - c. Install the battery onto the RS507/RS507x/RS6000.
 - d. Keep holding the Restore key for about five seconds until a chirp is heard and the Scan LEDs flash green.
 - e. Scan the barcode below to place the RS507/RS507x/RS6000 in HID mode.

Figure 75 RS507/RS507x Bluetooth HID Barcode



Figure 76 RS6000 Bluetooth HID Barcode

2. Remove the battery from the RS507/RS507x/RS6000.
3. Re-install the battery into the RS507/RS507x/RS6000.
4. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
5. Swipe down from the status bar and then touch .
6. Touch **Bluetooth**.
7. The device begins searching for discoverable Bluetooth devices in the area and displays them under **AVAILABLE DEVICES**.
8. Scroll through the list and select RS507/RS507x or RS6000.
The RS507/RS507x/RS6000 connects to the scanner and **Connected** appears below the device name.
The Bluetooth device is added to the **Paired devices** list and a trusted (“paired”) connection is established.

Pairing a DS3678 Scanner

To connect an DS3678 scanner to the VC8300, use one of the following methods:

- Simple Serial Interface (SSI) mode
- Bluetooth Human Interface Device (HID) mode.

Pairing Using Simple Serial Interface



IMPORTANT: Make sure that DS3678 scanner has firmware version CAACKS00-003-R00D0.DAT or higher.

To pair the DS3678 scanner with the VC8300 using SSI:


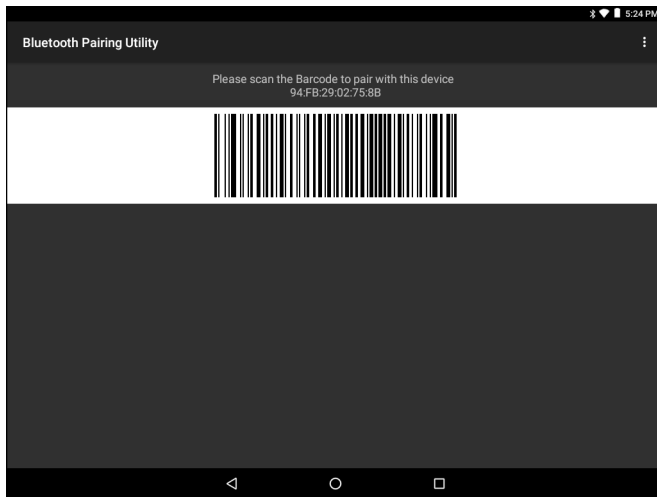

1. Ensure that the scanner is in SSI mode.
2. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
3. On the VC8300, swipe up from the bottom of the Home screen and touch .

Figure 77 Bluetooth Pairing Utility




4. Using the scanner, scan the barcode on the screen or scan the barcode on the right side of the VC8300. The scanner emits a high/low/high/low beeps. The Scan LED flashes green indicating that the scanner is attempting to establish connection with the VC8300. When connection is established, the Scan LED turns off and the scanner emits one string of low/high beeps.
5. On the VC8300, touch .

Pairing a DS3678 Scanner Using Human Interface Device



NOTE: The VC8300 supports Zebra DS3678, LI3678, LS3578, and DS3578 scanners in HID mode.

To pair the scanner with the VC8300 using HID:

1. Ensure that the scanner is in HID mode. Refer to the DS36X8 Product Reference Guide and scan the HID Keyboard barcode.
2. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
3. Swipe down from the status bar and then touch .
4. Touch **Bluetooth**.
5. The device begins searching for discoverable Bluetooth devices in the area and displays them under **AVAILABLE DEVICES**.
6. Scroll through the list and select the scanner.




The device connects to the scanner and **Connected** appears below the device name. The Bluetooth device is added to the **Paired devices** list and a trusted (“paired”) connection is established.

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 see [DataWedge on page 129](#).

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. The blue checkmark disappears from the checkbox indicating that DataWedge is disabled.
4. Touch .

Wireless

This section provides information on the wireless features:

- Wireless Local Area Network (WLAN)
- Bluetooth.

Wireless Local Area Networks



NOTE: If using an external antenna, ensure correct settings.

Wireless local area networks (WLANs) allow the VC8300 to communicate wirelessly inside a building. Before using the VC8300 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 VC8300 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 to configure the VC8300 to match the security scheme.

The VC8300 supports the following WLAN security options:

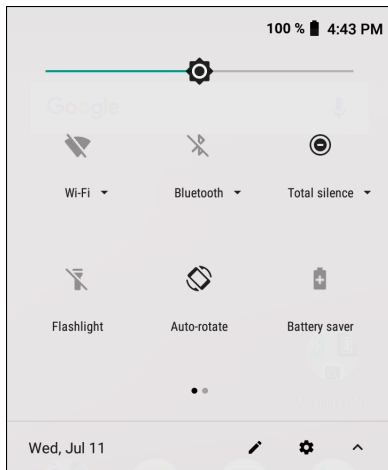
- Open
- Wireless Equivalent Privacy (WEP).
- Wi-Fi Protected Access (WPA)/WPA2 Personal (PSK).
- Extensible Authentication Protocol (EAP).

The **Status** bar displays icons that indicate Wi-Fi network availability and Wi-Fi status. See Status Bar for more information.

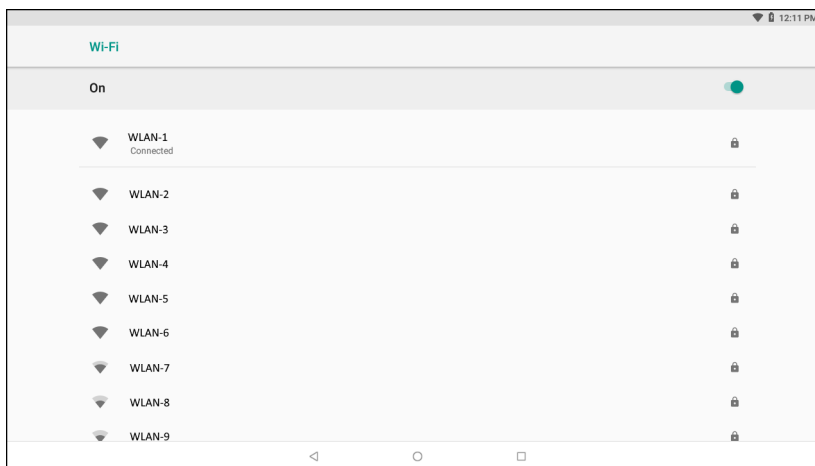
Scanning and Connecting to a Wi-Fi Network

To scan and connect to a Wi-Fi network:

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

Figure 78 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 79 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.

Remove a Wi-Fi Network

To remove a remembered or connected network:

1. Swipe down from the status bar and then touch **⚙**.
2. Touch **Wi-Fi**.
3. In the **Wi-Fi** list, touch and hold the name of the network.

4. In the menu, touch **Forget network**.
5. Touch .

Configuring a Wi-Fi Network

To set up a Wi-Fi network:


1. Swipe down from the status bar and then touch .
2. Touch **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 80 WLAN WEP Network Security Dialog Box

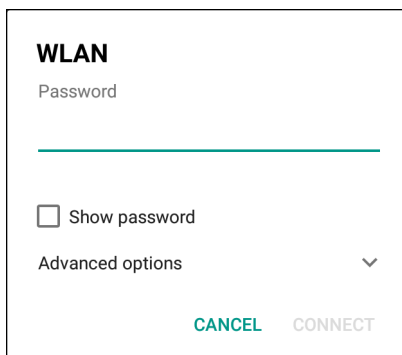


Figure 81 WLAN 802.11 EAP Network Security Dialog Box



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 on page 108](#) for setting connection to a proxy server and see [Configuring the Device to Use a Static IP Address on page 109](#) 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 and then touch .
2. Touch **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Scroll down to the bottom of the window and touch **Add network**.
5. In the **Enter the SSID** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, select the type of security. Options:
 - **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 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 on page 108](#) for setting connection to a proxy server and see [Configuring the Device to Use a Static IP Address on page 109](#) 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:


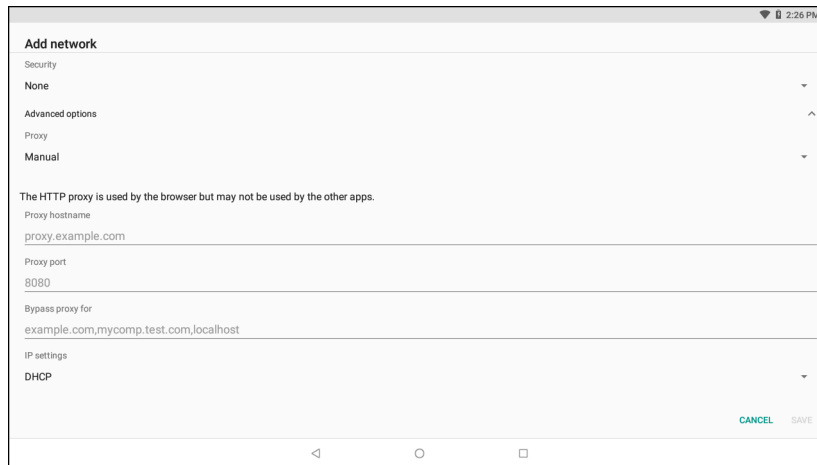

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Network & Internet > Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. Touch **Advanced options**.
6. Touch **Proxy** and select **Manual**.

Figure 82 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 83 Static IP Settings

The screenshot shows the 'Add network' screen in an Android settings application. The screen is titled 'Add network' and has a status bar at the top showing signal strength, Wi-Fi, and the time 2:26 PM. The settings are as follows:

- Proxy: None
- IP settings: Static
- IP address: 192.168.1.128
- Gateway: 192.168.1.1
- Network prefix length: 24
- DNS 1: 8.8.8.8
- DNS 2: 8.8.4.4

At the bottom right, there are 'CANCEL' and 'SAVE' buttons. At the bottom center, there are three navigation icons: a back arrow, a circle, and a square.

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

Wi-Fi Preferences

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

- **Open network notification** - When enabled, notifies the user when an open network is available.
- **Advanced - Touch to expand options.**
 - **Additional settings** - See Additional Settings.
 - **Install Certificates** - Touch to install certificates.
 - **Network rating provider** - To help determine what constitutes a good Wi-Fi network, Android supports external Network rating providers that provide information about the quality of open Wi-Fi networks. Select one of the providers listed or **None**. If none are available or selected, the Connect to open networks feature is disabled.
 - **Wi-Fi Direct** - Displays a list of devices available for a direct Wi-Fi connection.
 - **WPS Push Button** - Touch to connect to a network using Wi-Fi Protected Setup (WPS) push button method.
 - **WPS Pin Entry** - Touch to connect to a network using Wi-Fi Protected Setup (WPS) pin entry method.
 - **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
 - **IP address** - Displays the IP address of the device when connecting to Wi-Fi networks.

Additional Wi-Fi Settings



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

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

- **Regulatory**
 - **Country Selection** - Displays the acquired country code if 802.11d is enabled, else it displays the currently selected country code.
 - **Region code** - Displays the current region code.
- **Band and Channel Selection**
 - **Wi-Fi frequency band** - Set the frequency band to: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
 - **Available channels (2.4 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
 - **Available channels (5 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
- **Logging**
 - **Advanced Logging** – Touch to enable advanced logging or change the log directory.



NOTE: All log files are saved in /storage/sdcard/fusionlogs on the VC8300.

Fusion will ask the user whether to clear out previous logs before starting logging.

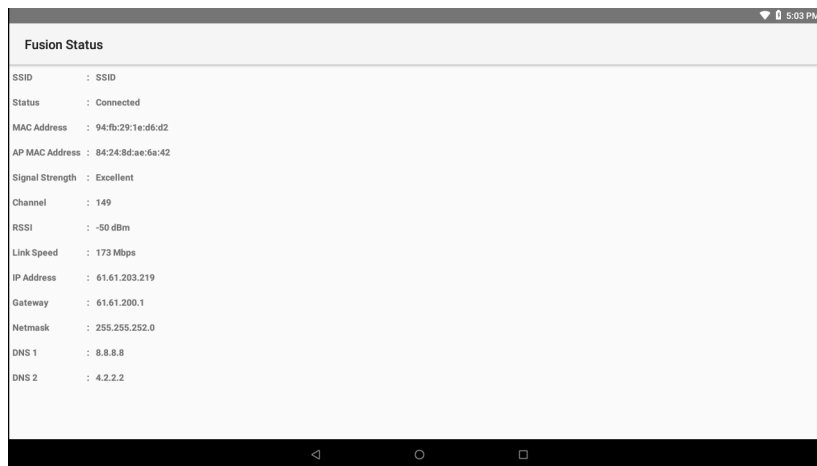
tcpdump capture file and fusion-sysinfo.log will only be generated when advanced logging is stopped.

- Android logcat output with time stamps and the kernel messages in the file: `fusion-wlan.log`.
- tcpdump intermediate capture of packets between network stack and driver in the file: `fusion-pktcap.pcap`
- Fusion versions, Wi-Fi state machine logs and other framework information in the file: `fusion-sysinfo.log`.
- **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.

Figure 84 Fusion Logger Screen



Figure 85 Fusion Status Screen

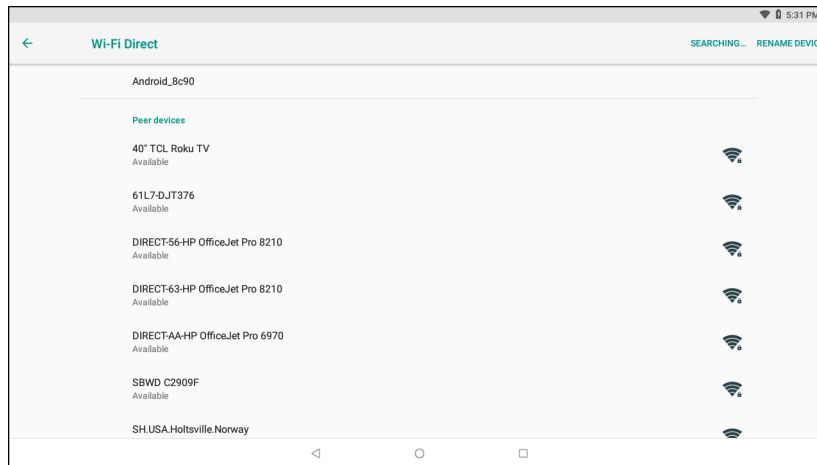


- **About**
 - **Version** - Displays the current Fusion information.

Wi-Fi Direct

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

1. Swipe down from the status bar and then touch **⚙**.
2. Touch **Wi-Fi > Wi-Fi preferences > Advanced > Wi-Fi Direct**. The device begins searching for another Wi-Fi Direct device.
3. Under **Peer devices**, touch the other device name.
4. On the other device, select **Accept**.
5. **Connected** appears on the device. On both devices, in their respective Wi-Fi Direct screens, the other device name appears in the list.

Figure 86 Wi-Fi Direct Screen

WPS Pin Entry

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

To use a PIN to connect to a wireless router:


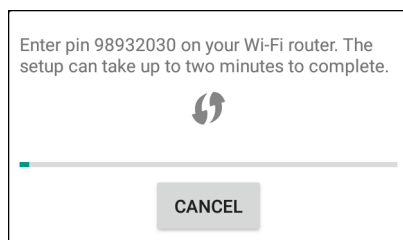
1. Log in to the router.
2. Go to the Add WPS Client screen. Refer to the wireless router user documentation specific information.
3. On the device, swipe down from the status bar and then touch .
4. Touch **Wi-Fi > Wi-Fi preferences > Advanced > WPS Pin Entry**. A dialog box displays with an Pin number.

Figure 87 Pin Entry Dialog Box

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

WPS Push Button

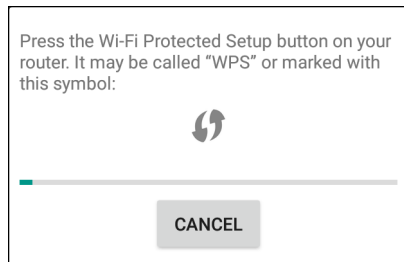
Wi-Fi Protected Setup (WPS) is a feature allowing devices to easily connect to Wi-Fi access points without typing a long password.

To use a wireless router WPS button:

1. On the device, swipe down from the status bar and then touch .

2. Touch **Wi-Fi > Wi-Fi preferences > Advanced > WPS Push Button**. A dialog box displays with an Pin number.

Figure 88 Pin Entry Dialog Box



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

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: enabled.
- **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.

Zebra Mobility Extensions

Zebra Mobility Extensions make use 802.11 specifications and Zebra proprietary extensions to achieve the highest level of performance, efficiency and reliability. The VC8300 adds support for the following Zebra Mobility Extensions.

- **Coverage Hole Detection** - The VC8300 includes enhancements to the IEEE 802.11k standard. These improvements will report gaps in signal coverage to the Zebra wireless LAN infrastructure. Network administrators can detect and mitigate coverage gaps present in the network for greater reliability. Default: enabled.
- **Aggregated Fast Transition** - Aggregated FT improves on IEEE 802.11r, Over-the-DS fast roaming. In conjunction with Zebra wireless LAN infrastructure, the VC8300 will achieve more reliable and consistent fast roaming. Default: enabled.
- **Scan Assist** - The VC8300 monitors neighbor access points and retrieves roaming related information from the Zebra wireless LAN infrastructure without doing scans. Using this Scan Assist feature, the VC8300 improves roaming. Default: enabled.

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 13 *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.
Advanced Audio Distribution Profile (A2DP)	Allows the device to stream stereo-quality audio to a wireless headset or wireless stereo speakers.
Audio/Video Remote Control Profile (AVRCP)	Allows the device to control A/V equipment to which a user has access. It may be used in concert with A2DP.
Personal Area Network (PAN)	Allows the use of Bluetooth Network Encapsulation Protocol to provide L3 networking capabilities over a Bluetooth link. Only PANU role is supported.

Table 13 *Bluetooth Profiles (Continued)*

Profile	Description
Human Interface Device Profile (HID)	Allows Bluetooth keyboards, pointing devices, gaming devices and remote monitoring devices to connect to the device.
Headset Profile (HSP)	Allows a hands-free device, such as a Bluetooth headset, to place and receive calls on the device.
Hands-Free Profile (HFP)	Allows car hands-free kits to communicate with the device in the car.
Phone Book Access Profile (PBAP)	Allows exchange of Phone Book Objects between a car kit and a mobile device to allow the car kit to display the name of the incoming caller; allow the car kit to download the phone book so you can initiate a call from the car display.
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.
Symbol Serial Interface (SSI)	Allows for communication with Bluetooth Imager.
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.
Dial Up Networking (DUN)	Provides a standard to access the Internet and other dial-up services over Bluetooth.
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 .

Accessories and Mounting

Introduction

This chapter provides accessory information, mounting options and instructions.

Accessories

Table 14 *Accessories*

Model Number	Description
Antennas	
AN2010	Antenna, dual band, 802.11 a/b/g/n/ac, 2 dBi, reverse polarity SMA connector, magnetic mount, 2.9 m (9.5 ft) cable.
AN2020	Antenna, 2.4 GHz, 802.11 b/g, 5 dBi, reverse polarity SMA connector, magnetic mount, 2.9 m (9.5 ft) cable.
AN2030	Whip antenna (stubby), dual band, 802.11 a/b/g/n/ac, 2.4 GHz 2 dBi, 5 GHz 3.7 dBi, reverse polarity SMA connector.
AR1000	Right Angle SMA reverse polarity plug-jack adapter.
Mounts	
MT4200	Quick release mount.
MT4205	Mounting plate for the MT4200 quick release mount.
MT4210	Adapter bracket kit for 82XX quick release mount.
MT4510	RAM rectangular base with 2.25" rubber ball.
MT4301	RAM mount, 4" arm.
MT4302	RAM mount, 12" arm.
MT3501	VESA base (for 4" or 12" RAM arm).
MT3502	Circular base (for 4" or 12" RAM arm).
MT3505	Clamp base (for 4" or 12" RAM arm), 2" max. width.
MT3507	Clamp base (for 4" or 12" RAM arm), 3" max. width.
MT3509	Rail base (for 4" or 12" RAM arm), 1-1/4" to 1-7/8".
MT3510	Rail base (for 4" or 12" RAM arm), 2" to 2-1/2"
KT-KYBDMNT-VC80-R	Function/Numeric keypad side mount bracket.

Table 14 *Accessories (Continued)*

Model Number	Description
MNT-VC80-ADPA1-1	Adapter for VC50 U-Mount.
MNT-VC80-ADPB1-1	Adapter for Honeywell U-Mount.
KT-U-MOUNT-VC80-R	U-Mount, with VC70 and 8585 / 8595 U-Mount hole pattern. Includes MNT-VC80-ADPA1-1 adapter.
Speaker/Mic	
M1000	Speaker/Mic with push-to-talk function.
Miscellaneous	
KT-VC80-BTRY1-01	Spare battery
WA4070	Ethernet to USB Dongle.
KT-AREFL-VC83-8-1	Anti Reflection Foil, pack of 3.
Power Supplies and Cables	
PS000145A01	100/240 VAC power supply, 24 VDC, 6.5 A, 150W (AC power cord sold separately)
PS1370	Pre-Regulator, 24 - 90 VDC in, 15 VDC out, 90 W
PS1450	100/240 VAC power supply, 12 VDC, 6 A. (AC power cord sold separately)
CB000417A01	DC power adaptor to VC50 extension cable
CB000416A01	DC Power adaptor to VC70 extension cable
CA1210	Power extension cable, DC, 6', waterproof
CA1230	Power extension cable for pre-regulator
CA1220	Power extension cable, DC, 180 cm, with ignition sense
CA1300	Screen blanking cable (DB9 to open wires)
A9169798	Adapter CPC to LXE/Honeywell VCX8, VX9, VM1, VM2 and VM3 DC Power Extension Cable.
A9169801	Adapter CPC and Serial to LXE VCX8 and VX9 DC Power Extension and Screen Blanking Cable.

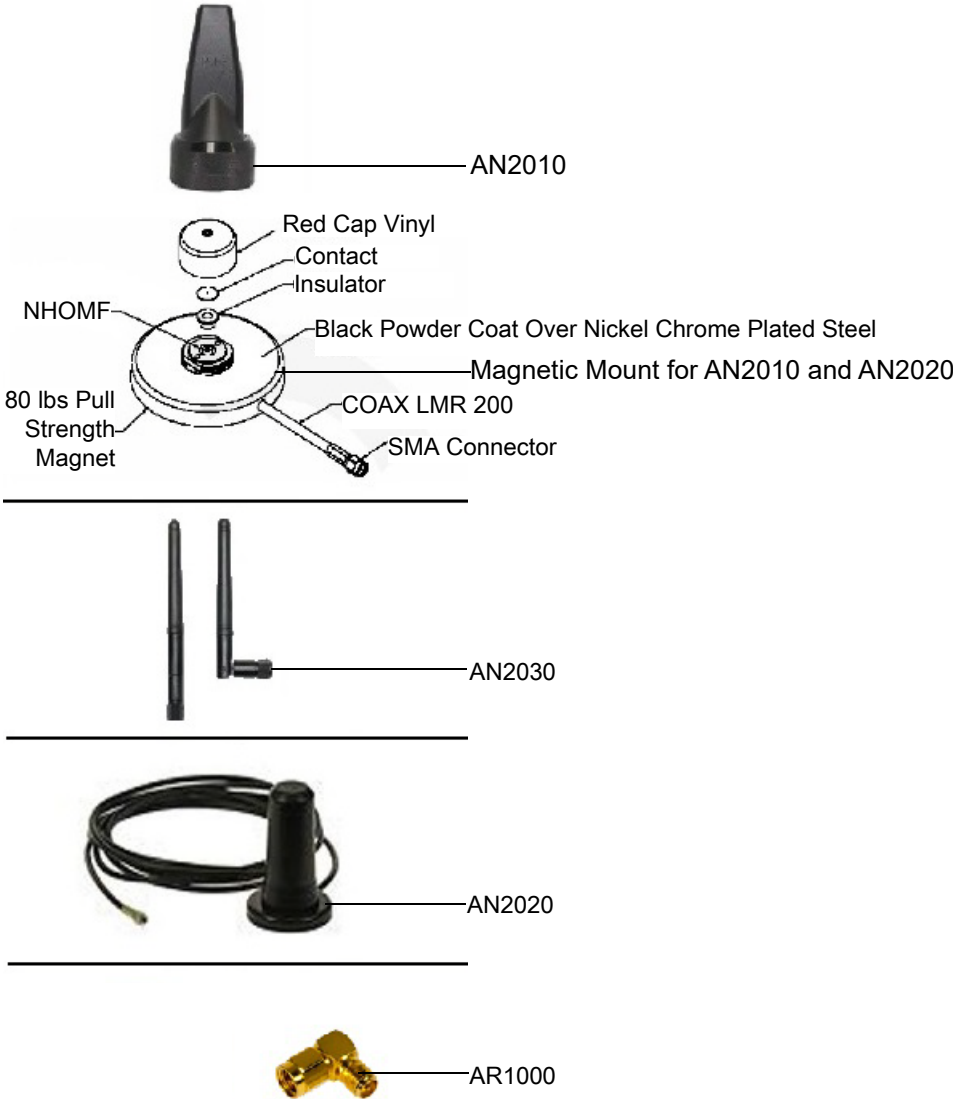
VC8300 Antenna Options

Antenna hardware configurations are located in [Table 14 on page 120](#). To determine the best antenna option for your location, contact your Zebra representative.



IMPORTANT: If using a magnetic mount antenna, place it in a location that balances the need for the VC8300 to communicate with the access points and local Bluetooth peripherals.

Figure 89 VC8300 Antenna Options



VC8300 Mounting Accessories



WARNING: Failure to install the mount correctly, or modifications to the mount, may result in serious injury or damage to property. Contact Zebra Technical Support or your Zebra representative if you have problems installing this mount. To ensure operator safety, you must use a calibrated torque wrench and the supplied mounting hardware when fastening the computer and mount. Use of this mount in vehicles driven on public roads or highways is prohibited. Contact Zebra for further details.

Before mounting a VC8300 in a vehicle, there are a number of operator safety issues that require careful attention. When mounting a VC8300 use only approved Zebra mounting hardware and mounting parts which are specific to the VC8300 model purchased. An improperly mounted VC8300 or use of non-approved parts may result in one or more of the following: operator injury, property damage, operator visibility obstruction, operator distraction, and/or poor ease of egress for the operator. Zebra strongly recommends that you seek professional mounting advice from the vehicle manufacturer.

If it is necessary to mount the VC8300 overhead, or in any position that could cause injury to the operator should the unit fall, it is critical that a secondary tether or other fail safe device be installed.

The following restrictions must be strictly enforced:

- Do not use the mount and/or the VC8300 as a hand-held. Using the mount in this manner may cause the person to fall or dislodge the mounting hardware and/or mounts.
- Do not add weight or attach any other items to the mount or VC8300. Additional elements may fall causing injury, or may increase the chance of failure and/or damage in mounting hardware and/or mounts.
- Mounts used in industrial or vibration generating environments may be subjected to fatigue, stress, and/or part wear. A periodic inspection of the mounting hardware and mounts should be performed to ensure parts are retightened to the correct torque, free of fractures, excessive wear, and/or other environmental damage. Any parts found to be unsafe should be removed and replaced immediately. After inspection or replacement of parts, readjust the mount as outlined in the pertinent sections below.
- Cable routing within a vehicle cab also requires careful consideration, especially for separately connected scanners and other devices with loose cables. If you are unable to obtain suitable advice, contact Zebra for assistance. For better protection, the equipment should be mounted inside the vehicle roll cage.
- When charging the vehicle battery, the VC8300 must be either disconnected from the battery or it must be determined that the maximum allowed input voltage of the VC8300 is not exceeded.

MT43XX RAM Mount



IMPORTANT: To avoid injury, this device must be properly secured when in a moving vehicle.

Keep this device away from magnetic fields.

Do not place the computer near a television or radio receiver.

Do not disassemble the VC8300 computer as there are no user-serviceable parts inside.



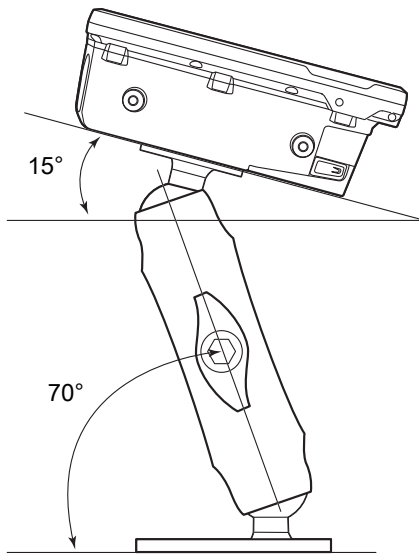
IMPORTANT: The operator can easily adjust the tilt and rotation of the VC8300. Use care to avoid operator injury or equipment damage if the computer slips due to a loosened hand screw.

The VC8300 may be installed using an articulating RAM Mount (Model MT43XX – 4 in. or 12 in. arm) secured to either a VESA or circular base.

The RAM articulating mount can be installed in a variety of orientations (see [Figure 91 on page 125](#)). Select the best orientation for the specific application. Preferred orientations maintain the center of mass of the computer assembly, directly over the center of the base.

For detailed mount installation information, refer to the instructions included with the mount kit.

Figure 90 Orientation of Vehicle-Mount Assembly



Optional Mounts

One of the following optional mounting kits shown in [Figure 91](#) may be substituted for the Vesa base or the circular base when mounting to a post or forklift roll cage.

To assemble the optional mount kit:

1. Mount the clamp base and lower base around the shaft.
2. Place the screws through the clamp and the lower base, and affix with the nuts.
3. Torque to 26 in-lbs.
4. Secure the RAM standard arm by inserting the RAM balls into both ends of the arm sockets.

Figure 91 Optional Mount Kits

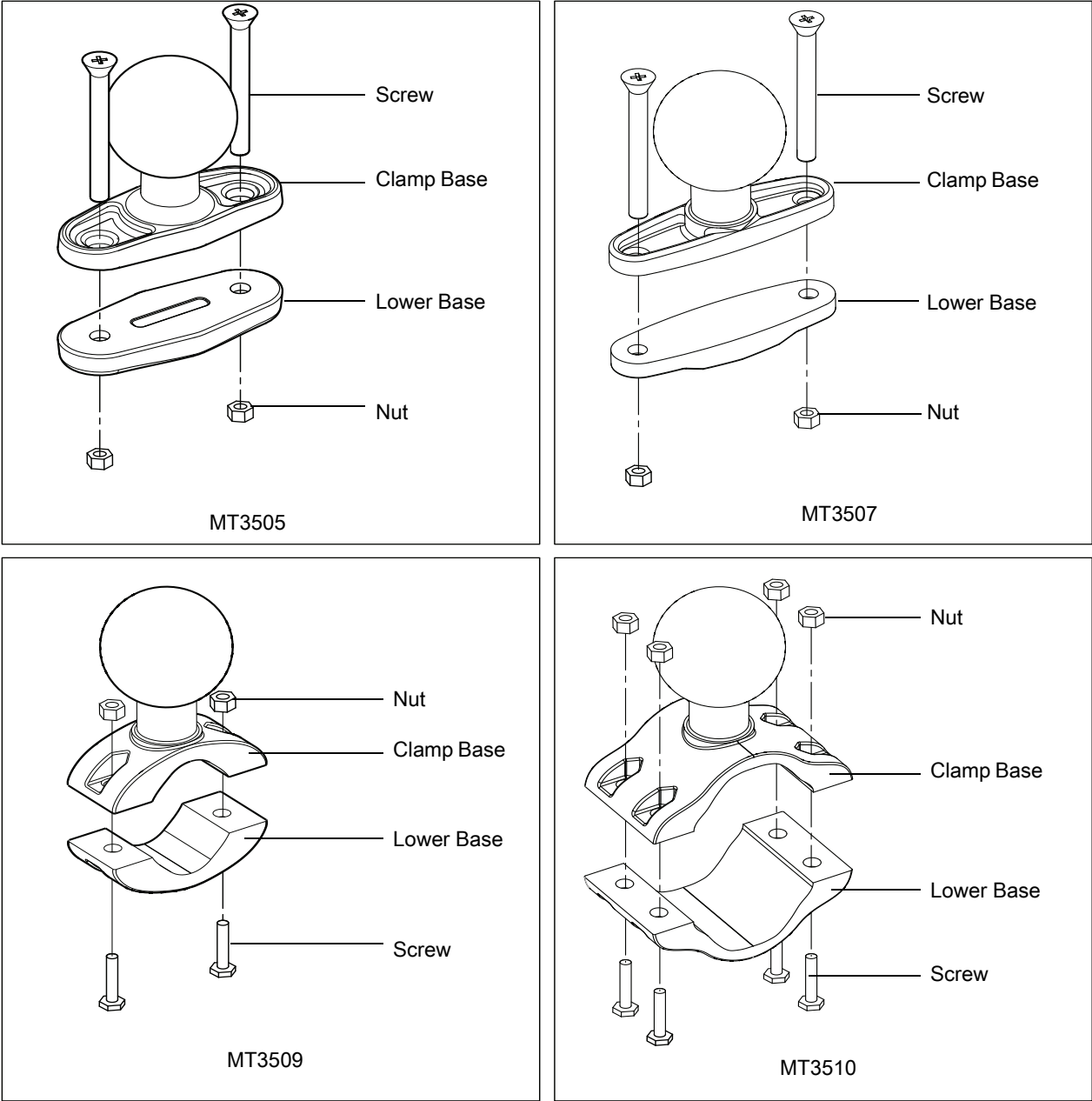


Plate Bases for MT35XX Mounts

Plate bases are not recommended for forklift mounting solutions. If this requires a plate rather than a clamp base, you must penetrate into the structure of the vehicle. This requires additional hardware. The following plate bases are available:

- MT3501 - VESA Plate
- MT3502 - Circular Plate

MT4200 Quick Release Mount

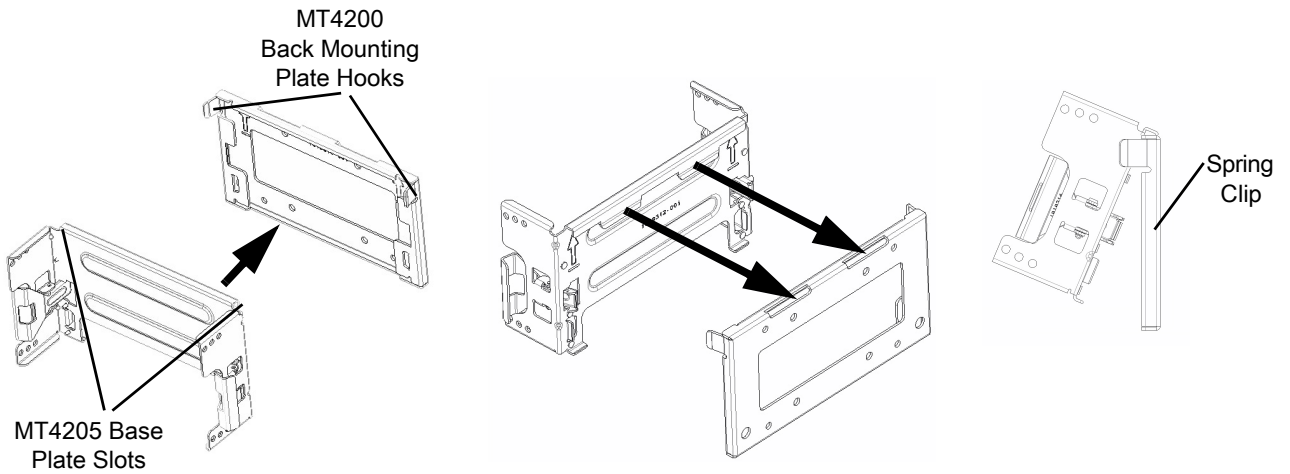
The MT4200 Quick Release Mount allows for removal without the need for tools.

Assembling MT4200

To assemble the MT4200 Quick Release Mount:

1. Place the back mounting plate hooks into the base plate slots.
2. Snap spring clips into place.

Figure 92 MT4200 Quick Release Mount Assembly

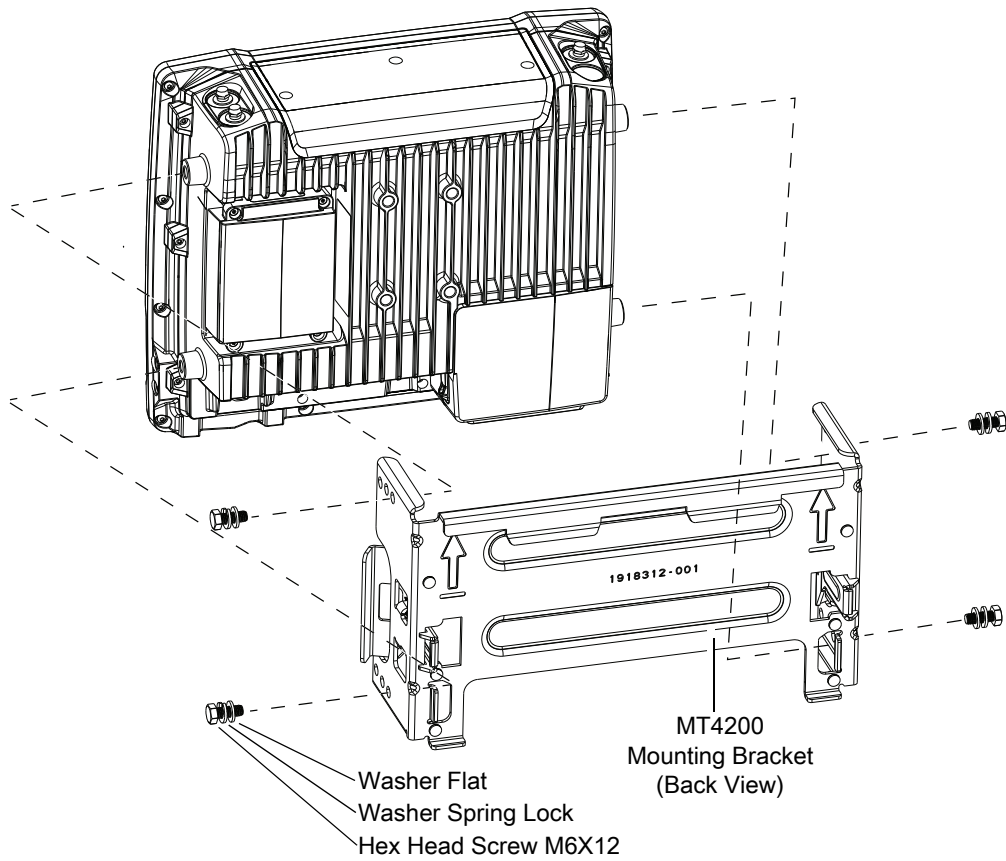


Attaching MT4200 to VC8300

To attach the MT4200 Quick Release Mount to the VC8300:

1. Line up the MT4200 mounting bracket holes with the holes on the sides of the VC8300 (two on each side).
2. Place the spring lock washer onto the hex head screw.
3. Place the flat washer onto the hex head screw (on top of the washer spring lock).
4. Screw the bracket onto the VC8300 (total of four). Torque to 34.7 in-lbs.

Figure 93 VC8300 and MT4200 Assembly



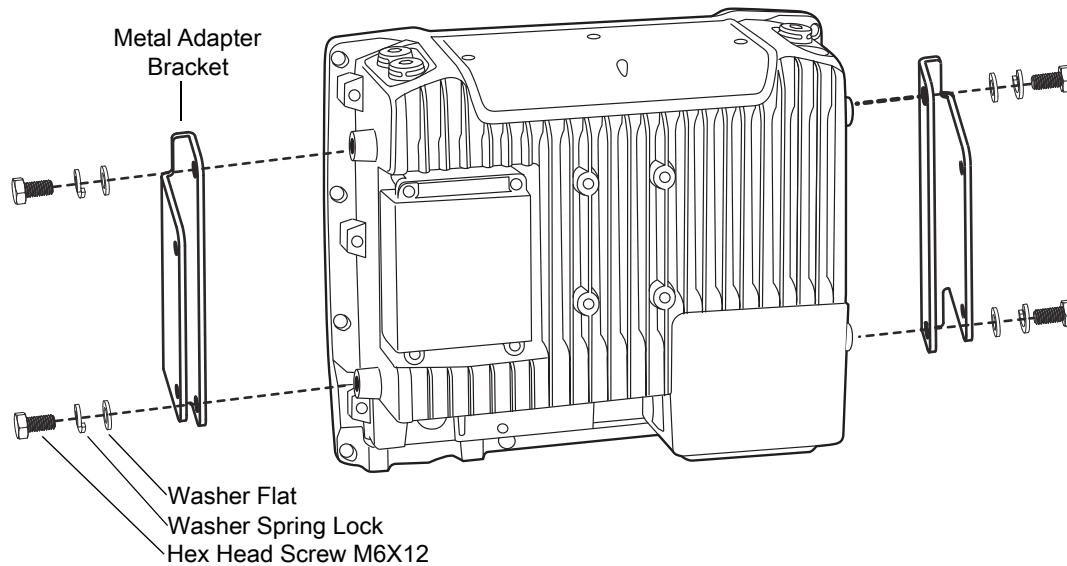
MT4210 Adapter Bracket

The MT4210 Adapter Bracket is for use with older mounts, such as the 82XX Quick Release Mount.

To assemble the MT4210 Adapter Bracket:

1. Line up the MT4210 mounting bracket holes with the holes on the sides of the VC8300 (two on each side).
2. Place the spring lock washer onto the hex head screw.
3. Place the flat washer onto the hex head screw (on top of the washer spring lock).
4. Screw the metal adapter bracket onto the VC8300 (total of four). Torque to 34.7 in-lbs.

Figure 94 MT4210 Adapter Bracket Assembly



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.

Profiles

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

Profile information consists of:

- Associated application
- Data Capture Plus configurations
- Input plug-in configurations
- Output plug-in configurations
- Process plug-in configurations.

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

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

- 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.

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.

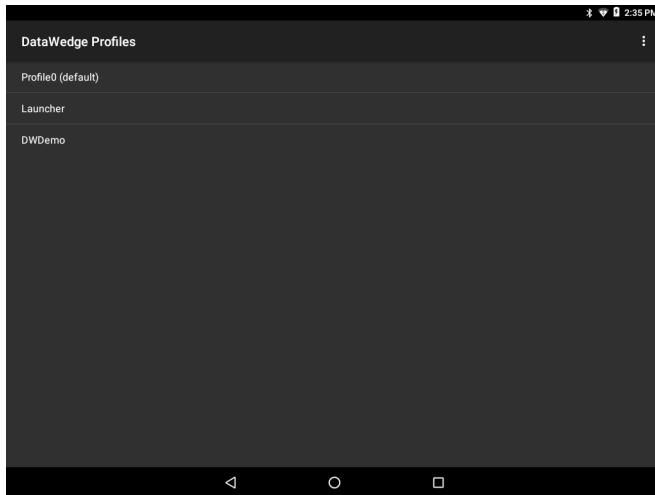
Profiles Screen

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 95 DataWedge Profiles Screen



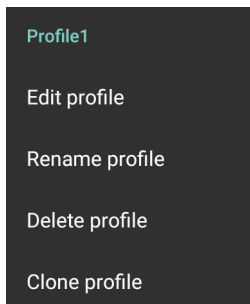
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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 96 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


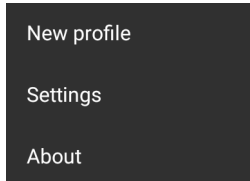


Touch  to open the options menu.

Figure 97 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:



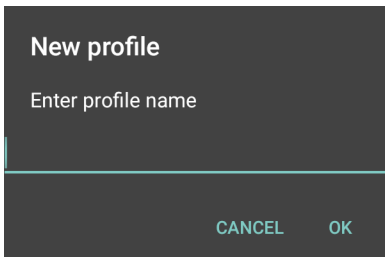
1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **New profile**.
4. In the **New profile** dialog box, enter a name for the new profile. It is recommended that profile names be unique and made up of only alpha-numeric characters (A-Z, a-z, 0-9).

Figure 98 New Profile Name Dialog Box



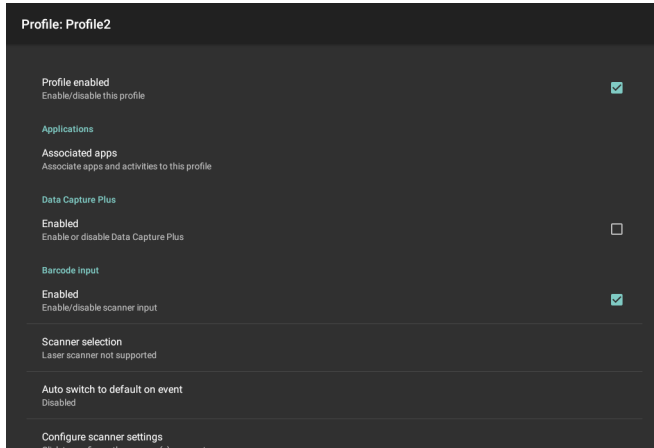
5. Touch **OK**.

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 99 Profile Configuration Screen



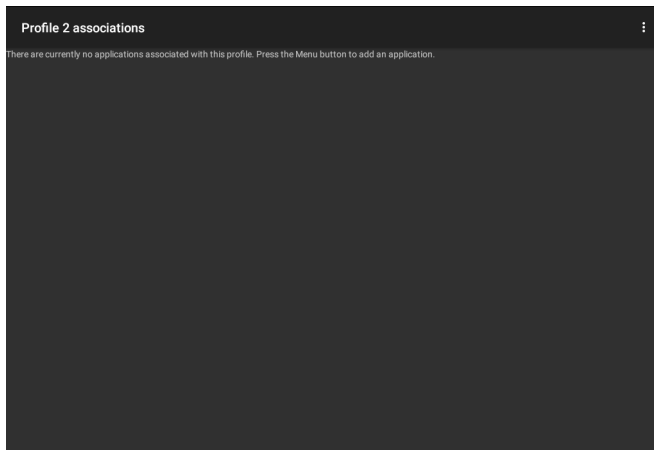
The configuration screen lists the following sections:

- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode Input
- Serial port input from Serial Port 1
- Serial port input from Serial Port 2
- Voice input
- Keystroke output
- Intent Output
- IP Output.

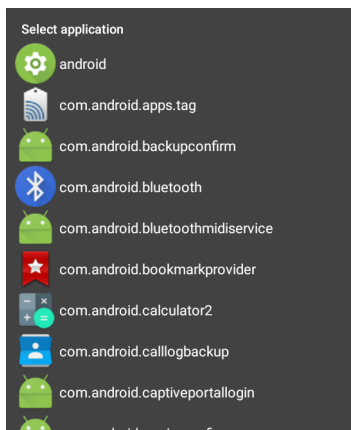
Associating Applications

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

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

Figure 100 Associated Apps Screen

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

Figure 101 Select Application Menu


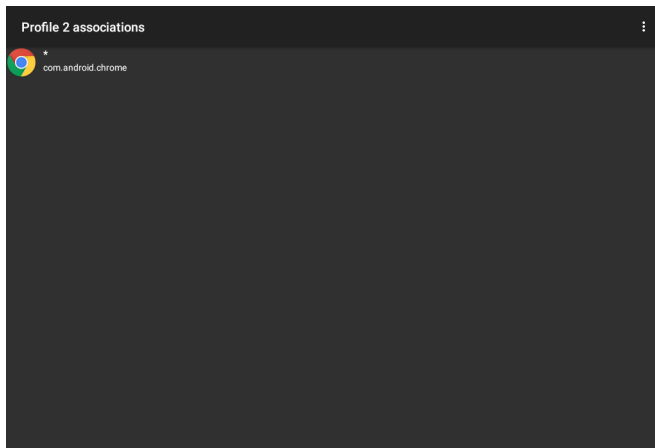
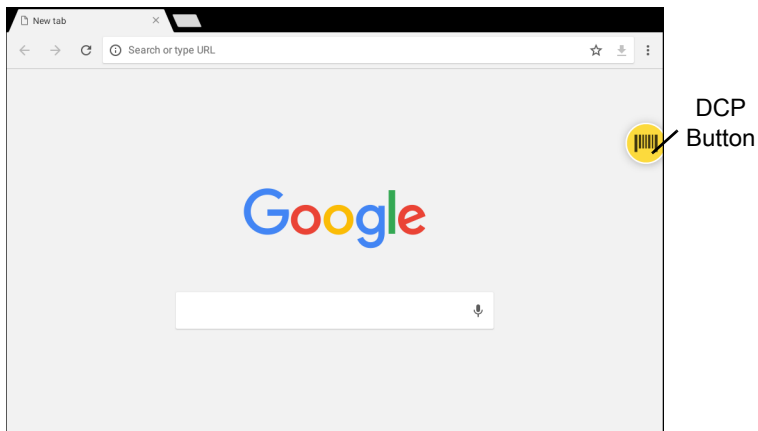
4. In the **Select application** screen, select the desired application from the list.
5. In the **Select activity** menu, selecting the activity adds that application/activity combination to the associated application list for that profile. Selecting * as the activity results in all activities within 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 102 Selected Application/Activity

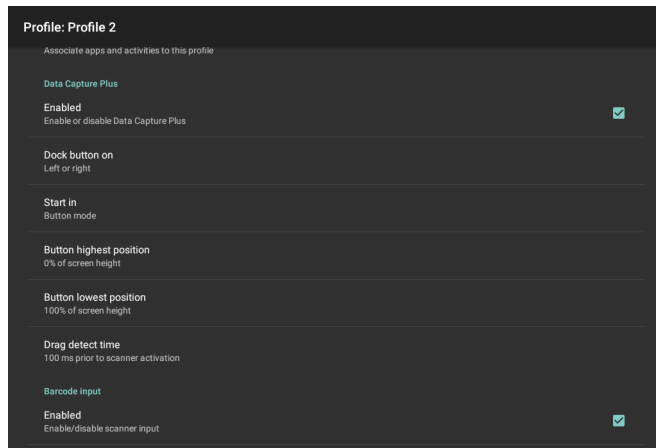
Data Capture Plus

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 103 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 104 Data Capture Panel Settings



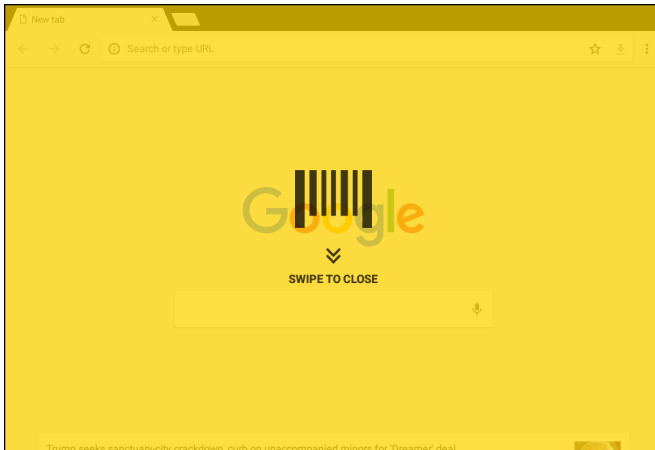
- **Enable** - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
 - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
 - **Left only** - Places the button on left edge of the screen.
 - **Right 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 105 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.
- **DS3608 USB SSI Scanner** - Scanning is performed using the optional USB scanner.
- **Bluetooth Scanner** - Scanning is performed using the optional Bluetooth scanner.
- **RS6000 Bluetooth Scanner** - Scanning is performed using the RS6000 Bluetooth scanner.
- **DS3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.
- **LI3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.
- **DS2278 Bluetooth Scanner** - Scanning is performed using the DS2278 Bluetooth scanner.
- **LI3608 USB SSI Scanner** - Scanning is performed using the optional USB scanner.

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.

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 15 Supported Decoders

Decoders	RS507/RS507X	RS6000	DS2278	DS36x8	LI36x8
Australian Postal	O	O	O	O	--
Aztec	X	X	X	X	--
Canadian Postal	--	O	--	--	--
Chinese 2 of 5	O	O	O	O	O
Codabar	X	X	X	X	X
Code 11	O	O	O	O	O
Code 128	X	X	X	X	X
Code 39	X	X	X	X	X
Code 93	O	O	O	O	O
Composite AB	O	O	O	O	--
Composite C	O	O	O	O	--
Discrete 2 of 5	O	O	O	O	O
Datamatrix	X	X	X	X	--
Dutch Postal	O	O	O	O	--
DotCode	O	O	O	O	O
EAN13	X	X	X	X	X
EAN8	X	X	X	X	X
GS1 DataBar	X	X	X	X	X

Table 15 Supported Decoders (Continued)

Decoders	RS507/RS507X	RS6000	DS2278	DS36x8	LI36x8
GS1 DataBar Expanded	X	X	X	X	X
GS1 DataBar Limited	O	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	O
Japanese Postal	O	O	O	O	--
Korean 3 of 5	O	O	O	O	O
MAIL MARK	--	X	X	X	--
Matrix 2 of 5	O	O	O	O	O
Maxicode	X	X	X	X	--
MicroPDF	O	O	O	O	--
MicroQR	O	O	O	O	--
MSI	O	O	O	O	O
PDF417	X	X	X	X	--
QR Code	X	X	X	X	--
Decoder Signature	O	O	O	--	--
TLC 39	O	O	O	O	O
Trioptic 39	O	O	O	O	O
UK Postal	O	O	O	O	--
UPCA	X	X	X	X	X
UPCE0	X	X	X	X	X
UPCE1	O	O	O	O	O
US4state	O	O	O	O	--
US4state FICS	O	O	O	O	--
US Planet	O	O	O	O	--
US Postnet	O	O	O	O	--

Touch  to return to the previous screen.

Decoder Params

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



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

Codabar

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

Code 11

- **Length1** - Use to set decode lengths (default - 4). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).
- **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 barcode.
 - **No Check Digit** - Do not verify check digit.
 - **1 Check Digit** - Barcode contains one check digit (default).
 - **2 Check Digits** - Barcode contains two check digits.

Code128

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 barcodes (default - disabled).
- **Ignore Code128 FNC4** - When enabled, and a Code 128 barcode has an embedded FNC4 character, it will be removed from the data and the following characters will not be changed. When the feature is disabled, the FNC4 character will not be transmitted but the following character will have 128 added to it (default - disabled).
- **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT barcodes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable Plain Code128** - Set the Plain Code128 subtype. Enables other (non-EAN or ISBT) Code 128 subtypes. A check in the checkbox indicates that the option is enabled (default - enabled).
- **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:
 - **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
 - **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
 - **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge

Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.

- **Length1** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Security Level** - The scanner offers four levels of decode security for Code 128 barcodes. Select increasing levels of security for decreasing levels of barcode quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.
 - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” barcodes.
 - **Security Level 1** - This setting eliminates most misdecodes (default).
 - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
 - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec barcodes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the barcodes.

Code39

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

Code93

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

Composite AB

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

Discrete 2 of 5

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

GS1 DataBar Limited

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

HAN XIN

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

Interleaved 2 of 5

- **Febraban** - Enable to insert special check characters in the transmitted data stream of Interleaved 2 of 5 barcodes which are of length 14 and meet specific Febraban criteria. A check in the checkbox indicates that the option is enabled (default - disabled).

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

Matrix 2 of 5

- **Length1** - Use to set decode lengths (default - 10). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).
- **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).

MSI

- **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
 - **One Check Digit** - Verify one check digit (default).
 - **Two Check Digits** - Verify two check digits.
- **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
 - **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
 - **Mod-10-10** - Both check digits are MOD 10.
- **Length 1** - Use to set decode lengths (default - 4). See Decode Lengths for more information.
- **Length 2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **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).

UK Postal

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

UPCA

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

There are three options for transmitting a UPCA preamble:

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

UPCE0

- **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).
- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.
There are three options for transmitting a UPCE0 preamble:
 - **Preamble None** - Transmit no preamble (default).
 - **Preamble Sys Char** - Transmit System Character only.
 - **Preamble Country and Sys Char** - Transmit System Character and Country Code ("0" for USA).
- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

UPCE1

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

US Planet

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

Decode Lengths

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

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

UPC EAN Params

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



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

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar barcodes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC barcodes. (default - disabled)
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **Bookland Format** - If Bookland EAN is enabled, select one of the following formats for Bookland data:
 - **Format ISBN-10** - The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
 - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **Coupon Report Mode** - Traditional coupon symbols are composed of two barcode: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded barcode. The new format offers more options for purchase values (up to \$999.999) and supports complex discount offers as a second purchase requirement. An interim coupon symbol also exists that contain both types of barcodes: UPC/EAN and

Databar Expanded. This format accommodates both retailers that do not recognize or use the additional information included in the new coupon symbol, as well as those who can process new coupon symbols.

- **Old Coupon Report Mode** - Scanning an old coupon symbol reports both UPC and Code 128, scanning an interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
- **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
- **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded. (default)
- **Ean Zero Extend** – Enable this parameter to add five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols. Disable this to transmit EAN-8 symbols as is. Default – disabled.
- **Linear Decode** - This option applies to code types containing two adjacent blocks, for example, UPC-A, EAN-8, EAN-13. Enable this parameter to transmit a bar code only when both the left and right blocks are successfully decoded within one laser scan. Enable this option when bar codes are in proximity to each other (default - enabled).
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).
- **Security Level** - The scanner offers four levels of decode security for UPC/EAN barcodes. Select higher security levels for lower quality barcodes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
 - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding “in-spec” UPC/EAN barcodes.
 - **Level 1** - As barcode quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed barcodes, and the misdecodes are limited to these characters, select this security level. (default).
 - **Level 2** - If the scanner is misdecoding poorly printed barcodes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
 - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec barcodes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the barcodes.
- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
 - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
 - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
 - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the barcode the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
 - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378,

379, 977, 978, 979, 414, 419, 434 or 439. If the barcode starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.

- **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN barcode not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN barcode not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN barcode 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.

Reader Params

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



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

- **Character Set Configuration** - Used to support the GB2312 Chinese characters encoding.
- **Character Set Selection** - Allows the user to convert the barcode data if different from default encoding type.
 - **Auto Character Set Selection (Best Effort)** - Automatic character convert option. Tries to decode data from the Preferred selection. The first correct decodable character set is used to convert the data and is sent.
 - **ISO-8859-1** - Part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
 - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
 - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.
 - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
- **Auto Character Set Preferred Order** - In **Auto Character Set Selection** mode, the system will try to decode the data in a preference order of character sets. The algorithm used is a best effort one. That is, there could be cases where the data can be decoded from more than one character set. The first character set from the preferred list which can decode the data successfully will be chosen to decode the data and sent to the user. Any other character set that is in the list but lower in the preferred order, would not be considered, even if the data could be successfully decoded using such character set.

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

- **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).

- **GB2312** - Character set of the People's Republic of China, used for simplified Chinese characters.
- **Auto Character Set Failure Option** - If the system cannot find a character set from the preferred list that can be used to successfully decode the data, the character set selected in **Auto Character Set Failure Option** is used to decode the data and send to the user. If **NONE** is used, Null data is returned as string data.
 - **NONE**
 - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
 - **ISO-8859-1** - Part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
 - **Shift_JIS** - ended for Western European languages.
 - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
 - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.
- **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 **Multibarcodes** can be set to read from 2 to 10 barcodes on a single scan.

Scan Params

Allows the configuration of Code ID and decode feedback options.



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

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

- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).
- **Decode Feedback LED Timer** - Set the amount of time (in milliseconds) that the green Data Capture LED stays lit after a good decode. (default - 75 msec.)
- **Beep Volume Control** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.



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

- **Ringer** - 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).

Multibarcodes params

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

Serial Port Input from Serial Port 1

Use to configure an RS-232 scanner connected to COM Port 1.

- **Enabled** - Touch checkbox to enable scanner input from COM port 1.
- **Serial Port Configuration** - Use to configure COM port settings. For Zebra scanners, correct settings are set as default.
 - **Baud rate** - Select baud rate for scanner (default - 9600).
 - **Data bits** - Select data bits for scanner. Options: **7**, or **8** (default)
 - **Parity** - Select data bits for scanner. Options: **None** (default), **Odd**, **Even**, **Mark**, or **Space**.
 - **Stop bits** - Select data bits for scanner. Options: **1** (default), or **2**.

Serial Port Input from Serial Port 2

Use to configure an RS-232 scanner connected to COM Port 2.

- **Enabled** - Touch checkbox to enable scanner input from COM port 2.

- **Serial Port Configuration** - Use to configure COM port settings. For Zebra scanners, correct settings are set as default.
 - **Baud rate** - Select baud rate for scanner (default - 9600).
 - **Data bits** - Select data bits for scanner. Options: **7**, or **8** (default)
 - **Parity** - Select data bits for scanner. Options: **None** (default), **Odd**, **Even**, **Mark**, or **Space**.
 - **Stop bits** - Select data bits for scanner. Options: **1** (default), or **2**.

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 Multibyte 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.

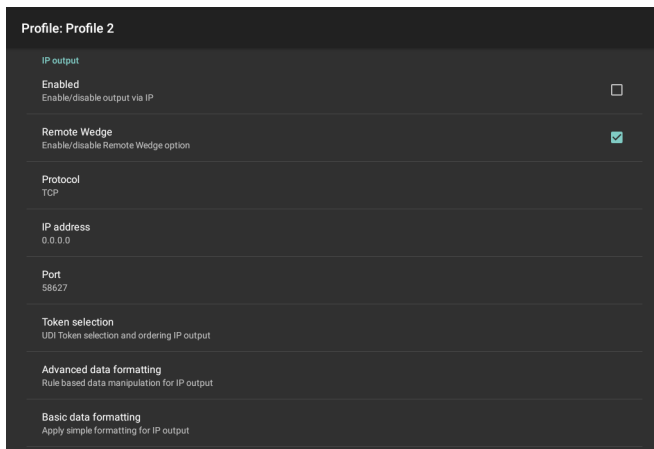
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol 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 Multibarcodes data.
 - **UDI specific** - Allows the output order of acquired UDI data to be adjusted and the optional insertion of a tab, line feed, or carriage return character between tokens.
 - **Send tokens** - Set to select the output format for UDI data. (default - disabled)
 - **Token separator** - Set to select a separator character. If no separator character is selected when Send tokens is set to Barcodes and tokens, two instances of the same data are sent. (default - none)
 - **Token order** - Set to include or exclude Tokens from the output and adjust their output order.
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
 - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
 - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See Generating Advanced Data Formatting Rules for more information.

- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
 - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
 - **Prefix to data** - Add characters to the beginning of the data when sent.
 - **Suffix to data** - Add characters to the end of the data when sent.
 - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
 - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Usage

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

Figure 106 IP Output Screen



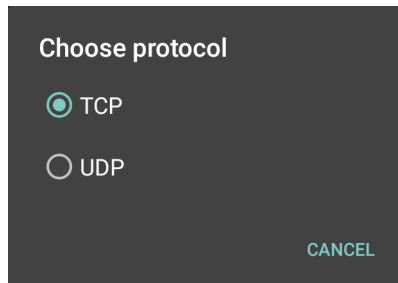
Using IP Output with IPWedge

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**.

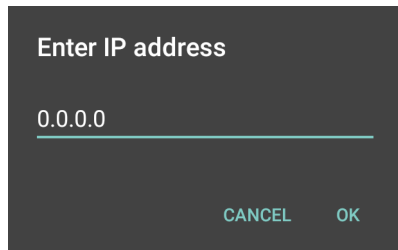
- In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).

Figure 107 Protocol Selection



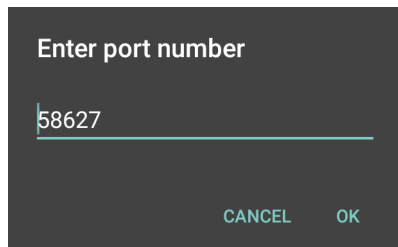
- Touch **IP Address**.
- In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

Figure 108 IP Address Entry



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

Figure 109 Port Number Entry



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

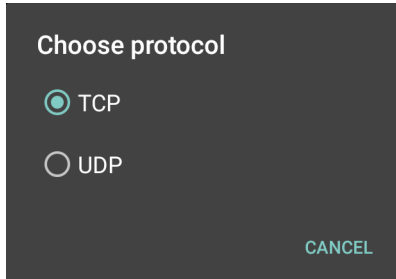
Using IP Output without IPWedge

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:

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

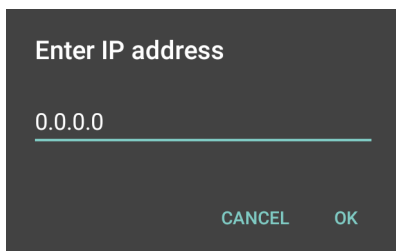
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

Figure 110 Protocol Selection



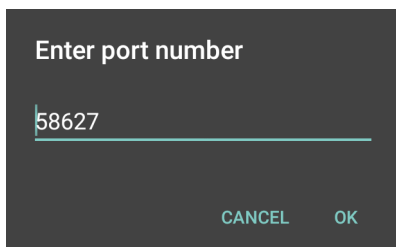
5. Touch **IP Address**.
6. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.

Figure 111 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 112 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.


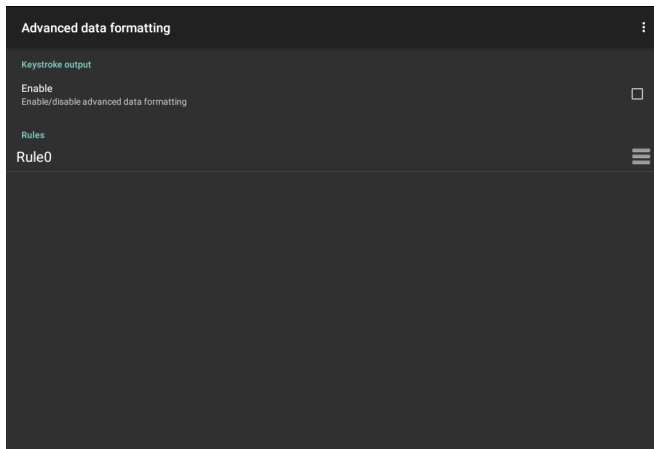
1. Swipe up from the bottom of the screen and touch .
2. Touch a DataWedge profile.
3. In **Keystroke Output**, touch **Advanced data formatting**.

Figure 113 Advanced Data Formatting Screen



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

Creating a Rule



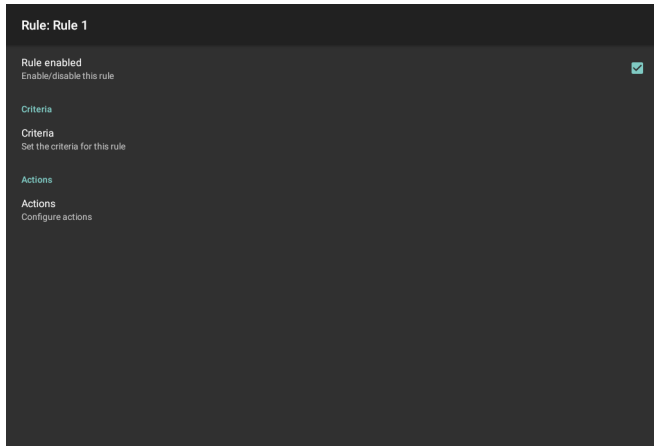
NOTE: By default, **Rule0**, is the only rule in the Rules list.

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 114 Rule List Screen

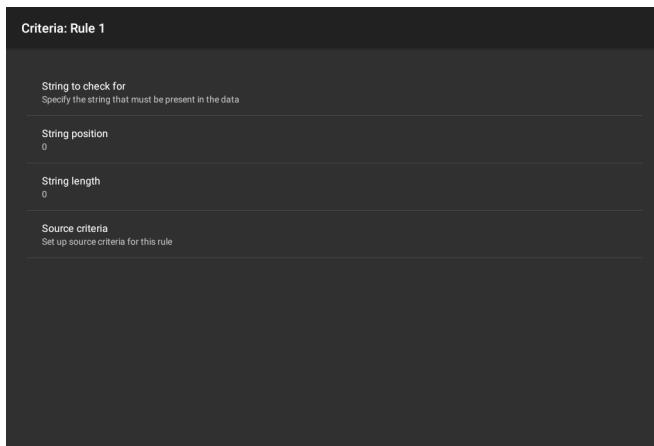


2. Touch the **Rule enabled** check box to enable the current rule.

Defining Criteria

1. Touch **Criteria**.

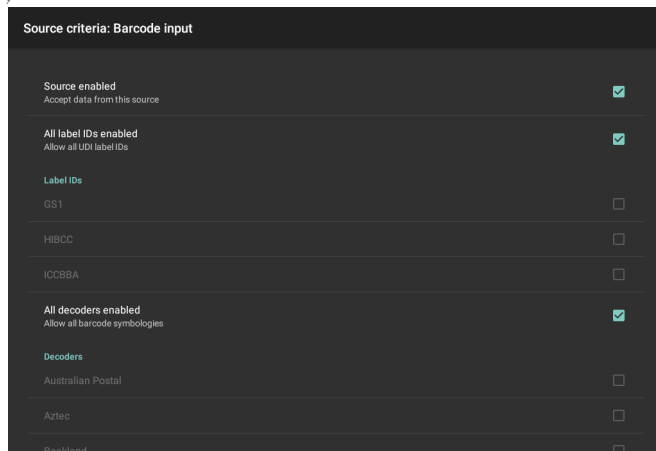
Figure 115 Criteria Screen





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 116 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 16 ADF Supported Actions

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

Table 16 ADF Supported Actions (Continued)

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

Deleting an Action

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:


When a user scans a 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**.


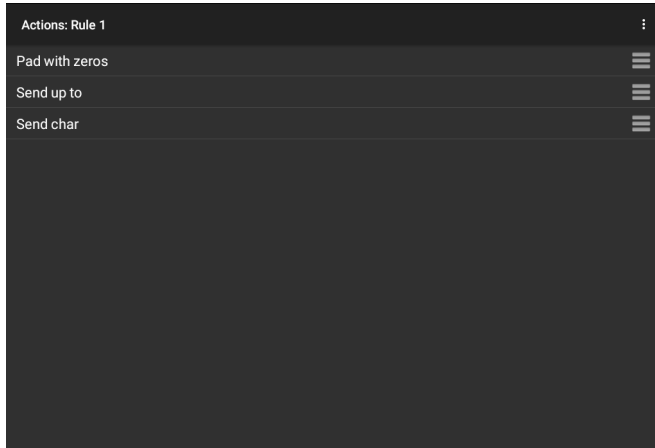
45. Touch .

Figure 117 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 118 Sample Barcode



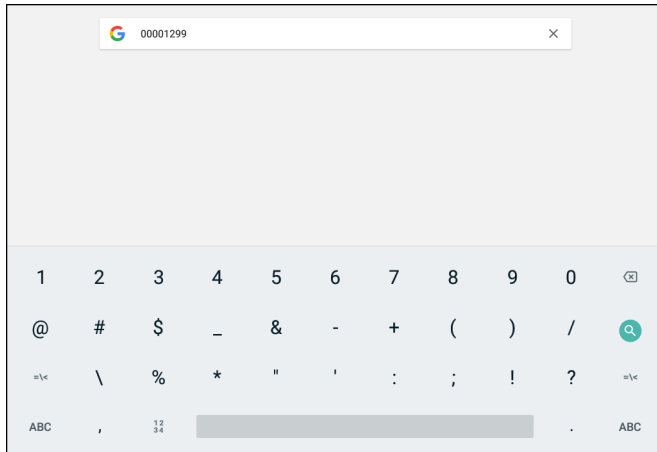
48. Press and hold the scan button.

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 scanner 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.

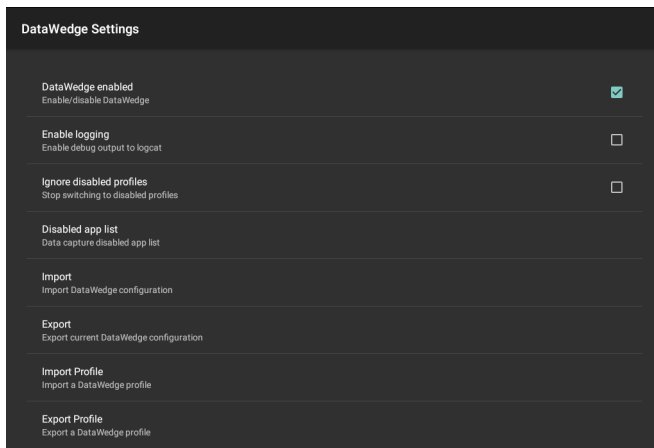
Figure 119 Formatted Data



DataWedge Settings

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



Figure 120 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**.

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.

To enable Reporting:

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **Reporting**.
5. Select the **Reporting enabled** check box.

Configuration and Profile File Management

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

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

Enterprise Folder

Internal storage contains the Enterprise folder (`/enterprise`). The Enterprise folder is persistent and maintains data after an Enterprise reset. After an Enterprise Reset, DataWedge checks folder `/enterprise/device/settings/datawedge/enterpriseset/` 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 `/enterpriseset` folders must be done programmatically, or with a staging client app or MDM.

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application



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

Capture Data and Taking a Photo in the Same Application

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

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

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.

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>");
```

Scanner Input Plugin

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



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

Function Prototype

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

Parameters

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

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

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

- "ENABLE_PLUGIN" - enables the plug-in

- "DISABLE_PLUGIN" - disables the plug-in

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, 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 registerReceiver(){
    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 unregisterReceiver(){
    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**

Settings



Introduction

This chapter describes settings available for configuring the device.

Setting the Date and Time

You are only required to set the time zone or set the date and time 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 **Update Interval**.
5. Select the interval time to synchronize your device time from the network.
6. Touch **Set date**.
7. In the calendar, set today's date.
8. Touch **OK**.
9. Touch **Set time**.
10. Touch the green circle, drag to the current hour and then release.
11. Touch the green circle, drag to the current minute and then release.
12. Touch **AM** or **PM**.
13. Touch **OK**.
14. Touch **Select time zone**.
15. Select the current time zone from the list.
16. Touch **Use 24-hour format**.
17. Touch .

Display Setting

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

Setting the Screen Brightness

To manually set the screen brightness press the Blue button twice to lock the button. Use the Display Brightness control keys to adjust the screen brightness.

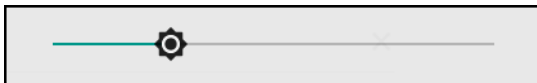
Figure 121 Brightness Control Keys



Alternately:



1. Swipe down with two fingers from the status bar to open the quick access panel.
2. Slide the brightness icon to adjust the screen brightness level.

Figure 122 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 > Sleep**.
3. Select one of the sleep values.
 - **15 seconds**
 - **30 seconds**
 - **1 minute** (default)
 - **2 minutes**
 - **5 minutes**
 - **10 minutes**
 - **30 minutes.**
4. Touch .

Setting Font Size

To set the size of the font in system apps:


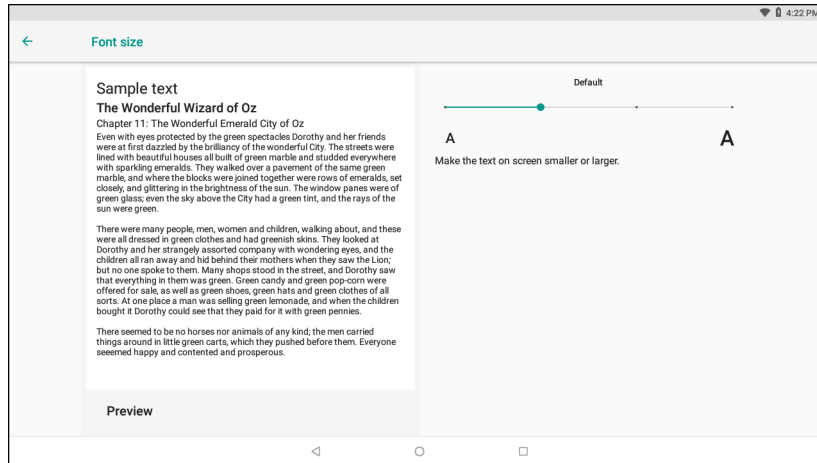

1. Swipe down from the Status bar to open the Quick Settings panel and then touch .
2. Touch **Display > Advanced**.
3. Touch **Font size**.

Figure 123 Font Settings




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

Setting Screen Rotation

By default, screen rotation is enabled.

To disable screen rotation:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **Display > Advanced**.
3. Touch **Auto-rotate screen**.



NOTE: To change the Home screen rotation, see Setting Home Screen Rotation.

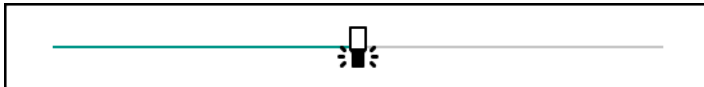
4. Touch .

The Keyboard Backlight

The intensity of the keyboard backlight and the conditions under which this backlight is activated can be configured by opening the Keyboard Light settings.

1. Swipe down select settings.
2. Touch **Display > Advanced > Keyboard backlight**.
3. Touch **Keyboard light level**. A slider appears.

Figure 124 Keyboard Light Level Slider



4. Adjust the light level by sliding the icon. Change level by 10% increments.
5. Touch **Keyboard light timeout**. The Keyboard light timeout dialog appears.
6. Select the amount of time that the backlight stays on before turning off.
 - 6 seconds (default)
 - 10 seconds
 - 15 seconds
 - 30 seconds
 - 1 minute
 - 2 minute
 - 5 minute
 - Always on.

General Sound Setting

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

To access sound settings:


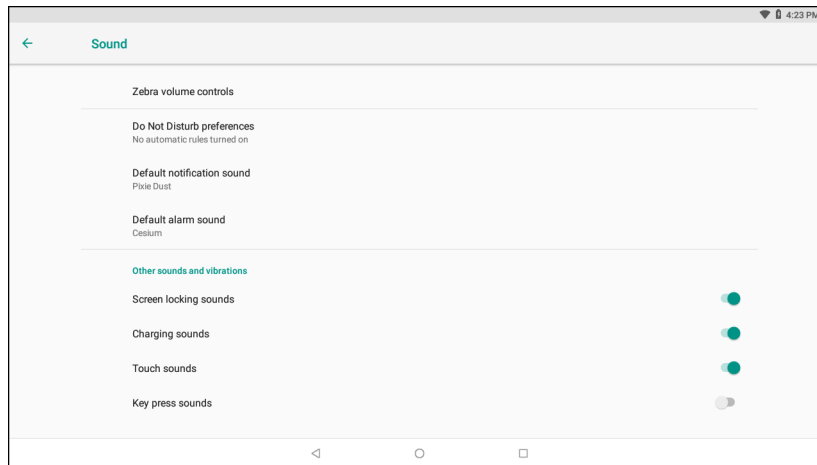


1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **Sound**.
3. Touch an option to set sounds.

Figure 125 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.
 -  - Enables all sounds at the user defined levels.
- **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.
 - **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**.
- **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**

- **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).
- **Key press sounds** - Play a sound when making keyboard button selections (default – disabled)

Do Not Disturb Feature

This mode mutes the device so that it does not make sounds.

For example, use Do Not Disturb to:

- Automatically limit sounds at night or during events
- Mute interruptions other than alarms
- Get alerted to messages only from favorite contacts.

Limit Sounds and Vibrations

Mute the device completely, or let through the important alarms or important calls.

Total Silence

To completely mute the device so that it does not make a sound, choose **Total silence**.


In Total silence mode:

- Alarms do not make noise.
- Device does not make sounds when receiving a message, or notification.
- Sounds from music, videos, games, and other media are muted.



NOTE: All alarms are silenced in Total silence mode.

1. Swipe down with two fingers from the Status bar to open the Quick Access panel.
2. Touch **Do not disturb > Total silence**.
3. Choose **Until you turn it off** or select a time period.
4. Touch **Done**.

When Total Silence is on,  appears in the quick access panel and the Status bar.


To turn off Total Silence, open quick access panel and touch **Total silence**.

Alarms Only

To mute the device so that you hear alarms, choose **Alarms only**. This option does not mute sounds from music, videos, games, or other media.

1. Swipe down with two fingers from the status bar to open the quick access panel.
2. Touch **Do not disturb > Alarms only**.
3. Choose **Until you turn it off** or select a time period.

4. Touch **Done**.

When Alarms Only is on,  appears in the quick access panel and the Status Bar.

To turn off Alarms Only, open the Quick Access panel and touch **Alarms only**.



NOTE: To quickly turn on Alarms Only, with the screen on, press and hold the Volume Down button until the volume is all the way down. Then, press Volume Down again to turn on Alarms Only.


To turn off Alarms Only, press either the Volume Up or Volume Down button and the touch **END NOW** in the alert message.

Automatically Block Sounds and Vibrations

Automatically silence the device during certain times or events, turn sounds back on, and override Do Not Disturb mode.


Silence Sounds During Certain Times

To automatically silence the device during certain times, like at night or on weekends:

1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **Sound > Do Not Disturb preferences**.
3. Touch a default **Weekend** or **Weeknight**. Or, to make a new rule, touch **Add more > Time rule**.
4. Enter a rule name.
5. Touch **OK**.
6. Edit the new rule:
 - **Rule name** - Rename the rule.
 - **Days, Start time, and End time** - Set the rule's schedule.
 - **Do Not Disturb preferences** - Choose whether the rule uses **Alarms only**, **Priority only**, or **Total silence**.
 - **Alarm can override end time** - Allow the alarm to continue to make sound until the next alarm begins.
7. Touch the On/Off switch at the top to turn on the rule.



Silence Sounds During Events and Meetings

To automatically silence the device during events or meetings, set an event rules.

1. Swipe down from the Status bar to open the Quick Settings bar and then touch .
2. Touch **Sound > Do Not Disturb preferences**.
3. To edit the default rule, touch **Event**. Or, to create a new rule, touch **Add rule > Event rule**.

4. Edit the rule settings.
 - **Rule name** - Rename the rule.
 - **During events for** - Select which Google Calendar events the rule uses.
 - **Where reply is** - Set to: **Yes, Maybe, or Not replied, Yes or Maybe, or Yes.**
 - **Do Not Disturb preferences** - Choose whether the rule uses **Priority only, Alarms only, or Total silence.**
5. Touch the On/Off switch at the top to turn on the rule.

Turn Sounds Back On


When the device is in Do Not Disturb mode, Alarms only or Priority only display as , or Total silence displays as .

To turn off Do Not Disturb, either:

- In the Quick Access panel, touch **Alarms only, Priority only, or Total silence.**
- Press the Volume Down button and touch **End Now.**

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


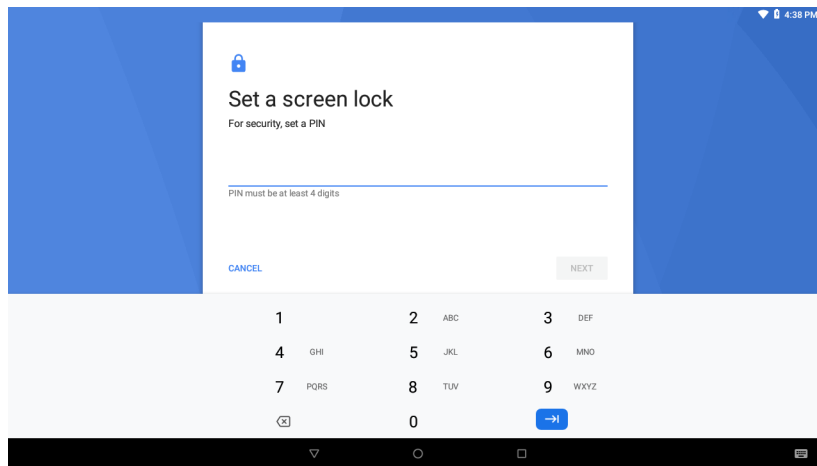

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. To require a PIN upon device start up select **Yes**, or select **No** not to require a PIN.

Figure 126 PIN Screen



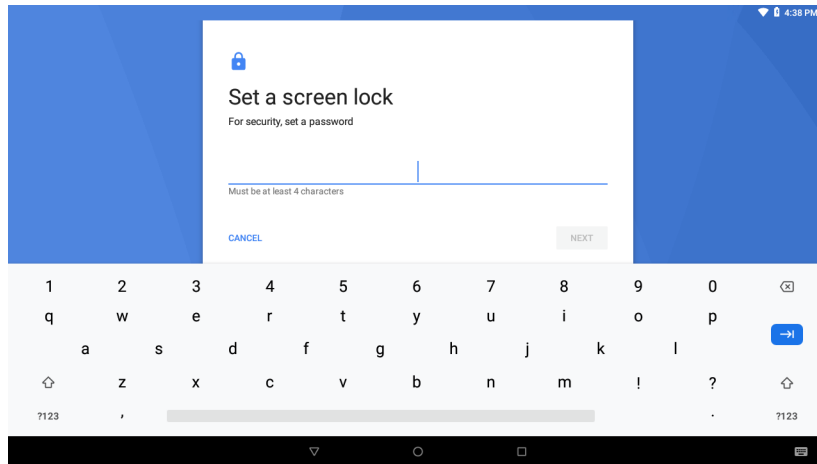
6. Touch in the text field.
7. Enter a PIN (4 numbers) then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch . The next time the device goes into suspend mode a PIN is required upon waking.

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 127 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


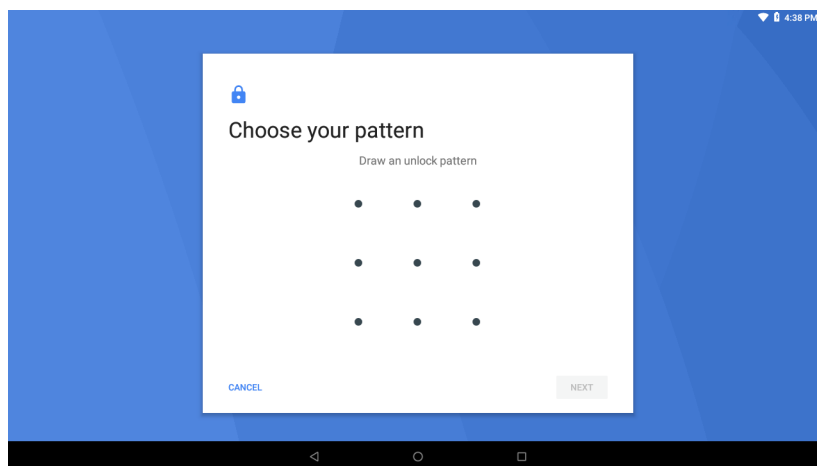

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Pattern**.
5. To require a pattern upon device start up select **Yes**, or select **No** not to require a pattern.

Figure 128 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.

Passwords



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

1. Swipe down from the status bar and then touch  > **Security & location**.
2. Slide the **Show passwords** switch to the ON position.




System Language Usage

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


Adding Languages




1. Swipe down from the status bar and then touch .
2. Touch **System > Language & input**.
3. Touch **Languages**.
4. Touch **Add a language**.
5. Scroll through the list and touch a language. The language appears in the language list.
6. Touch .

Selecting a Language



1. Swipe down from the status bar and then touch .
2. Touch **System > Language & input**.
3. Touch **Languages**.
4. Touch and drag a language to the top of the list.
5. Touch . The operating system text changes to the selected language.
6. Touch .

Removing a Language

1. Swipe down from the status bar and then touch .
2. Touch **System > Language & input**.

3. Touch **Languages**.
4. Touch .
5. Touch **Remove**.
6. Select the languages to remove.
7. Touch .
8. Touch **OK**.
9. Touch .

Adding Words to the Dictionary

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

Virtual Keyboard Settings


Use the **Language & input** settings for configuring the on-screen virtual keyboards.

Enterprise Keyboard Configuration

Upon initial boot-up of the device, the **Enterprise Keyboard** app appears in the All Apps window. Run the app to enable and configure the Enterprise keyboard. After configuration, the app disappears from the All Apps windows.

Enabling Keyboards

To enable the installed virtual keyboard:

1. Swipe down from the status bar and then touch .
2. Touch **System > Language & input**.
3. Touch **Virtual keyboard**.
4. Touch **Manage keyboards**.
5. Touch one or more of the keyboard input method switches.
6. Touch **OK**.

7. Touch ←.

Configuring the GBoard Keyboard

To configure the GBoard keyboard:

1. Touch and hold (comma) > ⚙️. The **Preferences** screen appears.
2. Select **Languages** to change the language layout of the keyboard.
By default, the keyboard uses the default system languages. To override the system languages:
 - a. Touch **Use system languages** to disable the default setting.
 - b. Scroll through the list and select languages for the keyboard.
 - c. Touch ←.

Configuring the Enterprise Keyboard

To configure the Enterprise keyboard:

Settings

Select **System** > **Languages & input** > **Virtual keyboard** > **Enterprise keyboard**.

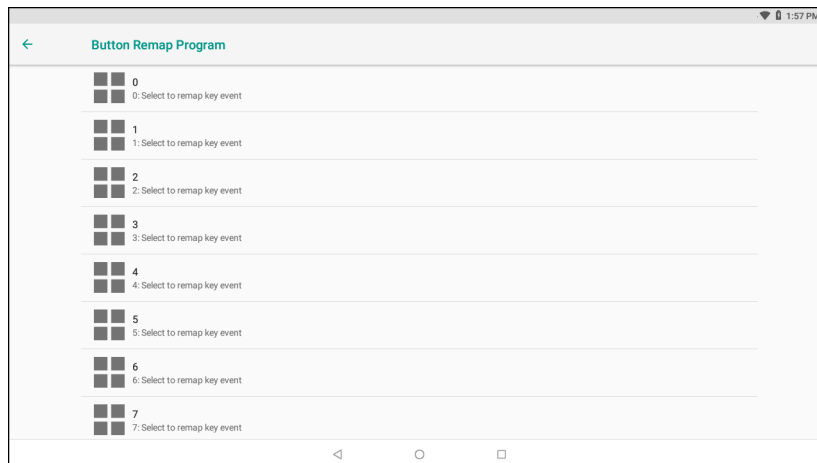
Key Programmer

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

Remapping a Button

1. Swipe down from the status bar and then touch ⚙️.
2. Touch **Key Programmer**.

Figure 129 Key Programmer Screen

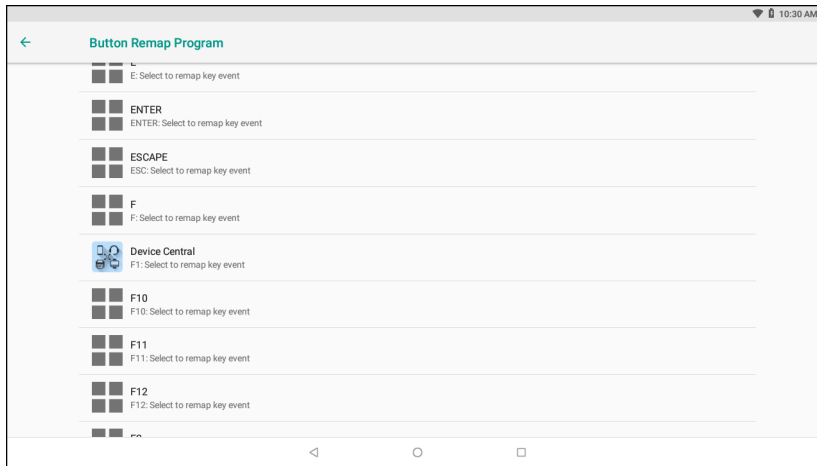



3. Select the button to remap.
4. Touch the **BUTTON REMAPPING**, or **SHORTCUT** tab that lists the available functions and applications.
5. Touch a function or application shortcut to map to the button.



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

Figure 130 Remapped Button



6. Touch .

About Phone

Use About phone settings to view information about the device. Swipe down with two fingers 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.
 - **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 device's 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.

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.

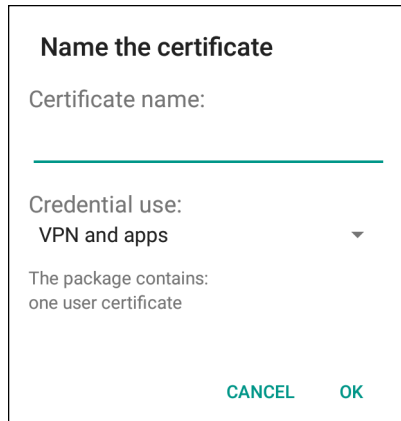
Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the USB drive or 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 131 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 USB drive or 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**.
 - **Trusted credentials** - Touch to display the trusted system and user credentials.
 - **Install from storage** - Touch to install a secure certificate from the USB drive or 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.
- documentation.html and docs directory
 - The SDK documentation is provided locally and on the Web. It's largely in the form of JavaDocs, making it easy to navigate the many packages in the SDK. The documentation also includes a high-level Development Guide and links to the broader community.
- Samples directory
 - The samples subdirectory contains full source code for a variety of applications, including ApiDemo, which exercises many APIs. The sample application is a great place to explore when starting application development.
- Tools directory
 - Contains all of the command-line tools to build applications. The most commonly employed and useful tool is the adb utility.
- usb_driver
 - Directory containing the necessary drivers to connect the development environment to an enabled device. These files are only required for developers using the Windows platform.

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

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



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.
The **Allow USB debugging?** dialog box appears on the device.
10. On the device, touch **OK**.
11. On the host computer, navigate to the **platform-tools** folder.
12. Type **adb devices**.
The following displays:
List of devices attached
XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

13. Touch .

Application Installation

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

- USB drive, see [Installing Applications Using a USB Drive on page 200](#).
- Android Debug Bridge, see [Installing Applications Using the Android Debug Bridge on page 201](#).
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

Installing Applications Using a USB Drive



IMPORTANT: USB Drive must have FAT32 format.

1. Plug the USB drive into the USB port on the host computer.
2. On the host computer, open a file explorer application.
3. Copy the application `.apk` file from the host computer to the USB drive.
4. Eject the USB drive from the host computer.



CAUTION: Follow the host computer's instructions to eject the USB drive correctly to avoid losing information.


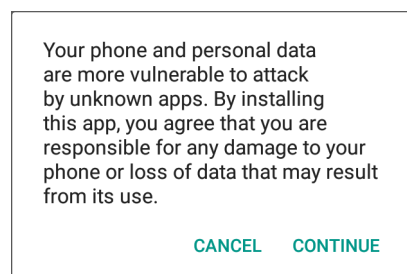
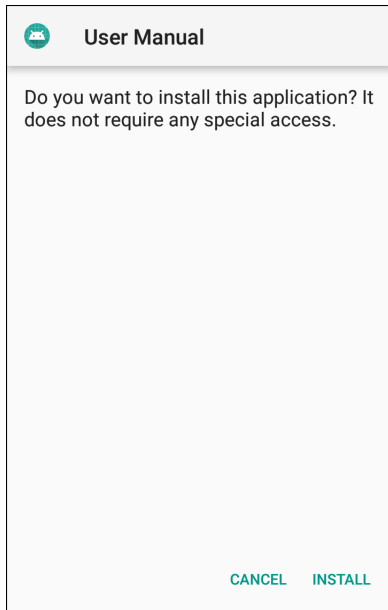
5. Remove the dust cover on the back of the device. See [Figure 3 on page 20](#).
6. Plug the USB drive into the USB port on the device, see [Figure 4 on page 20](#). A notification appears indicating that the device detected the USB drive.
7. Swipe the screen up and select  to view files on the USB drive.
8. Touch **General USB drive**.
9. Locate the application `.apk` file.
10. Touch the application file.

Figure 132 Install App Permission Dialog Box



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

Figure 133 Accept Installation Screen



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

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

14. Disconnect the USB drive from the host computer.

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

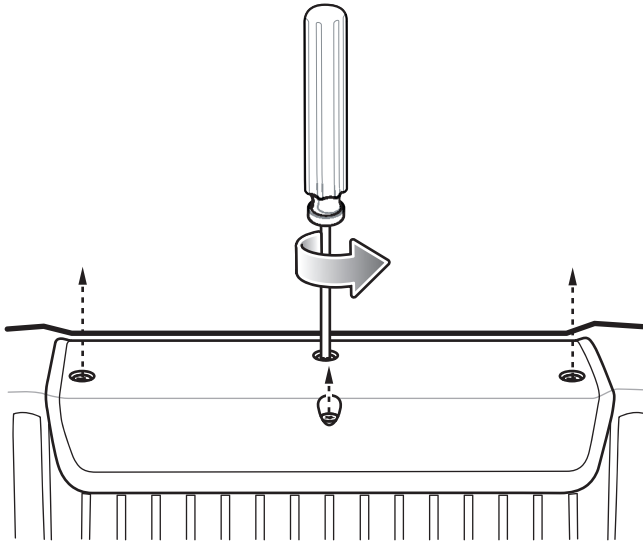


CAUTION: When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.


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

1. Using a T10 Torx screwdriver, remove four screws securing the top cover to the device.

Figure 134 Remove Top Cover

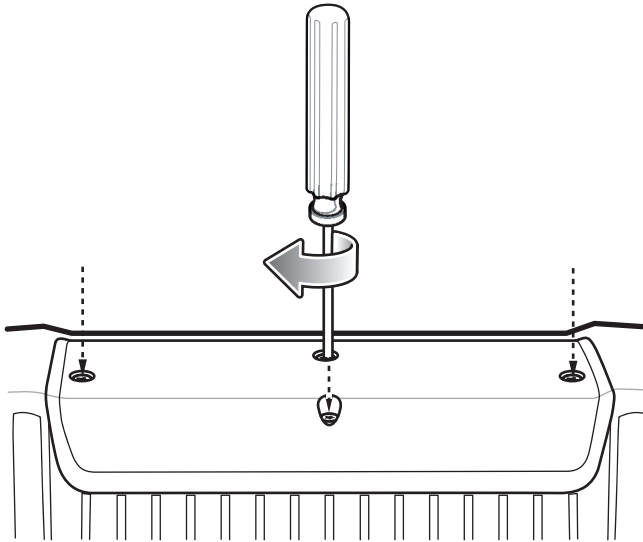


IMPORTANT: When the user connects a USB cable to the USB port on top of the device, the USB and RS-232 ports on the bottom are disabled.

2. Connect the device to a host computer using USB. See USB Communication.
3. 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 install <application>
where: <application> = the path and filename of the apk file.
9. Disconnect the device from the host computer. See USB Communication. Replace the top cover.

10. Secure the top cover to the device using the four screws.

Figure 135 Replace Top Cover



11. Torque the screws to 6 kg-cm (5.2 lbs-in).

Uninstalling an Application

To uninstall an application:


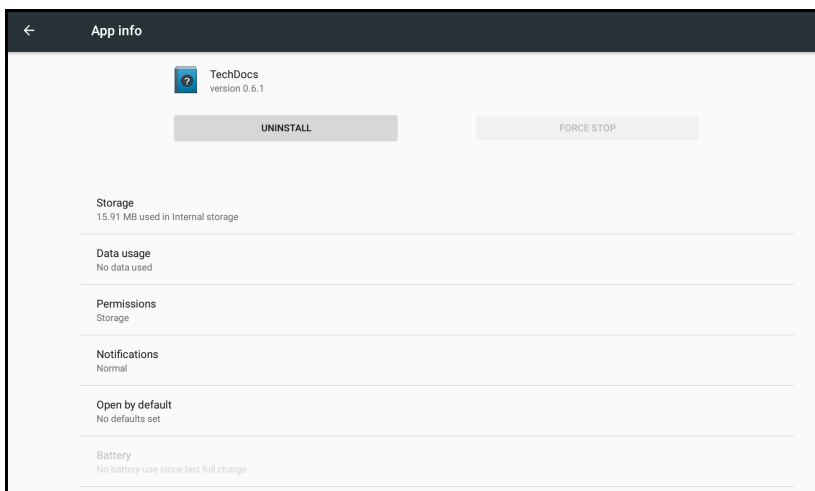
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Apps & notifications**.
3. Touch **See all apps** to view all apps in the list.
4. Scroll through the list to the app.
5. Touch the app. The **App info** screen appears.

Figure 136 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 either a USB drive or 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 USB Drive



WARNING: Do not remove the USB drive during system update. Damage to device can occur.

To update the system using a USB drive:



IMPORTANT: USB drive must have FAT32 format.

1. Install the USB drive into the host computer USB port.
2. Copy the System Update zip file to the root of a USB drive.
3. Properly eject the USB drive from host computer and remove the USB drive.
4. Remove the dust cover from the back of the device.
5. Insert the USB drive into the USB port.
6. Press and hold the Power button until the menu appears.
7. Touch **Restart**. The device resets.
8. Press and hold the **blue** button until the Zebra logo screen appears. The System Recovery screen appears.
9. Press the Up and Down buttons to navigate to **apply upgrade from USB drive**.
10. Press the Power button.
11. Use the Up and Down buttons to navigate to the System Update zip file.
12. Press the Power button. The System Update installs and then the device returns to the Recovery screen.
13. Press the Power button to reboot the device.


Using ADB

To update the system using ADB:

1. Using a T10 Torx screwdriver, remove four screws securing the top cover to the device.



IMPORTANT: When the user connects a USB cable to the USB port on top of the device, the USB and RS-232 ports on the bottom are disabled.

2. Connect the device to a host computer using a USB cable.
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
XXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX 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. Press the Up and Down buttons to navigate to **apply from adb**.
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.
16. Replace the top cover.
17. Secure the top cover to the device using the four screws. See [Figure 135 on page 203](#).
18. Torque the screws to 6kg-cm (5.2lbs-in).

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 USB drive or 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 a USB Drive

To perform an Enterprise Reset using USB drive:

1. Copy the Enterprise Reset zip file to the root of the USB drive.
 - Copy the zip file to a USB drive using a host computer and then installing the USB drive into the device.
 - Connect the device with a USB drive already installed to the host computer and copy zip file to the USB drive. Disconnect the device from the host computer.
2. Press and hold the Power button until the menu appears.
3. Touch **Restart**. The device resets.
4. Press and hold the **blue** button until the Zebra boot screen appears. The Android Recovery screen appears.
5. Press the Up and Down buttons to navigate to the **apply update from USB drive**.
6. Press the Power button.
7. Press the Up and Down buttons to navigate to the Enterprise Reset file.
8. Press the Power button. The Enterprise Reset occurs and then the device returns to the Recovery screen.
9. Press the Power button.

Using ADB


To perform an Enterprise Reset using ADB:

1. Using a T10 Torx screwdriver, remove four screws securing the top cover to the device. See [Figure 134 on page 202](#).



IMPORTANT: When the user connects a USB cable to the USB port on top of the device, the USB and RS-232 ports on the bottom are disabled.

2. Connect the device to a host computer using a micro USB cable.

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
XXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXX 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. Press the Up and Down buttons to navigate to **apply from adb**.
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 Enterprise Reset package installs and then the Recovery screen appears.
15. Press the Power button to reboot the device.
16. Replace the top cover.
17. Secure the top cover to the device using the four screws. See [Figure 135 on page 203](#).
18. Torque the screws to 6kg-cm (5.2lbs-in).

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 a USB Drive

1. Copy the Factory Reset zip file to the root of the USB drive.
 - Copy the zip file to a USB drive using a host computer and then installing the USB drive into the device.
 - Connect the device with a USB drive already installed to the host computer and copy the zip file to the USB drive. Disconnect the device from the host computer.
2. Press and hold the Power button until the menu appears.
3. Touch **Restart**. The device resets.
4. Press and hold the **blue** button until the Zebra boot screen. The System Recovery screen appears.
5. Press the Up and Down buttons to navigate to the **apply update from USB drive**.
6. Press the Power button.
7. Press the Up and Down buttons to navigate to the Android Reset file.
8. Press the Power button. The Factory Reset occurs and then the device returns to the Recovery screen.
9. Press the Power button.


Using ADB

To perform an Factory Reset using ADB:

1. Using a T10 Torx screwdriver, remove four screws securing the top cover to the device. See [Figure 134 on page 202](#).



IMPORTANT: When the user connects a USB cable to the USB port on top of the device, the USB and RS-232 ports on the bottom are disabled.

2. Connect USB cable to the device.
3. Connect the USB cable to the host computer.
4. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
5. Touch **System > Developer options**.
6. Slide the switch to the **ON** position.
7. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
8. Touch **OK**.
9. On the host computer, open a command prompt window and use the adb command:
adb reboot recovery
10. Press Enter. The System Recovery screen appears.
11. Press the Up and Down buttons to navigate to **apply from adb**.
12. Press the Power button.

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

adb devices.

The following displays:

List of devices attached

XXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

14. Type:

adb reboot recovery

15. Press Enter. The System Recovery screen appears.

16. Press the Up and Down buttons to navigate to **apply from adb**.

17. Press the Power button.

18. On the host computer command prompt window type:

adb sideload <file>

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

19. Press Enter. The Factory Reset package installs and then the Recovery screen appears.

20. Press the Power button to reboot the device. Replace the top cover.

21. Secure the top cover to the device using the four screws. See [Figure 135 on page 203](#).

22. Torque the screws to 6kg-cm (5.2lbs-in).


Storage

The device contains four types of file storage:

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

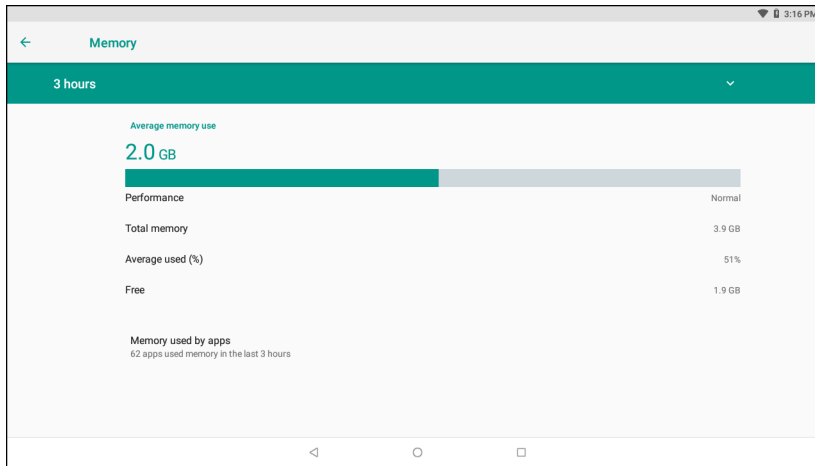
Random Access Memory

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

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

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

Figure 137 Memory Screen




The screen displays the amount of used and free RAM.

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

Internal Storage

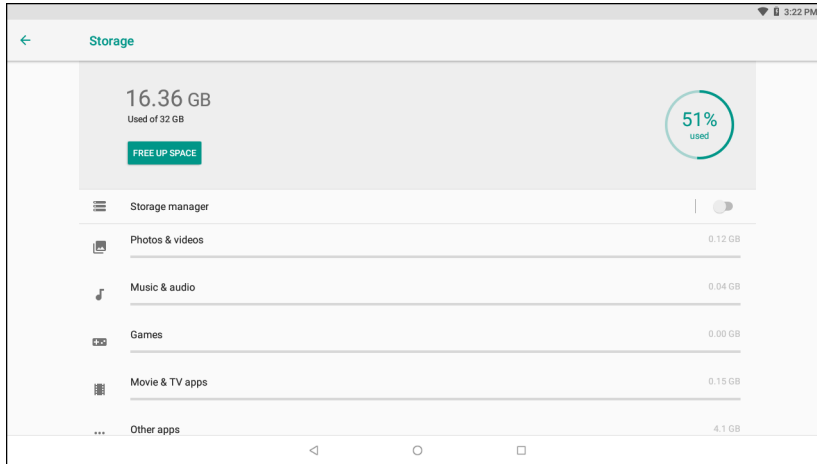
The device has internal storage. The internal storage content can be viewed and files copied to and from when the device is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

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

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

2. Touch **Storage**.

Figure 138 Storage Screen



The screen displays the total amount of space on internal storage and amount used as well as the amount of storage used by apps, photos, videos, audio and other files.

External Storage

The device can have a removable USB drive. The USB drive content can be viewed and files copied to and from when the device is connected to a host computer.

To view the used and available space on the USB drive:


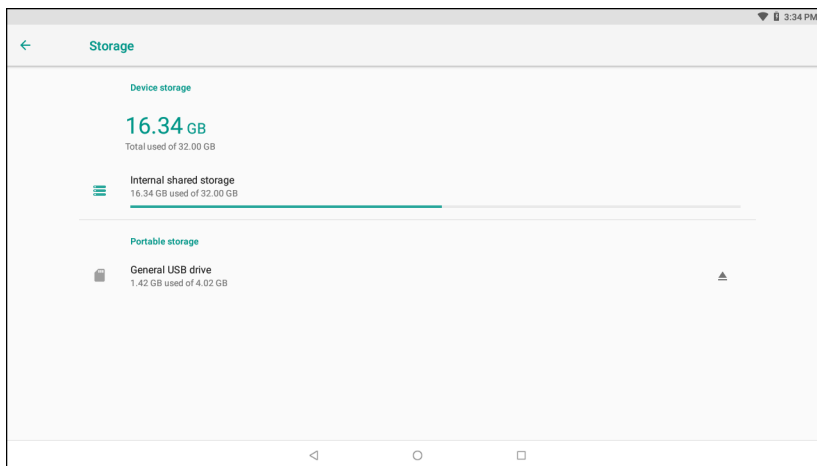
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Storage**.

Figure 139 External Storage Screen



Portable storage displays the total amount of space on the installed USB drive and the amount used.

To unmount the USB drive, touch .

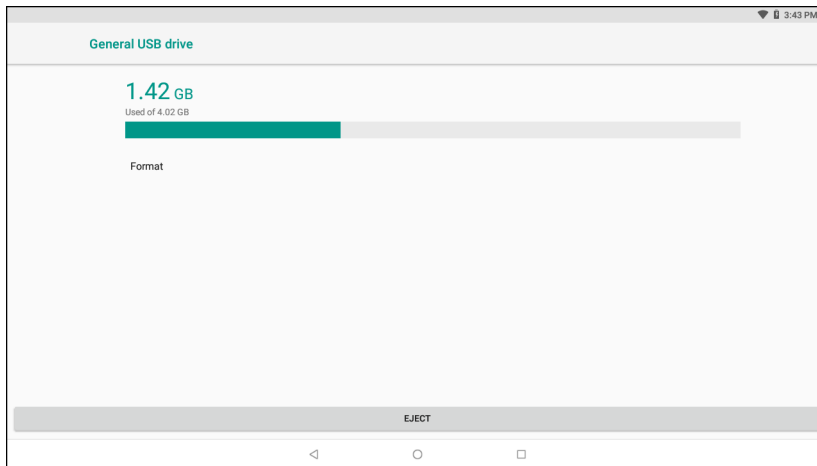
Touch **General USB Drive** to view the contents of the card.

Formatting a USB Drive

To format an installed USB drive as portable storage:

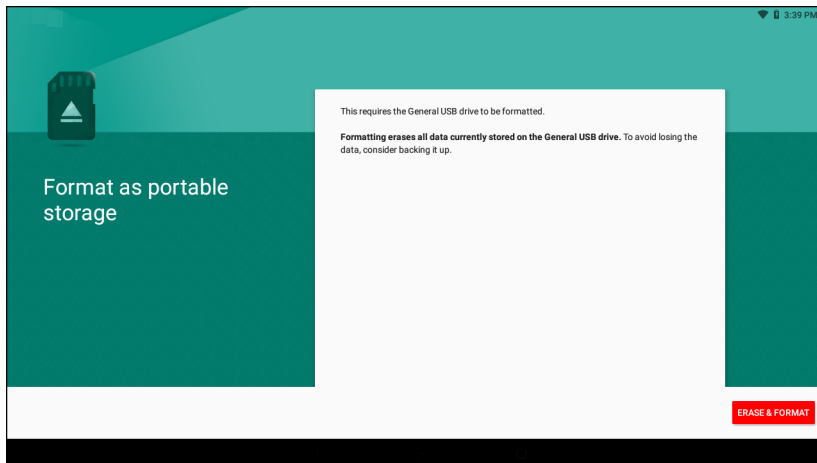
1. Touch **General USB Drive**.
2. Touch **⋮** > **Storage Settings**.

Figure 140 USB Drive Settings Screen



3. Touch **Format**.

Figure 141 Format Screen



4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.

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.


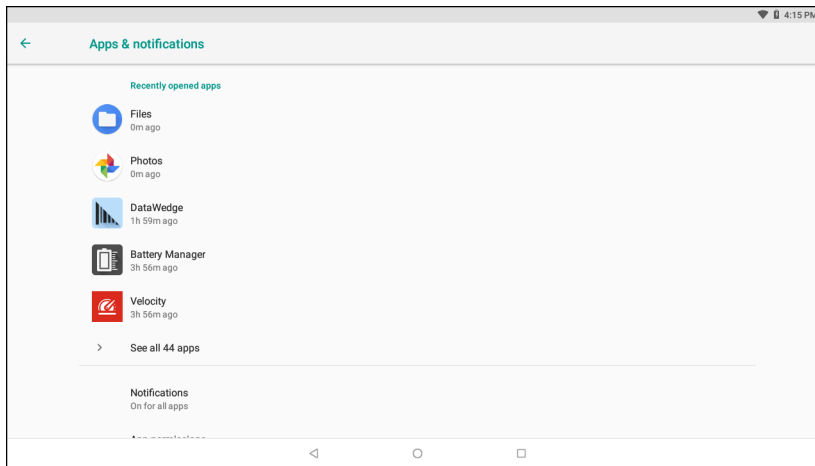
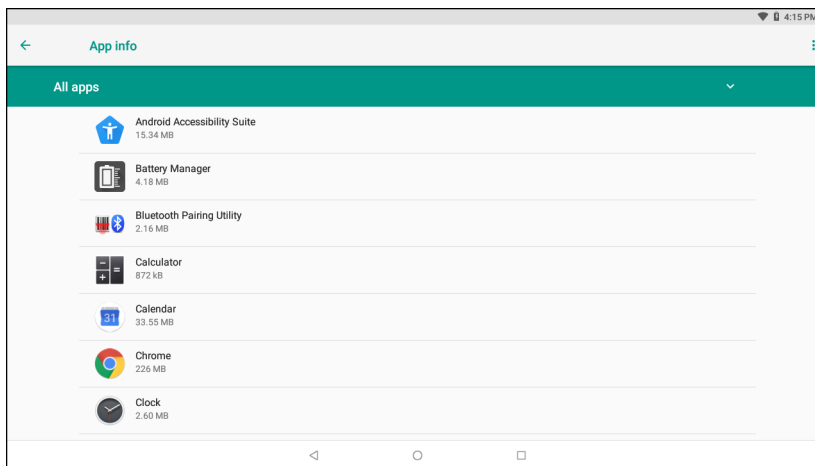
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Apps & notifications**.


Figure 142 Apps & Notifications Screen



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

Figure 143 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 USB drive or Internal storage in the Downloads directory. Use the Downloads app to view, open, or delete downloaded items.



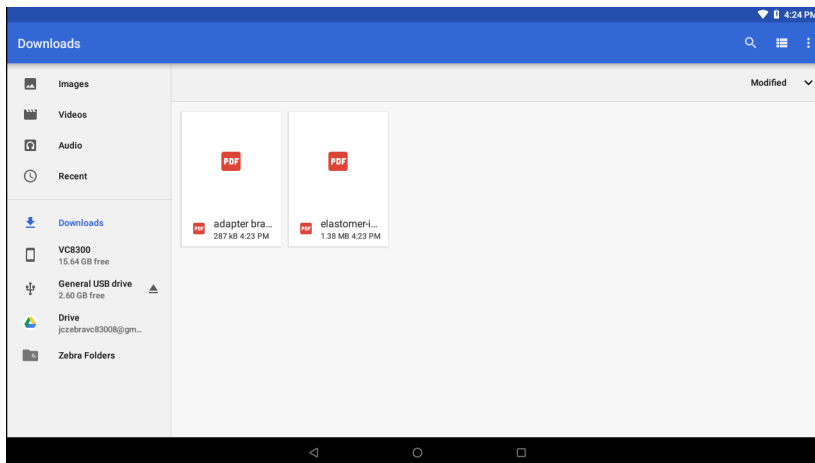

1. Swipe the screen up and touch .
2. Touch  > **Downloads**.

Figure 144 Files - Downloads Screen



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

Maintenance and Troubleshooting

Introduction

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



WARNING: Danger due to electric shock when cleaning and maintaining the device. To avoid electric shock, turn the device off and disconnect it from the power supply before cleaning or maintaining it.

Cleaning



CAUTION: Do not use compressed air, a high-pressure cleaner or vacuum cleaner, as this can damage the surface. Using a high-pressure cleaner poses the additional risk of water entering the device and damaging the electronics or display.

Housing Cleaning

Clean the fully assembled device vehicle mount computer housing using only a mild detergent on a lightly dampened soft cloth.

Touchscreen Cleaning

Use neutral detergent or isopropyl alcohol on a clean soft cloth to clean the panel surface. Do not use any kind of chemical solvent, acidic or alkali solution.

Touchscreen

The device is equipped with a capacitive touchscreen.



CAUTION: Keep the touchscreen clean (see Touchscreen Cleaning on page 215).

Do not apply adhesives to the surface.

Avoid high voltage and/or static charge.

Do not use ball point pens, writing utensils, tools, or sharp objects.

Touch the panel only with your finger to ensure normal operation.

Operate in a stable environment. Abrupt variation of temperature and humidity may cause malfunction.

Avoid applying excessive activation force or sudden impact on the touchscreen surface.

Operation of the capacitive touch screen is recommended with:

- Clean, dry fingers.
- Clean, dry, soft gloves.

Troubleshooting

Table 17 *Troubleshooting*

Symptom	Possible Cause	Solution
The vehicle computer does not power on or shuts off suddenly.	The power cable ignition sense wire (yellow) is not connected properly.	Verify that the power cable is connected properly. See Wiring Vehicle Power to the VC8300 on page 26 .
	Power cable not connected properly or unplugged.	Connect power cable to power cable portion underside of vehicle computer. Turn the main power switch on.
	If the vehicle computer is powered by a vehicle battery, the vehicle battery is depleted.	Replace or charge the vehicle battery.
Cannot see characters on display.	Vehicle computer not powered on (Power LED is Off).	Press the Power button on.
	Screen is too dark.	Adjust the brightness; see Figure 1 on page 19 .
	The vehicle computer is in suspend mode (Power LED is on).	Press the Power button to turn on the vehicle computer.
The touchscreen is not working.	Replacement screen protector was damaged.	Replace screen protector.
	Touch screen is damaged.	See system administrator.

Table 17 *Troubleshooting (Continued)*

Symptom	Possible Cause	Solution
The optional serial scanner does not operate.	Scanner is not properly connected to the vehicle computer.	Connect the scanner to the COM1 or COM2 port. Ensure the proper COM port is selected in the VC Settings application, see Connecting an RS-232 Scanner on page 96. If the problem continues, refer to the scanner Product Reference Guide.
	External power is not connected.	Verify external power connection.
	Power is not applied to COM port.	Enable power to COM ports. See VC Settings on page 88 .
	Serial COM port in not enabled in DataWedge.	Enable the serial COM port in the DataWedge profile. See Serial Port Input from Serial Port 1 on page 151 or Serial Port Input from Serial Port 2 on page 151 .
	USB cable is connected to USB port on top of device.	Disconnect USB cable from top of device.
The optional USB scanner does not operate.	USB cable is connected to USB port on top of device.	Disconnect USB cable from top of device.
	Scanner not configured for correct protocol (SSI or HID)	Configure scanner to correct protocol. See Data Capture on page 91 .
	USB connector not connected properly.	Remove USB cable and re-connect.
No sound is heard when you tap the touchscreen or press a key.	Volume is turned down.	Adjust the volume; see Figure 1 on page 19.
	Application currently running disabled the sound.	Configure the application to enable the sound.
	Faulty speaker.	Contact Zebra support at www.zebra.com/support .
	The optional M1000 speakerphone/mic is connected to the device.	Normal operation, sound is through speaker / mic.
Missing pixels on the display.	Faulty LCD.	Contact Zebra support. See www.zebra.com/support .
COM1 or COM2 port is not working.	Another application, or DataWedge is using the port.	Stop the application using the port or change the DataWedge COM Port Settings.
	USB cable connected to the USB port on top of the device.	Disconnect USB cable from USB port on top of the device.

Table 17 *Troubleshooting (Continued)*

Symptom	Possible Cause	Solution
No keys are working on the built-in keyboard.	The application does not require keyboard input.	Configure the application to use the keyboard.
	Vehicle computer is not responding.	Warm boot the vehicle computer.
The vehicle computer cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s).
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
When installed on some electric forklifts, the scanner range is shorter than it is when installed on other forklifts.	Electro-magnetic interference caused by the forklift.	Consult forklift vendor about reducing the interference by adding a capacitor between the forklift chassis and its battery's negative terminal, or another recommended solution.
Wi-Fi Signal strength degraded.	Incorrect antenna selection.	Check antenna selection. See VC Settings on page 88 .
	Damaged external antenna.	Either right or left external antenna broken or not connected properly.
	Using wrong antenna.	See accessory list for correct antenna for device.
Cannot find Bluetooth devices.	Incorrect antenna selection.	Check antenna selection. See VC Settings on page 88 .
	Damaged external antenna.	Right external antenna broken or not connected properly.
	Using wrong antenna.	See accessory list for correct antenna for device.

Specifications

Introduction

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

Technical Specifications

Table 18 *Technical Specifications*

Item	Description
Physical and Environmental Characteristics	
Dimensions	276 mm L x 238 mm W x 90 mm D 10.9 in. L x 9.4 in. W x 3.5 in. D
Weight	3.7 kg (8.2 lbs)
Display: Size: Resolution: Brightness:	8 in. color WXGA 1280 x 720 LCD with LED backlight; 24 bit color depth 1000 NITs
UPS Battery	Rechargeable UPS battery for operation during power loss
IP Sealing	IP 66
Interface Ports	Standard sealed and secured connectors: <ul style="list-style-type: none">• Two RS-232 serial port• One standard USB port• One powered USB port• One 3.5 mm audio jack
Thermal Shock	-30°C to 50°C (-22°F to 122°F)
User Environment	
Operating Temperature	-30°C to 50°C (-22°F to 122°F)
Storage Temperature	-40°C to 60°C (-40°F to 140°F)
Relative Humidity	5% to 95% non-condensing (standard version) 5% to 95% condensing (freezer version with internal heating)

Specifications

Table 18 *Technical Specifications (Continued)*

Item	Description
Salt Fog	48 hours of 5% solution at 35°C (95°F)
Solar Radiation	MIL STD 810-G, Method 505.5
ESD	±15kV air discharge ±8kV contact discharge ±8kV indirect discharge
Integrated Sensors	Motion (accelerometer); temperature; ignition
Shock/Vibration	IEC 60721-3-5M3; MIL-STD 810G; Method 514.6; MIL-STD 810G; Method 516.6
Power Consumption (12 - 48 VDC input Voltage)	
Off	<1 W
Suspend	4 - 7.5 W
Run Mode	10 - 13 W Display brightness at 50%, keyboard backlight off, Wi-Fi radio in receiving mode, and UPS battery fully charged.
	36 - 40 W Display brightness at 100%, keyboard backlight at 100%, Wi-Fi radio receiving and transmitting, UPS battery is charging, and scanner connected.
	61 - 65 W Display brightness at 100%, keyboard backlight at 100%, Wi-Fi radio receiving and transmitting, UPS battery is charging, scanner connected, and touch screen heater is on.
Performance Characteristics	
CPU/RAM	Qualcomm Snapdragon™ 660 octa-core 2.2 GHz
Operating System	Android™ 8.1.0 Oreo
Mass Storage	eMMC pSLC mode 32 GB
Additional Software	Zebra Mobility DNA, and Ivanti Velocity
Application Development	Zebra Enterprise Mobility Developer Kit (EMDK) for Android
Touchscreen	<ul style="list-style-type: none"> • Capacitive touchscreen with finger operation. • Freezer version includes integrated touchscreen heater for evaporates external condensation. • Construction: Gorilla Glass • Hardness of surface: 3H (ASTM D3363)

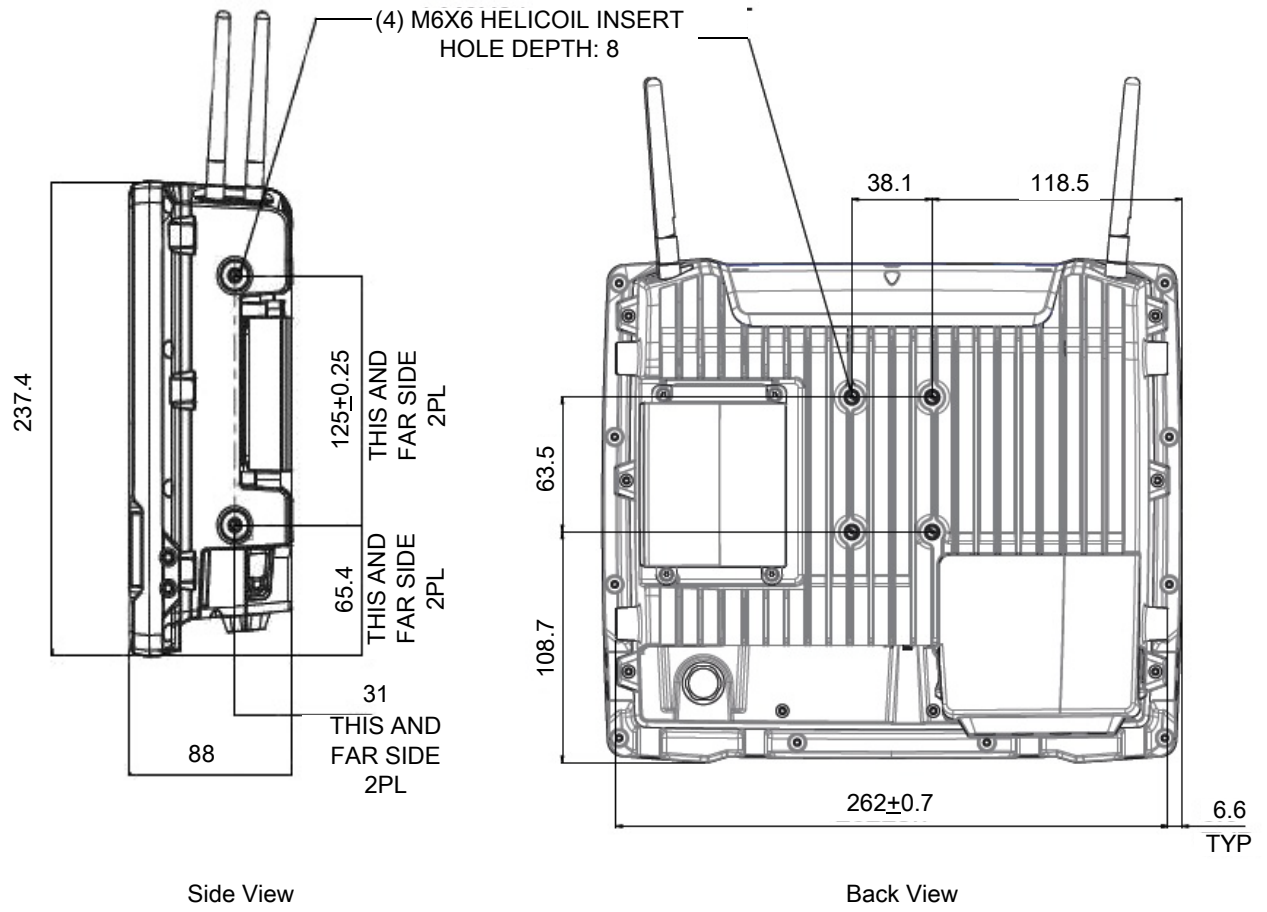
Specifications

Table 18 *Technical Specifications (Continued)*

Item	Description
Audio	High volume 87 dBA speaker (at 1 foot distance)
Push-to-Talk	External optional M1000 speaker/microphone
WLAN Wireless Data Communications	
WLAN radio	IEEE 802.11 a/b/g/n/ac/k/r 2x2 MU-MIMO
Output Power	2.4 GHz=+18.5 dBm max, 5 GHz=+18.5 dBm max
Data Rates	5 GHz: 802.11a/n/ac—up to 866.7 Mbps 2.4 GHz: 802.11b/g/n—up to 300 Mbps
Operating Channels	Channel 1-13 (2412-2472 MHz): 1,2,3,4,5,6,7,8,9,10,11,12,13 Channel 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 Channel Bandwidth: 20, 40, 80 MHz Actual operating channels/ frequencies and bandwidths depend on regulatory rules and certification agency.
WLAN Security	WEP (40 or 104 bit) WPA/WPA2 Personal (TKIP and AES) WPA/WPA2 Enterprise (TKIP and AES) - EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0-MSCHAPv2, PEAPv1-EAP-GTC and LEAP, EAP-PWD FIPS 140-2 Level 1: Data in Motion and Data at Rest2
Multimedia	Wi-Fi Multimedia (WMM and WMM-PS; Including TSPEC)
Certifications	WFA (802.11n, WMM-PS, 802.11ac, PMF, WMM-AC, Voice Enterprise, WiFi Direct and WPS 2.0)
Fast Roam	PMKID caching, Cisco CCKM, OKC, 802.11r
Antenna	Internal or external (software switchable)
WPAN Wireless Data Communications	
Bluetooth	Class 2, Bluetooth v5.0, Bluetooth Low Energy (BLE)
Power Supply	
Power Supply	Internal power supply 12-48V nominal

Drill Hole Dimensions

Figure 145 Drill Hole Dimensions



Index

A

adaptive frequency hopping	115
advanced data formatting rules	159
airplane mode	23
alarms only	186
apps	49
accessing	51
adding shortcuts	41
battery manager	56
datawedge demonstration	60
files	66
shortcuts	41
VC Settings	88
Velocity	90
automatically block sounds and vibrations	187

B

barcode input	137
enabled	137
battery	
low power notification	23
management	22
monitor usage	22
battery manager	56
Bluetooth	104
bluetooth	115
change name	118
disabling	118
discovering devices	118
enabling	117
PIN	116
power states	117
profiles	116
security	116

C

cable dust cover	27
cables, installing in vehicle	25
change bluetooth name	118
cleaning	
housing	215
connect to WLAN	104
contacts	59
adding	59
deleting	59
editing	59
CPU	220

- D**
- data capture 91
 - data capture plus 135
 - datawedge 102
 - advanced data formatting rules 159
 - associating applications 133
 - auto import 170
 - auto switch to default on event 137
 - barcode input 137
 - configuration and profile file management 169
 - configuring ADF plug-in 160
 - creating a new profile 132
 - data capture plus 135
 - decoders 138
 - disabling 132, 171
 - enterprise folder 170
 - exporting a configuration file 168
 - importing a configuration file 168
 - input plugins 130
 - intent output 154
 - intent overview 155
 - IP output 156
 - keystroke output 153
 - multibarcodes params 151
 - options menu 132
 - output plug-ins 130
 - plug-ins 130
 - process plug-ins 130
 - profile configuration 133
 - profile context menu 131
 - profile0 129
 - profiles 129
 - profiles screen 131
 - programming notes 170
 - reader params 147
 - reporting 169
 - scan params 150
 - scanner selection 137
 - settings 167
 - UDI params 151
 - UPC EAN params 145
 - voice input 152
 - datawedge demonstration 60
 - decoder params
 - Codabar 140
 - Code 11 140
 - Code 128 140
 - Code 39 141
 - Code 93 142
 - Composite AB 142
 - decode lengths 145
 - Discrete 2 of 5 142
 - GS1 DataBar Limited 142
 - HAN XIN 142
 - Interleaved 2 of 5 142
 - Matrix 2 of 5 143
 - MSI 143
 - UK Postal 144
 - UPCA 144
 - UPCE0 144
 - UPCE1 144
 - US Planet 145
 - decoders 138
 - diagnostic tool
 - battery test information 69
 - dimensions 219
 - disable bluetooth 118
 - discover bluetooth devices 118
 - display 219
 - display settings 182
 - do not disturb feature 186
- E**
- EAP 104
 - electrical installation 24
 - emergency shutdown 18
 - enable bluetooth 117
 - external antenna 26
- F**
- files 66
 - folders
 - creating 42
 - naming 42
 - removing 42
 - font size 183
 - Forklift 29
 - forklift battery replacement 29
 - forklift installation 24, 25
 - front keys 21
- G**
- general sound setting 184
 - google
 - mobile services 34
 - ground bolt 25
- H**
- hard reset 54
 - Heater Control
 - battery port heater 72
 - serial port heater 71
 - temperatures 71
 - USB port heater 72
 - Heater Status 22
 - home screen 34
 - moving items 41
 - home screen wallpaper 42

- I**
- imager scanning 91
 - installation
 - non-vehicle 31
 - vehicle 31
- K**
- keyboard 120
 - keyboards
 - additional character tab 47
 - alpha tab 47
 - numeric tab 47
- L**
- LAN 22
 - LED indicators 21
 - lock screen notifications 39
 - low battery notification 23
- M**
- managing notifications 38
 - message URL http
 - //www.zebra.com/support 74
 - monitor battery usage 22
 - mounting
 - assembly steps 27
 - instructions 24
 - MT43XX RAM Mount kit 124
 - multibarcodes params 151
- N**
- notification icons 37
 - notifications
 - lock screen 39
 - managing 38
- O**
- operating
 - emergency 18
 - operating system 220
 - optional mount kits 124
- P**
- picklist 92
 - power
 - power down device 22
 - power up device 22
 - supply 18
 - protection 18
 - safety 18
 - PTT Express 74
- Q**
- quick access panel 39
 - quick settings
 - edit icons 40
- R**
- RAM Mount kit 124
 - reader params 147
 - resetting the device 54
 - RS507/RS507x scanning 94, 95
 - RS6000 scanning 93
 - RxLogger 78
- S**
- scan params 150
 - scanning 91
 - screen blanking 89
 - screen font size 183
 - screen rotation 183
 - security 104
 - settings
 - automatically block sounds and vibrations 187
 - datawedge 167
 - display 182
 - do not disturb 186
 - general sound 184
 - home screen wallpaper 42
 - limit sounds and vibrations 186
 - soft reset 54
 - software version 15
 - software versions 14
 - specifications 15, 219
 - status bar 35
 - strain relief rail 28
- T**
- technical specifications 219
 - touchscreen 215
 - cleaning 215
 - operation 215
 - specifications 215
 - transferring files using USB 54
 - troubleshooting 216
- U**
- UDI params 151
 - unpacking 17
 - UPC EAN params 145
 - USB 54

V

VC Settings	88
built-in speaker	89
display	88
ignition detection	89
peripheral power	88
screen blanking	89
WIFI antenna switching	89
VC8300	
features	19
vehicle	
battery, charging	18
vehicle-mount installation	
cables	25
Velocity	90
voice input	152

W

weight	219
WEP	104
widgets	41
wi-fi	
advanced features	114
Wi-Fi direct	112
wi-fi network	104
wireless local area network	104
WLAN	22, 104
WPA	104
WPS pin entry	113
WPS push button	113

