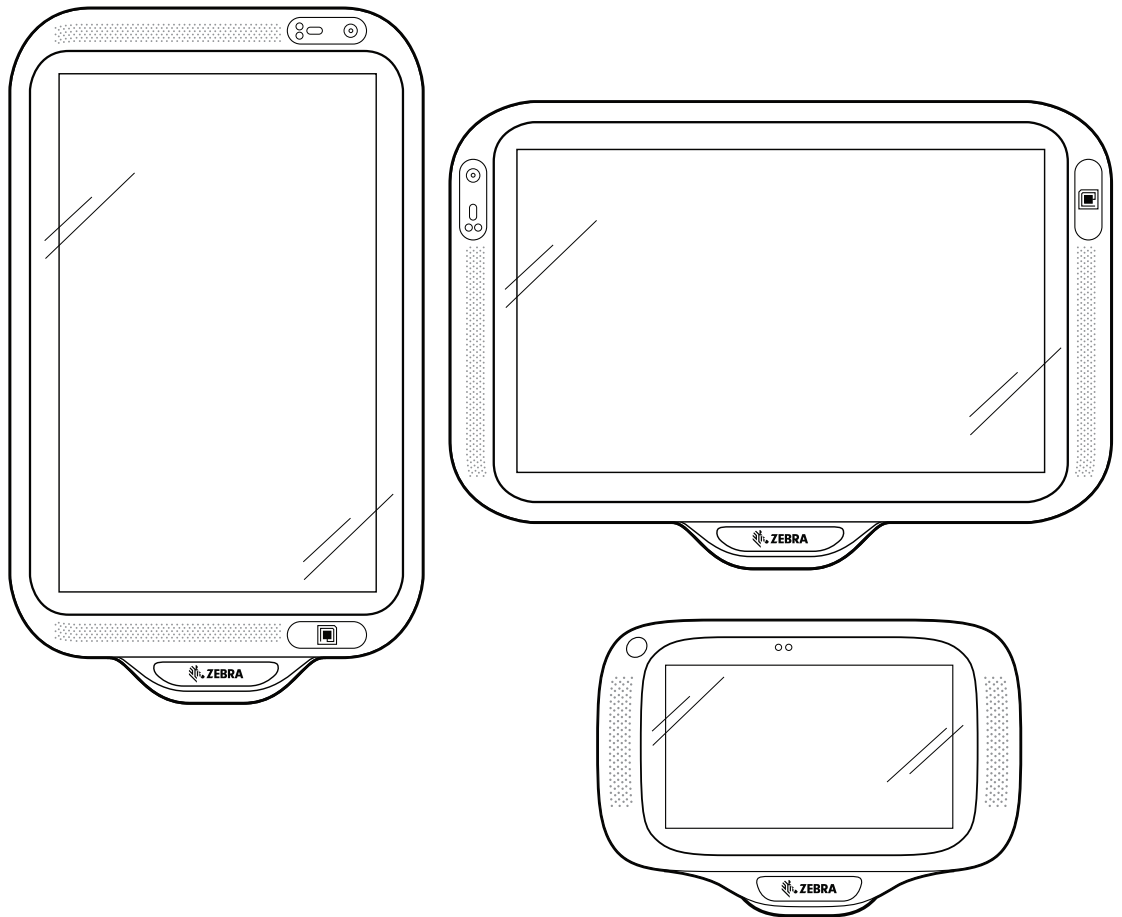


CC600/CC6000

Customer Concierge



Integrator Guide
for Android™ 8.1.0 Oreo



ZEBRA

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

©2019 Zebra Technologies Corporation and/or its affiliates. All rights reserved. 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	5/2019	Initial Release

Table of Contents

Copyright	2
Terms of Use	2
Revision History	2
About This Guide	10
Introduction	10
Documentation Set	10
Configurations	11
Accessories	11
Software Versions	12
Chapter Descriptions	13
Notational Conventions	14
Service Information	14
Provide Documentation Feedback	14
Getting Started	15
Introduction	15
Unpacking	15
Features	16
Setup	20
Inserting the microSD Card (Optional)	21
Mounting the Device	21
Google Account Setup	28
Zebra Visibility Services	28
Resetting the Device	28
Settings	30
Introduction	30
WLAN Configuration	30

Table of Contents

Configuring a Secure Wi-Fi Network	30
Manually Adding a Wi-Fi Network	32
Configuring for a Proxy Server	33
Configuring the Device to Use a Static IP Address	35
Wi-Fi Preferences	36
Additional Wi-Fi Settings	37
Wi-Fi Direct	39
Setting Screen Lock	39
Setting Screen Lock Using PIN	40
Setting Screen Unlock Using Password	41
Setting Screen Unlock Using Pattern	42
Showing Passwords	42
Accounts	43
Language Usage	43
Changing the Language Setting	43
Adding Words to the Dictionary	43
Keyboard Settings	43
PTT Express Configuration	44
RxLogger	44
RxLogger Configuration	44
RxLogger Settings	45
ANR Module	45
Kernal Module	45
Logcat Module	46
LTS Module	47
Ramoops Module	47
Resource Module	48
Snapshot Module	48
TCPDump Module	49
Tombstone Module	49
Configuration File	49
Enabling Logging	49
Disabling Logging	49
Extracting Log Files	49
RxLogger Utility	50
App View	50
Viewing Logs	50
Backup	52
Archive Data	52
Overlay View	52
Initiating the Main Chat Head	52
Removing the Main Chat Head	53
Viewing Logs	53

Table of Contents

Removing a Sub Chat Head Icon	54
Backing Up In Overlay View	54
About Phone	54
USB/Ethernet Communication.....	56
Introduction	56
Transferring Files with a Host Computer via USB	56
Transferring Files	56
Transferring Photos	57
Disconnect from the Host Computer	57
USB/Ethernet Communication	58
Ethernet Settings	58
Configuring Ethernet Proxy Settings	58
Configuring Ethernet Static IP Address	59
Establishing Ethernet Connection	60
DataWedge	61
Introduction	61
Basic Scanning	61
Barcode Capture with an Imager	61
Profiles	62
Profile0	62
Plug-ins	63
Input Plug-ins	63
Process Plug-ins	63
Output Plug-ins	63
Profiles Screen	64
Profile Context Menu	64
Options Menu	65
Disabling DataWedge	65
Creating a New Profile	65
Profile Configuration	66
Associating Applications	66
Data Capture Plus	68
Barcode Input	70
Enabled	70
Scanner Selection	70
Auto Switch to Default on Event	70
Configure Scanner Settings	71
Decoders	71
Decoder Params	74

Table of Contents

Codabar	74
UPC EAN Params	79
Reader Params	81
Scan Params	84
UDI Params	85
Keep enabled on suspend	85
Voice Input	85
Keystroke Output	86
Intent Output	87
Intent Overview	88
IP Output	89
Usage	90
Using IP Output with IPWedge	91
Using IP Output without IPWedge	92
Generating Advanced Data Formatting Rules	93
Configuring ADF Plug-in	93
Creating a Rule	94
Defining a Rule	95
Defining Criteria	95
Defining an Action	97
Deleting a Rule	97
Order Rules List	97
Deleting an Action	98
ADF Example	98
DataWedge Settings	102
Importing a Configuration File	102
Exporting a Configuration File	103
Importing a Profile File	103
Exporting a Profile	103
Restoring DataWedge	103
Configuration and Profile File Management	104
Enterprise Folder	104
Auto Import	104
Programming Notes	105
Capture Data and Taking a Photo in the Same Application	105
Disable DataWedge on Device and Mass Deploy	105
DataWedge APIs	105
Reporting	105
Soft Scan Trigger	106
Function Prototype	106
Scanner Input Plugin	106
Function Prototype	106
Parameters	106
Return Values	106

Table of Contents

Example	107
Comments	107
Enumerate Scanners	107
Function Prototype	108
Parameters	108
Return Values	108
Example	109
Comments	109
Set Default Profile	110
Default Profile Recap	110
Usage Scenario	110
Function Prototype	110
Parameters	110
Return Values	110
Example	111
Comments	111
Reset Default Profile	111
Function Prototype	112
Parameters	112
Return Values	112
Example	112
Comments	112
Switch To Profile	113
Profiles Recap	113
Usage Scenario	113
Function Prototype	113
Parameters	113
Return Values	114
Example	114
Comments	114
Notes	115
Imager as Camera	115
Application Deployment.....	117
Introduction	117
Security	117
Secure Certificates	117
Installing a Secure Certificate	117
Configuring Credential Storage Settings	118
Development Tools	118
Android	118
EMDK for Android	119
StageNow	120
ADB USB Setup	120

Enabling USB Debugging	120
Application Installation	121
Installing Applications Using the USB Connection	121
Installing Applications Using the Android Debug Bridge	122
Installing Applications Using a microSD Card	123
Uninstalling an Application	124
Performing a System Update	125
Downloading the System Update Package	125
Using microSD Card	125
Using ADB	126
Verify System Update Installation	127
Performing an Enterprise Reset	127
Downloading the Enterprise Reset Package	127
Using microSD Card	127
Using ADB	128
Performing a Factory Reset	128
Downloading the Factory Reset Package	128
Using microSD Card	129
Using ADB	129
Storage	130
Random Access Memory	130
Internal Storage	131
External Storage	132
Formatting a microSD Card	133
Formatting as Internal Memory	134
Enterprise Folder	135
App Management	135
Viewing App Details	136
Managing Downloads	137
Maintenance and Troubleshooting	138
Introduction	138
Maintaining the Device	138
Cleaning Instructions	138
Approved Cleanser Active Ingredients	138
Harmful Ingredients	139
Device Cleaning Instructions	139
Special Cleaning Notes	139
Cleaning Materials Required	139
Cleaning Frequency	139
Cleaning the Device	140

Table of Contents

Housing	140
Display	140
Camera and Exit Window	140
Troubleshooting	141
Technical Specifications	143
Introduction	143
Technical Specifications	143
CC6000	143
CC600	145
Decode Distances	147
CC6000 - SE4710 Scan Engine	147
CC600 - SE2100 Scan Engine	148

About This Guide

Introduction

This guide provides information about using the CC600 and CC6000 Customer Concierge and accessories.



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

Documentation Set

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

- CC600 Customer Concierge Quick Start Guide for Android Version 8.1, p/n MN-003314-xx, - describes how to get the device up and running.
- CC6000 Customer Concierge Quick Start Guide for Android Version 8.1, p/n MN-003315-xx, - describes how to get the device up and running.
- CC600/CC6000 Customer Concierge User Guide for Android Version 8.1, p/n MN-003313-xx, - describes how to use the device.
- CC600/CC6000 Customer Concierge Integrator Guide for Android Version 8.1, p/n MN-003411-xx, - describes how to set up the device and accessories.

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

Configurations

This guide covers the configurations listed in [Table 1](#) and [Table 2](#).

Table 1 *CC600 Device Configurations*

Configuration	Description	Front Camera	Scan Engine
CC600-5-3200LNWW	5 inch, OS: Android™ 8.1.0 Oreo, 32GB, Ethernet/Wi-Fi, Imager, Worldwide Configuration	No	SE2100
CC600-5-3200LNNA	5 inch, OS: Android™ 8.1.0 Oreo, 32GB, Ethernet/Wi-Fi, Imager, North America Configuration	No	SE2100
CC600-5-3200LNEU	5 inch, OS: Android™ 8.1.0 Oreo, 32GB, Ethernet/Wi-Fi, Imager, Europe Configuration	No	SE2100
CC600-5-3200LNIN	5 inch, OS: Android™ 8.1.0 Oreo, 32GB, Ethernet/Wi-Fi, Imager, India Configuration	No	SE2100

Table 2 *CC6000 Device Configurations*

Configuration	Description	Front Camera	Scan Engine
CC6000-10-3200LCWW	10 inch, OS: Android™ 8.1.0 Oreo, 32GB, Landscape, Imager, Worldwide Configuration	No	SE4710
CC6000-10-3200PCWW	10 inch, OS: Android™ 8.1.0 Oreo, 32GB, Portrait, Imager, Worldwide Configuration	Yes	SE4710
CC6000-10-3200LCNA	10 inch, OS: Android™ 8.1.0 Oreo, 32GB, Portrait, Imager, North America Configuration	Yes	SE4710
CC6000-10-3200PCNA	10 inch, OS: Android™ 8.1.0 Oreo, 32GB, Portrait, Imager, North America Configuration	Yes	SE4710
CC6000-10-3200LNNA	10 inch, OS: Android™ 8.1.0 Oreo, 32GB, Landscape, Imager, North America Configuration	No	SE4710

Accessories

Table 3 *Accessories*


Accessory	Part Number	Description
Mounting Plates		
CC600 Wall Mount	21-118517-01R	CC600 Wall Mounting Kit
CC600 Pole Mount	21-118517-02R	CC600 Pole Mounting Kit

Table 3 *Accessories*

Accessory	Part Number	Description
CC6000 Wall Mounting Kit	KT-152097-03	CC6000 Wall Mounting Kit with Power Supply Storage
CC6000 Wall Mounting Kit	KT-152097-01	100mm VESA
CC6000 Wall Mounting Kit	KT-152098-03	Slimmer, CC6000 specific mount
CC6000 Pole Mounting Kit	KT-152096-03	100mm VESA Includes additional storage shelf to hold power supply Modified over KT0152096-02 to better hold Level VI power supply.
CC6000 Pole Mounting Kit	KT-152096-01	100mm VESA
Charge and Communication Cables		
USB-C Cable	CBL-TC2X-USBC-01	Used to communicate with CC6000 via the USB OTG port.
USB-C Cable	CBL-TC5X-USBC2A-01	Used to communicate with CC6000 via the USB OTG port.
Power Supplies		
DC Line Cord	CBL-DC-383A1-01	Used with Power Supply (PWR-BUA5V16W0WW) Cable length is 6 ft
Power Supply	PWR-BUA5V16W0WW	100-240VAC, 5.4V, 3A, 16W Meets US DOE Level VI efficiency standard Replaces PWRS-14000-249R
AC Line Cord	50-16000-182R	Used with 50-14000-147R/50-14000-249R?PWRS-14000-249R/PWR-BUA5V16W0WW

Software Versions

To determine the current software versions:

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

4. The following information displays:
 - Status
 - SW Components
 - Legal Information
 - Model
 - Android version
 - Android security patch level
 - Kernel version
 - Build Fingerprint
 - Build number

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

Chapter Descriptions

Topics covered in this guide are as follows:

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

Notational Conventions

The following conventions are used in this document:

- “Device” refers to all configurations of the CC600 Customer Concierge and CC6000 Customer Concierge.
- **Bold** text is used to highlight the following:
 - Dialog box, window and screen names
 - Drop-down list and list box names
 - Check box and radio button names
 - Icons on a screen
 - Key names on a keypad
 - Button names on a screen.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Service Information

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

When contacting support, please have the following information available:

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

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

If the problem cannot be solved by Customer Support, the user may need to return the equipment for servicing and will be given specific directions. We are not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty. Remove the SIM card and/or microSD card from the device before shipping for service.

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

Provide Documentation Feedback

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

Getting Started

Introduction

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

Unpacking

1. Carefully remove all protective material from the device and save the shipping container for later storage and shipping.
2. Verify that the following are included:
 - CC600 or CC6000 interactive kiosk.
 - Regulatory Guide.
 - CC600 only: Ferrite bead for EMI. Attaches to the DC power module.
3. Inspect the equipment for damage. If any equipment is missing or damaged, contact the Global Customer Support center immediately.
4. Prior to using the device for the first time, remove the protective shipping film that covers the display.

Features



NOTE: Although the orientations differ, the features on the CC6000 landscape and portrait devices are the same.

Figure 1 CC6000 Front View

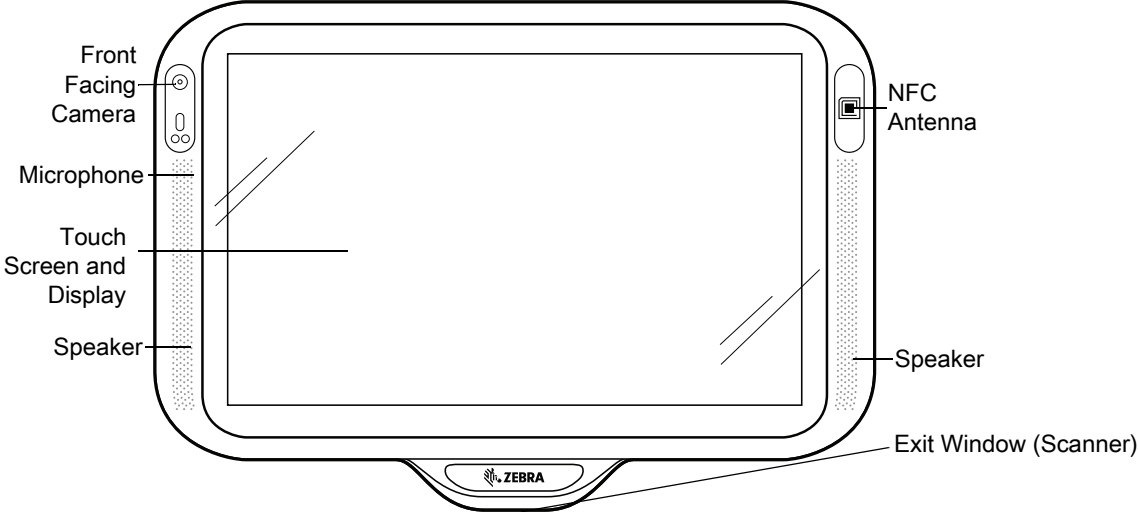


Figure 2 CC6000 Back View

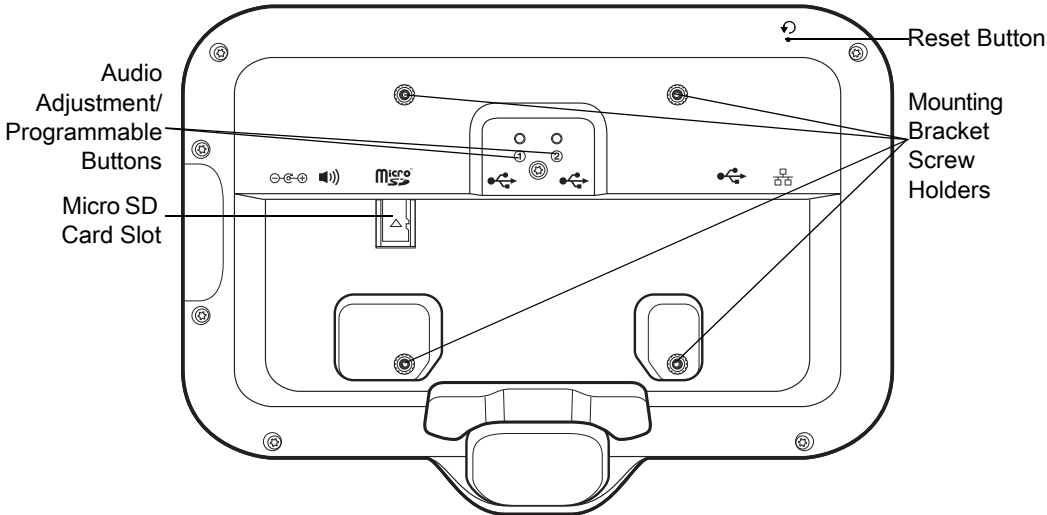


Figure 3 CC6000 Power and Cable Ports

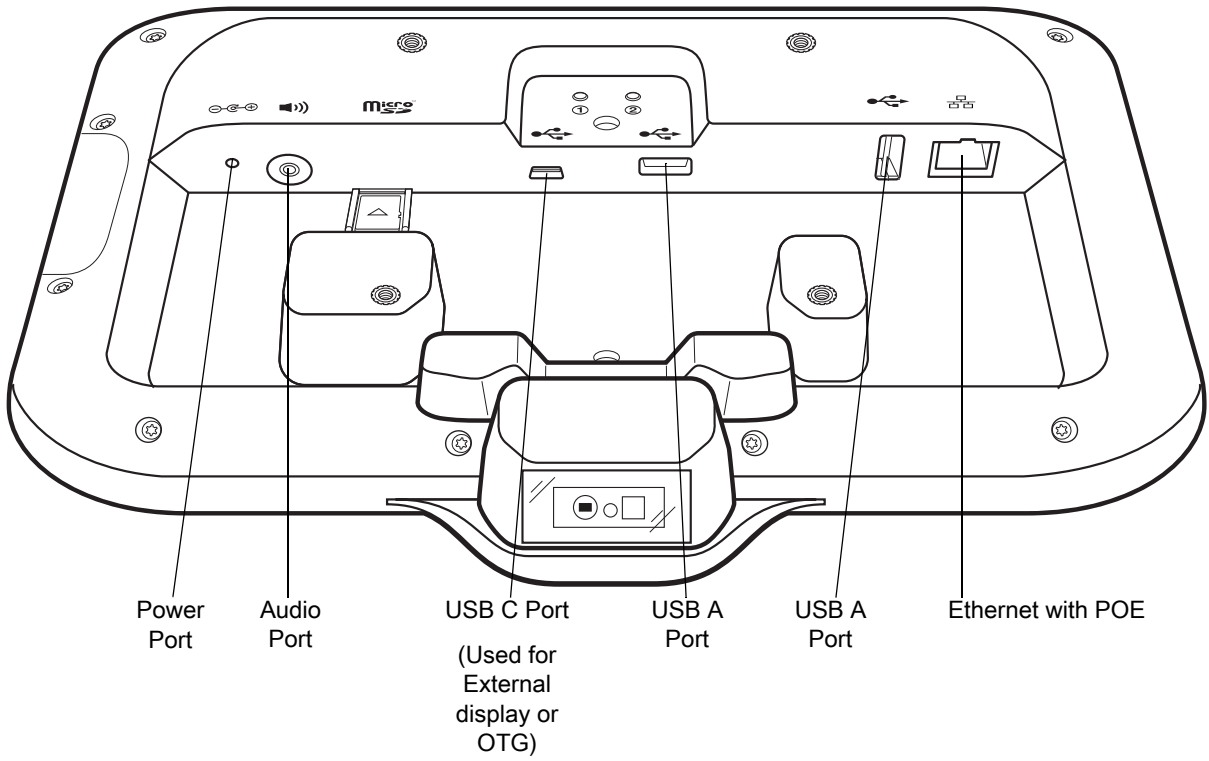


Figure 4 CC6000 Back With Bracket View

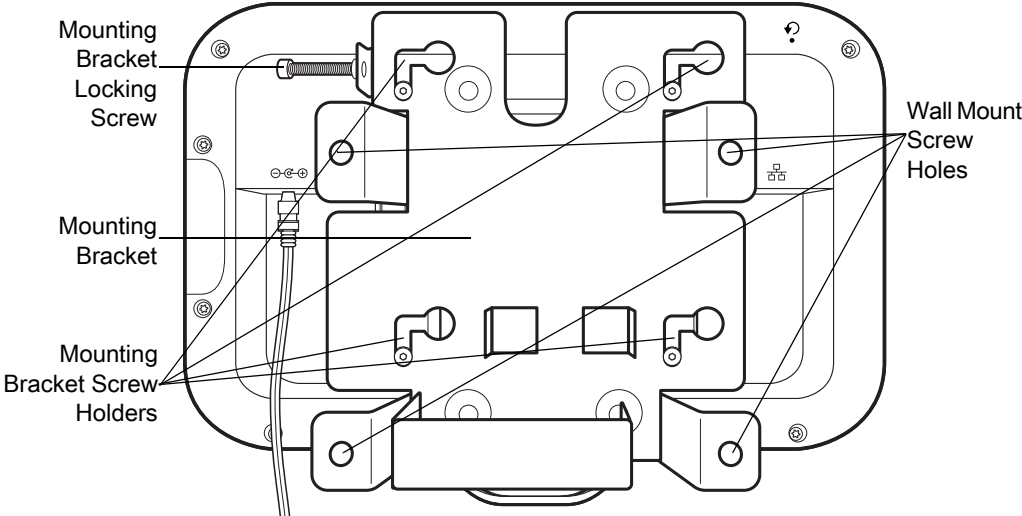


Figure 5 CC600 Front Views

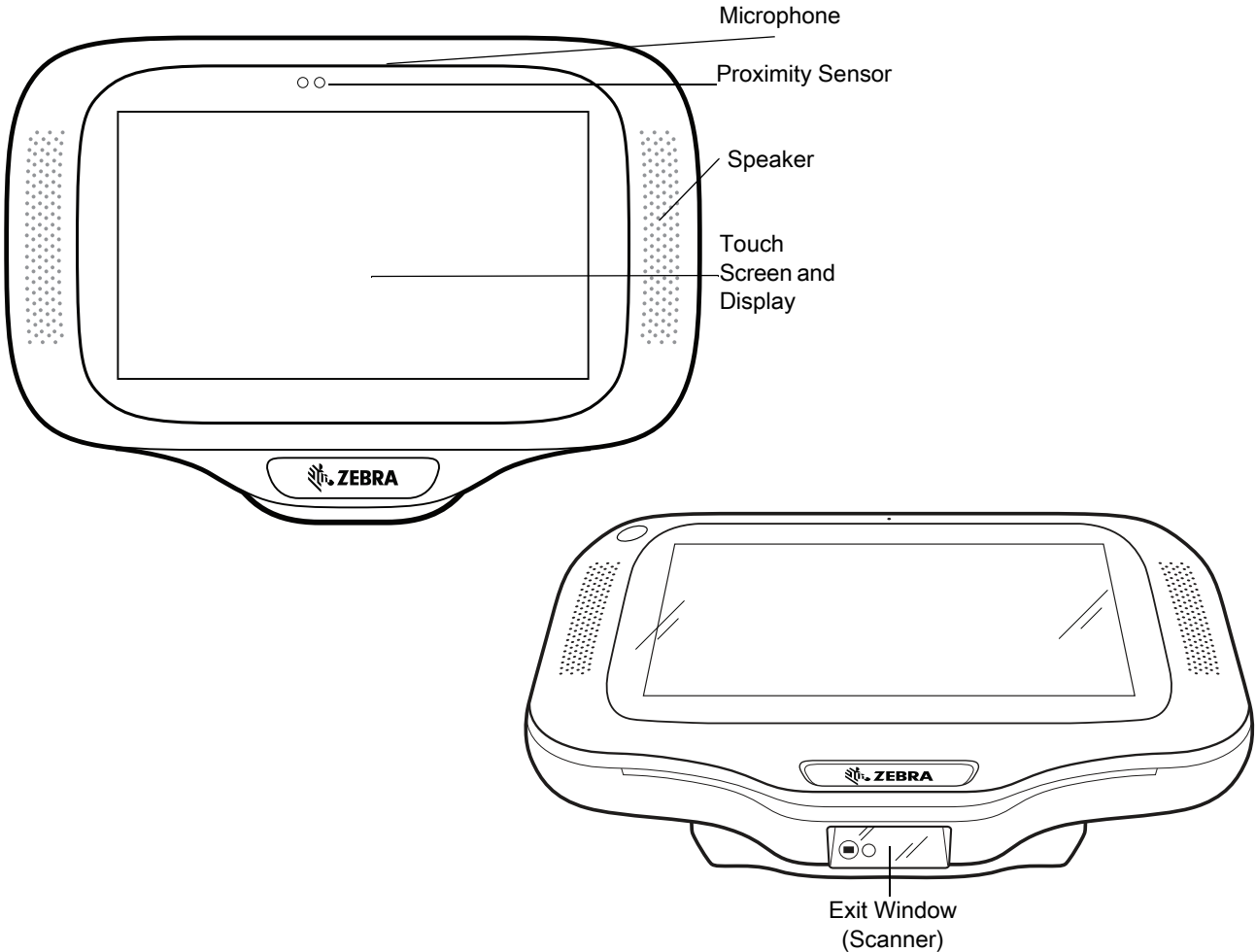


Figure 6 CC600 Back View

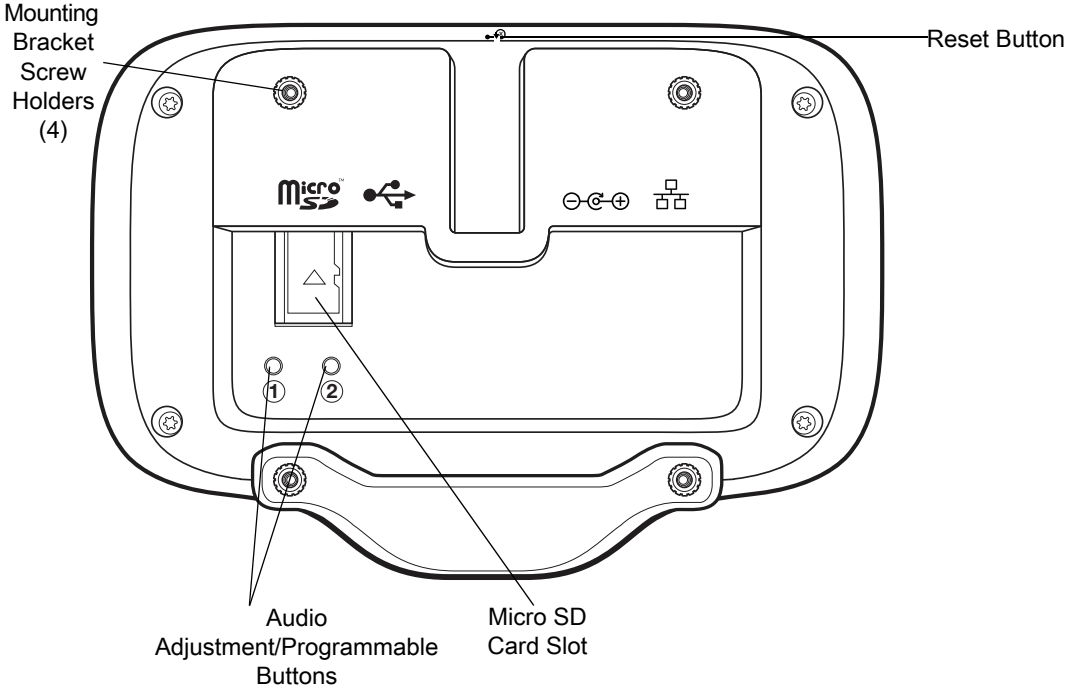


Figure 7 CC600 Power and Cable Ports

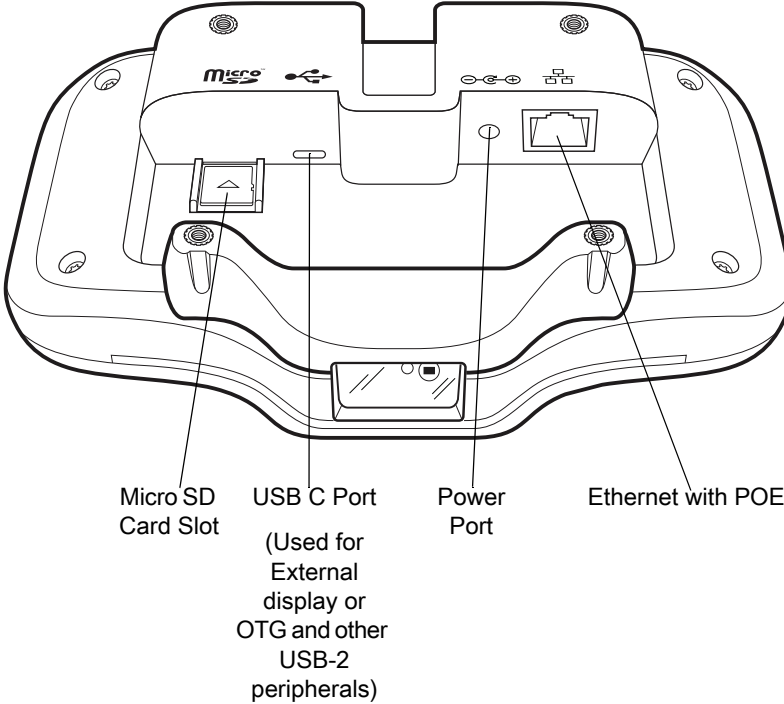


Figure 8 CC600 Back With Bracket View

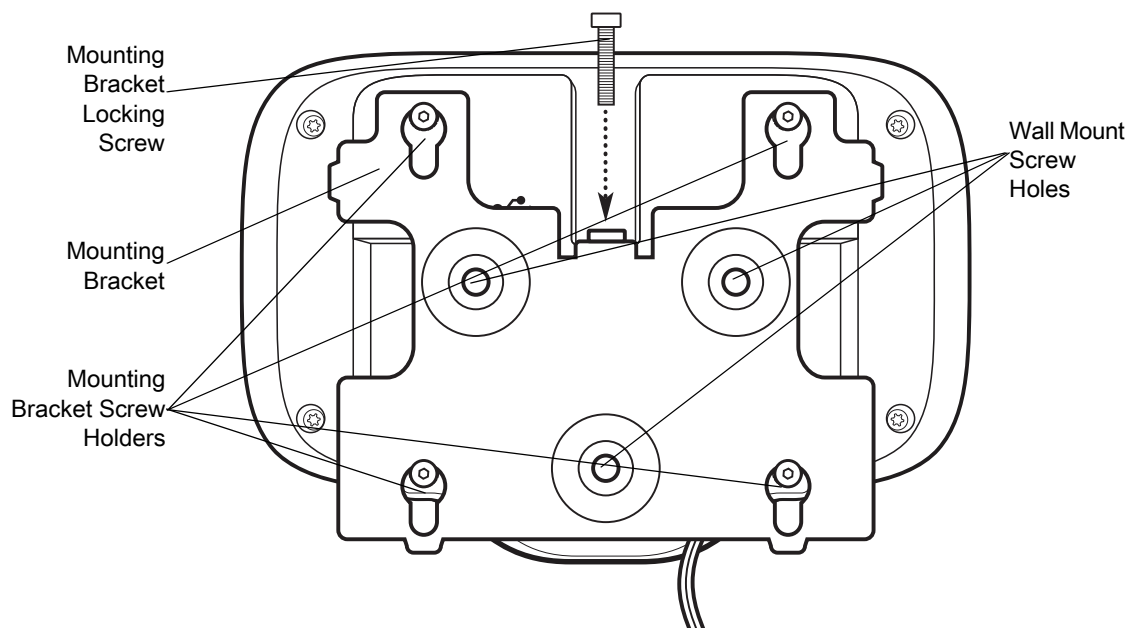


Table 4 Feature Descriptions

Item	Function
Touch Screen and Display	Displays all information needed to operate the device.
Exit Window (Scanner)	Provides data capture using the imager and reads a barcode. Note: To read a barcode, a scan-enabled app is required on the device.
Speaker	Provides audio output for video and music playback. Provides audio in speaker-phone mode.
NFC Antenna	Reads NFC tags. (CC6000 Only)
Proximity Sensor	Identifies the proximity of a user for turning up the display.
Microphone	Use for communications in Speakerphone mode.
Front Facing Camera	Captures still photos and videos. Note: Select CC6000 devices only.
Interface Connectors	See Figure 3 and Figure 7 .
Volume Up/Down Button	Increase and decrease audio volume (programmable).
External Display	Designated for USB-C port utilization.

Setup

Perform this procedure to start using the device for the first time.

- Install a micro secure digital (SD) card (optional).
- Connect the power supply to power on the device.
- Configure the device.

- Mount the device with the mounting bracket.
- Setup a Google account.

Inserting the microSD Card (Optional)

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

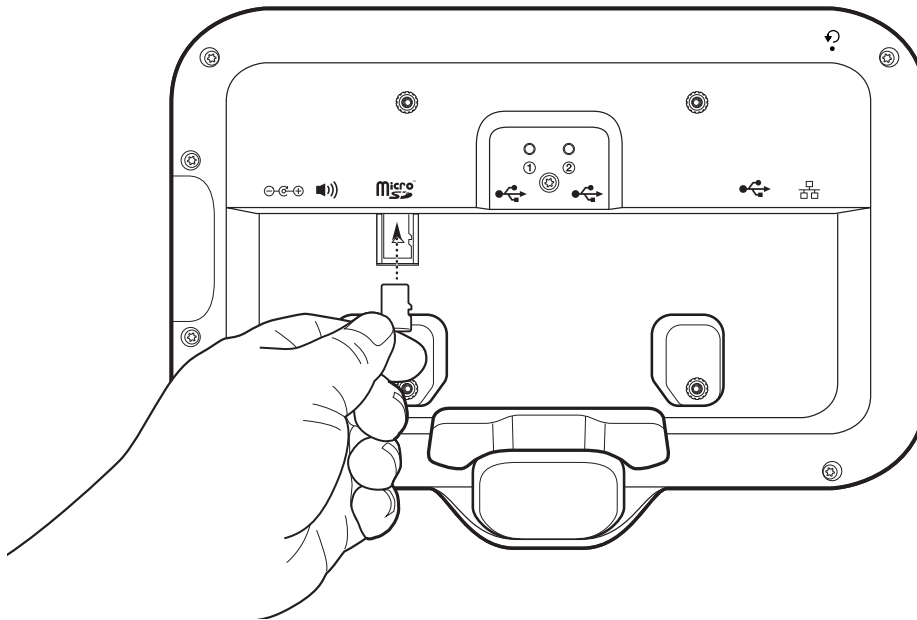


CAUTION: Follow proper electrostatic discharge (ESD) precautions to avoid damaging the microSD card. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

To install the microSD card:

1. Remove the device from the mounting bracket, if installed.
2. Slide the microSD card, connectors down, into the device as shown in [Figure 9](#).

Figure 9 Inserting microSD Card



Mounting the Device

Each configuration of the device requires the appropriate mounting bracket to mount the device to a wall or other flat surface. The diameter of the holes for the wall screws is 5.8mm (0.228 in).



NOTE: Device measurements in [Figure 10](#), [Figure 11](#) and [Figure 12](#) are in millimeters.

Figure 10 CC600 Measurements

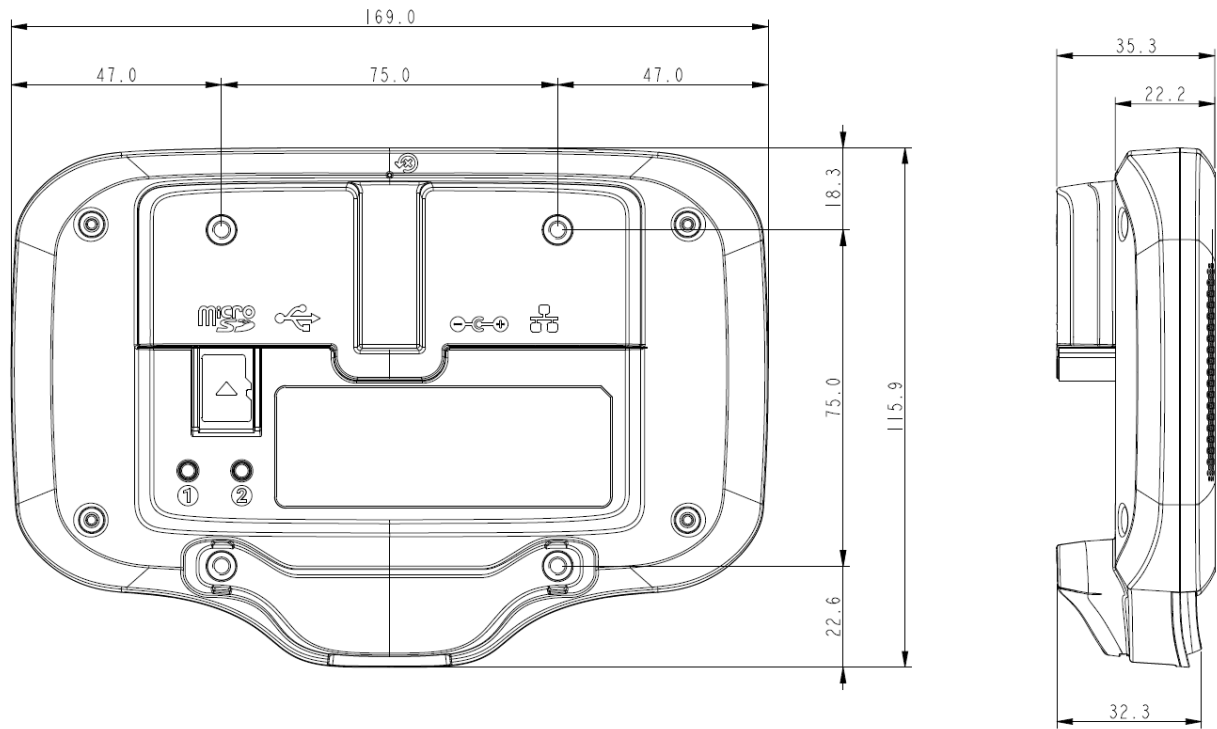


Figure 11 CC6000 Portrait Measurements

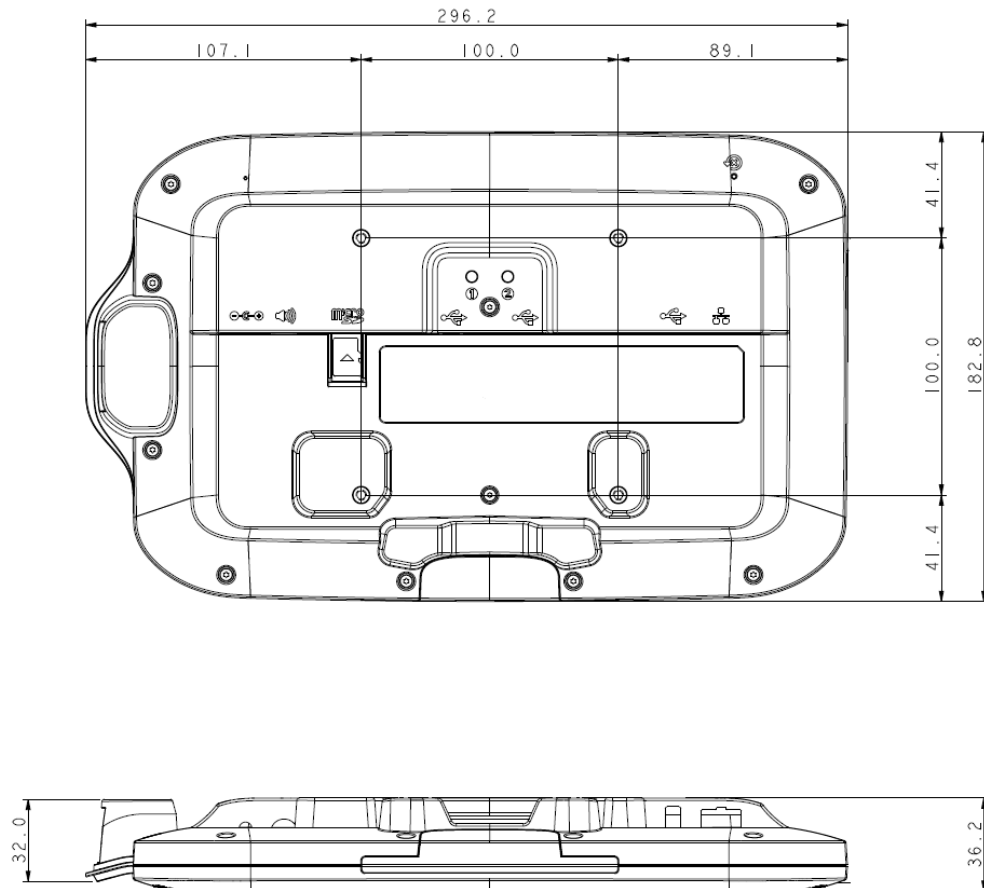


Figure 12 CC6000 Landscape Measurements

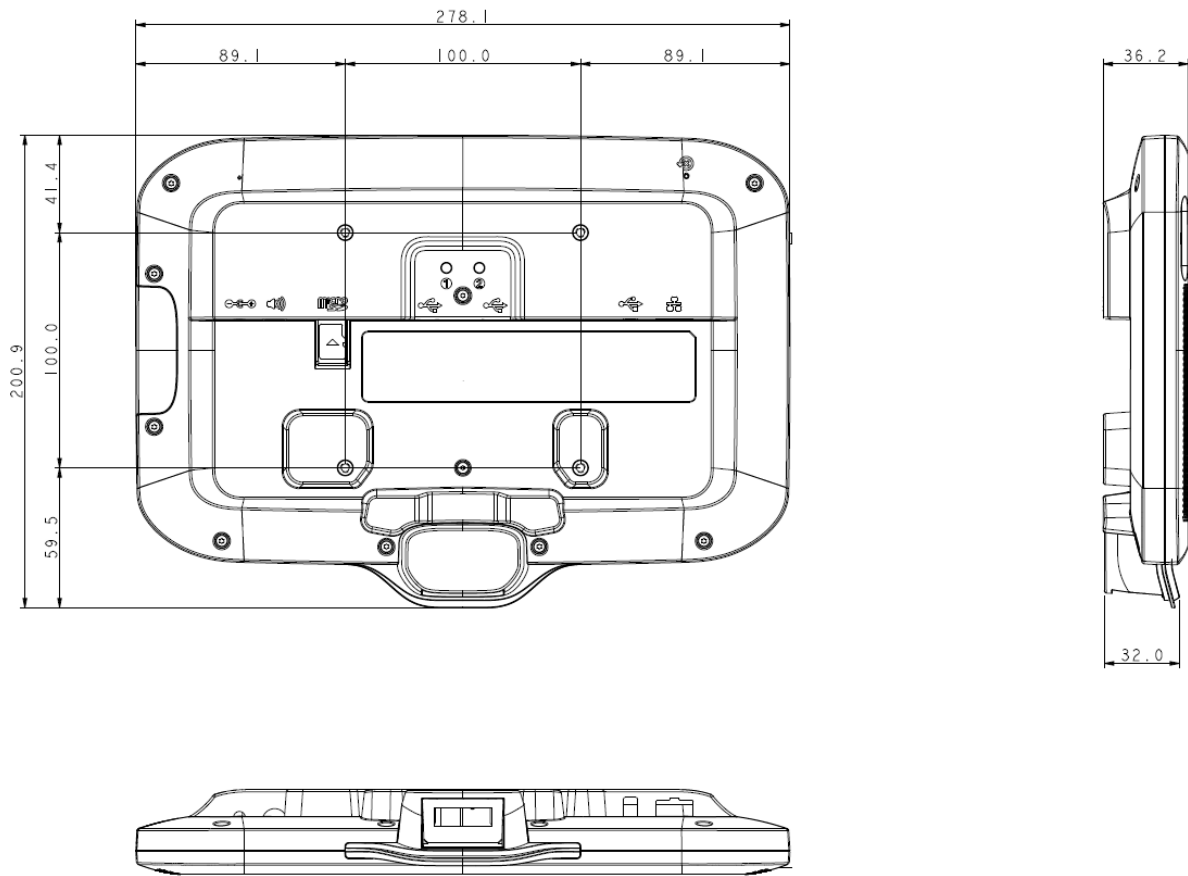


Figure 13 CC600 Mounting Bracket

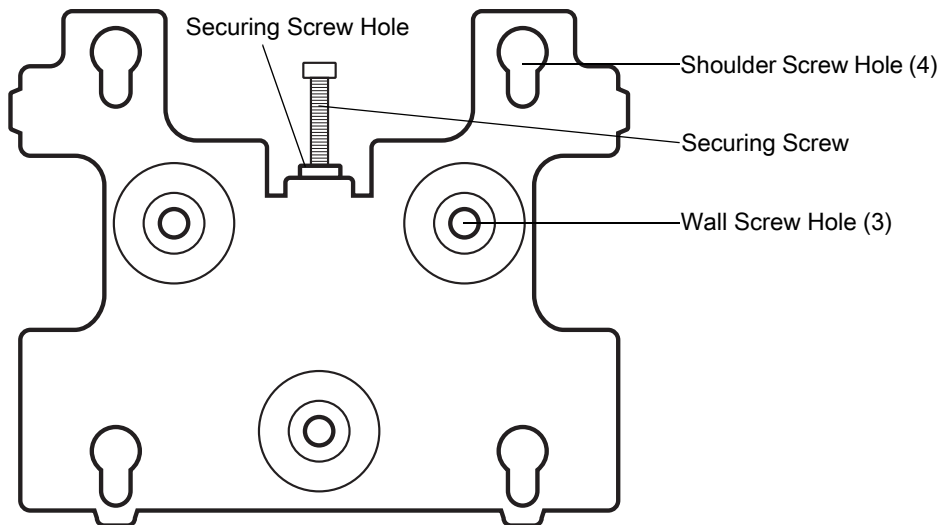


Figure 14 CC6000 Mounting Bracket - Portrait Orientation

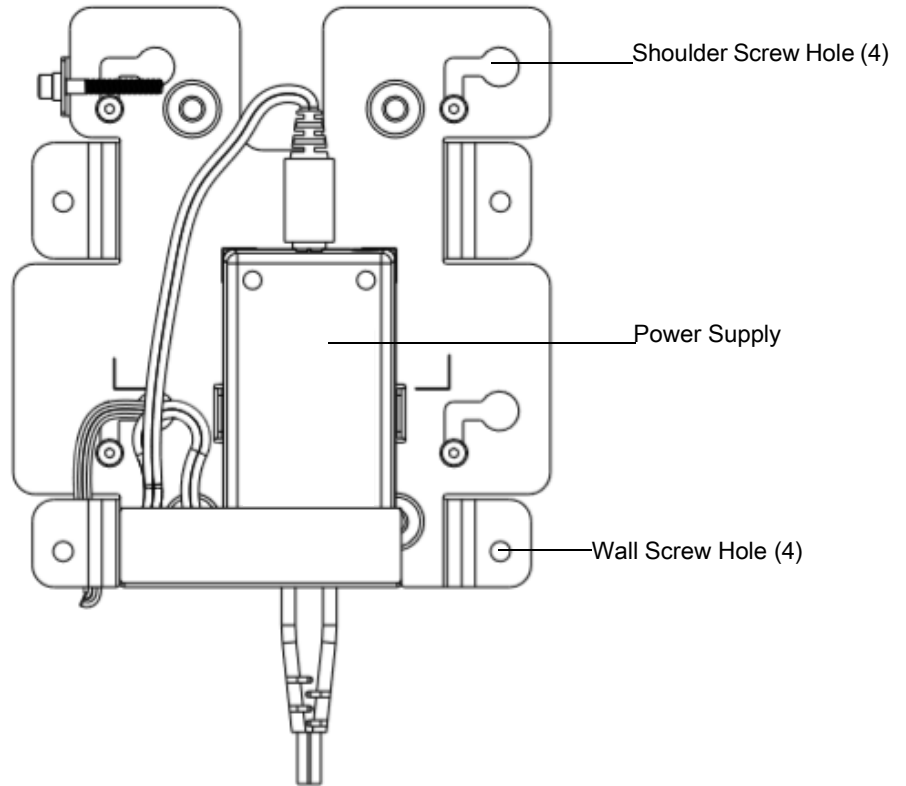
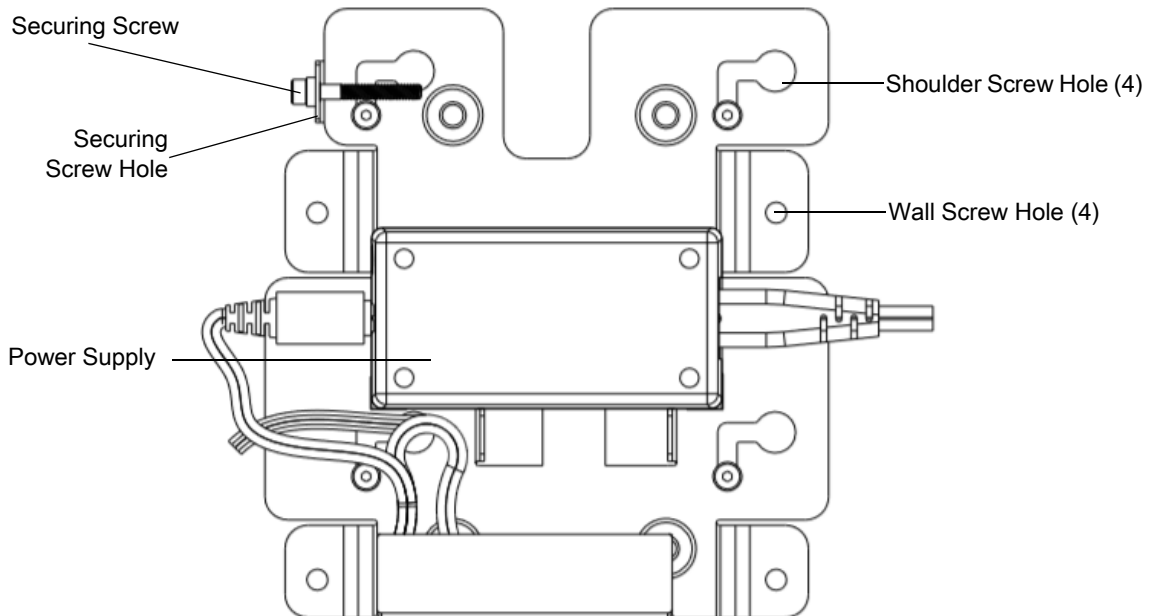


Figure 15 CC6000 Mounting Bracket (KT-152098-03) - Landscape Orientation



To mount the device:

1. Determine the CC600 or CC6000 mounting location.
2. Secure the mounting plate to the wall using the screws provided (three screws for the CC600 plate and four screws for the CC6000).

Figure 16 Attaching the CC600 Bracket To Wall

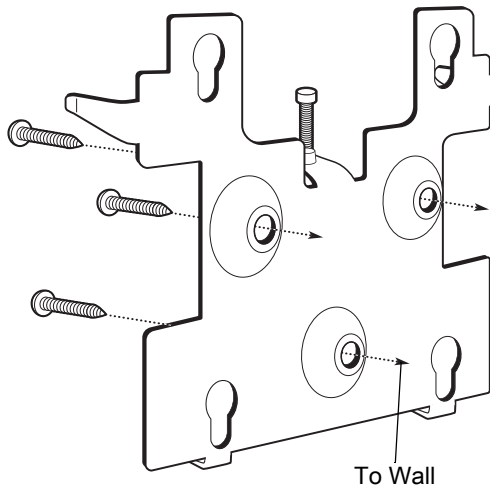
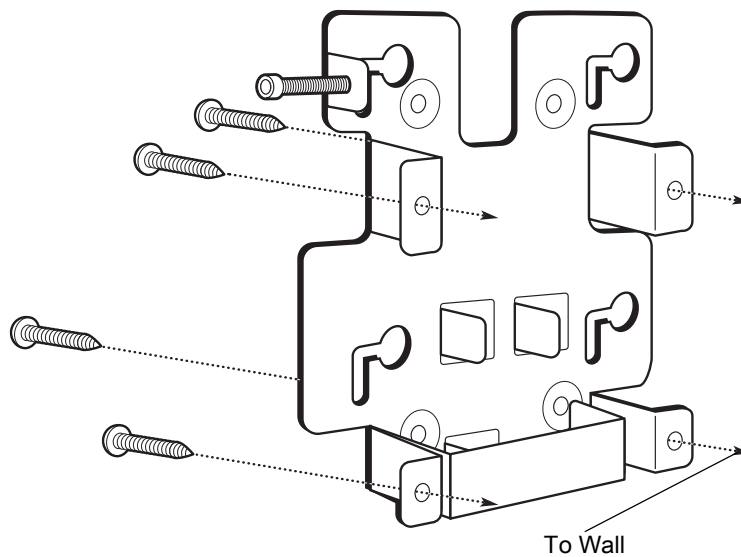
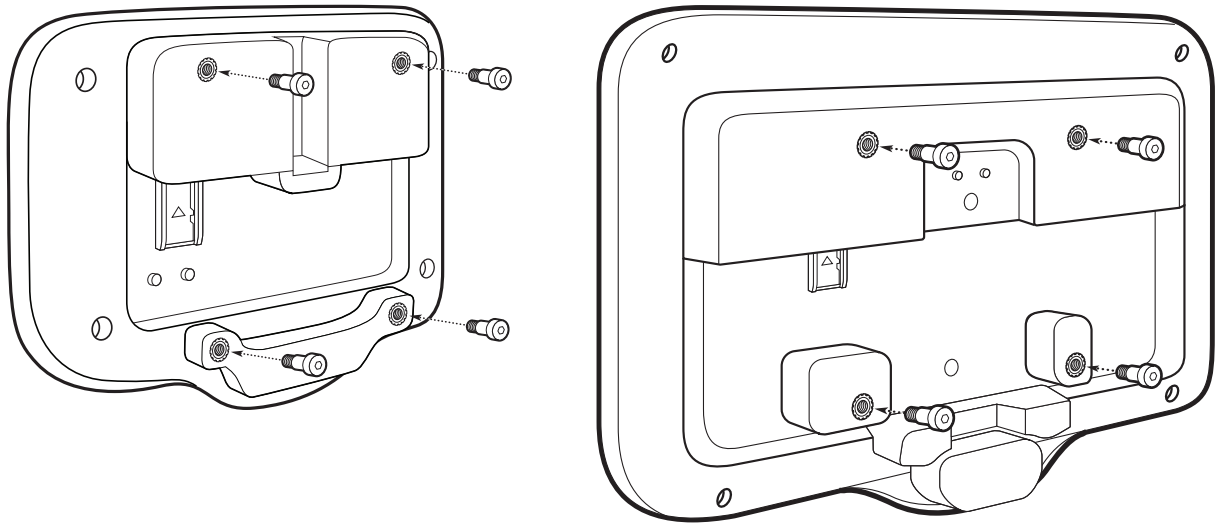


Figure 17 Attaching the CC6000 Bracket To Wall



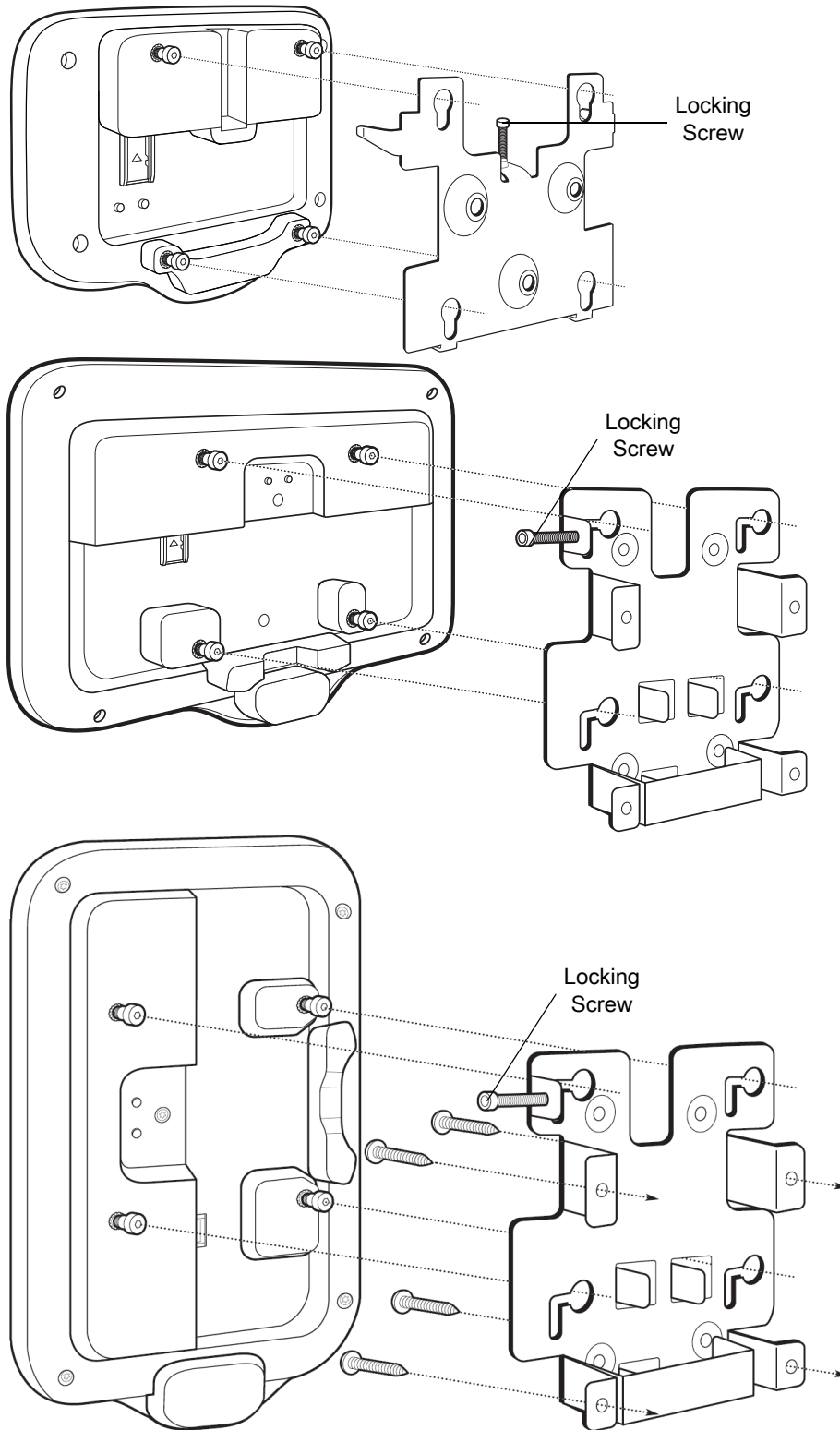
3. Insert the four shoulder screws, also provided, into the mounting holes in the back of the device.

Figure 18 Inserting Shoulder Screws



4. Connect the power supply to the power port. Connect any additional cables into the appropriate ports shown in [Figure 3](#) and [Figure 7](#).
5. Mount the device by placing the shoulder screws through the four keyholes on the mounting plate, and slide the device down to secure in place.

Figure 19 Attaching the Device to the Bracket



6. Insert the locking screw through the hole in the tab at the top of the mounting plate. Hand tighten the screw to secure the device.

Google Account Setup



NOTE: The device has to be connected to the Internet in order to set up a Google account (optional). A Google account is only required on devices with GMS software.

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

Zebra Visibility Services

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

Figure 20 Zebra Services



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

Resetting the Device

The device has a recessed reset button (see [Features on page 16](#) for the location of the button).

To activate the reset button, use the tip of a small paper clip (1mm in diameter), insert into the recess, push and hold for 3 seconds.

Device has a recovery console accessible via pressing the Button #1 on the back of the device upon power up or via ADB connection and command.

The following reset functions are supported:

- Soft reset is performed with an ADB command.
- Enterprise reset (see [StageNow on page 120](#) for more information)
- Factory reset (see [StageNow on page 120](#) for more information)

The device recovery mode supports the following functions:

- Flash image from zip file on an SD card or from internal flash.
- Apply a system update from an SD card or from internal flash.

Settings

Introduction


This chapter describes settings available for configuring the device.

WLAN Configuration

This section provides information on configuring Wi-Fi settings.

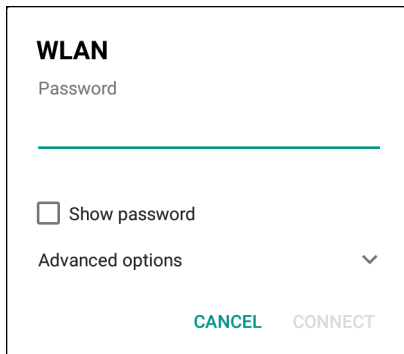
Configuring a Secure Wi-Fi Network

To set up a Wi-Fi network:

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

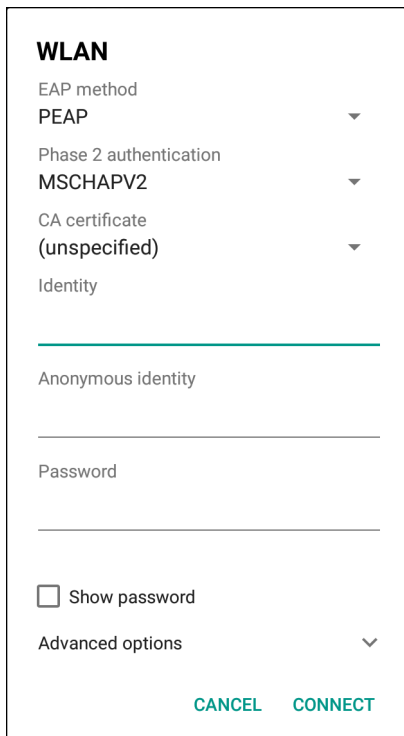
6. Touch the desired network. If the network security is **Open**, the device automatically connects to the network. For all other network security a dialog box appears.

Figure 21 WLAN WEP Network Security Dialog Box



The dialog box is titled "WLAN" and contains the following elements: a "Password" label above a text input field; a "Show password" checkbox; an "Advanced options" label with a downward arrow; and two buttons at the bottom: "CANCEL" and "CONNECT".

Figure 22 WLAN 802.11 EAP Network Security Dialog Box



The dialog box is titled "WLAN" and contains the following elements: "EAP method" dropdown menu with "PEAP" selected; "Phase 2 authentication" dropdown menu with "MSCHAPV2" selected; "CA certificate" dropdown menu with "(unspecified)" selected; an "Identity" label above a text input field; an "Anonymous identity" label above a text input field; a "Password" label above a text input field; a "Show password" checkbox; an "Advanced options" label with a downward arrow; and two buttons at the bottom: "CANCEL" and "CONNECT".

7. If the network security is **WEP** or **WPA/WPS2 PSK**, enter the required password and then touch **Connect**.

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




NOTE: By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See [Configuring for a Proxy Server on page 33](#) for setting connection to a proxy server and see [Configuring the Device to Use a Static IP Address on page 35](#) for setting the device to use a static IP address.

9. Touch **Connect**.
10. Touch .

Manually Adding a Wi-Fi Network

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

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Network & Internet > Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Scroll to the bottom of the list and select **Add network**.
5. In the **Network name** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, set the type of security to:
 - **None**
 - **WEP**
 - **WPA/WPA2 PSK**
 - **802.1x EAP**.
7. If the network security is **None**, touch **Save**.
8. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password and then touch **Save**.

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



NOTE: By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See [Configuring for a Proxy Server on page 33](#) for setting connection to a proxy server and see [Configuring the Device to Use a Static IP Address on page 35](#) 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. In the network dialog box, touch a network.
2. Touch **Advanced options**.

3. Touch **Proxy** and select **Manual**.

Figure 23 Proxy Settings

WLAN

Proxy
Manual

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

Proxy hostname
proxy.example.com

Proxy port
8080

Bypass proxy for
example.com,mycomp.test.com,localhost

IP settings
DHCP

CANCEL CONNECT

Add network

Password
.....

Show password

Advanced options

Proxy
Manual

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

Proxy hostname
proxy.example.com


Proxy port
8080

Bypass proxy for
example.com,mycomp.test.com,localhost

IP settings
DHCP

CANCEL SAVE

4. In the **Proxy hostname** text box, enter the address of the proxy server.
5. In the **Proxy port** text box, enter the port number for the proxy server.
6. 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.

7. Touch **Connect**.
8. Touch .

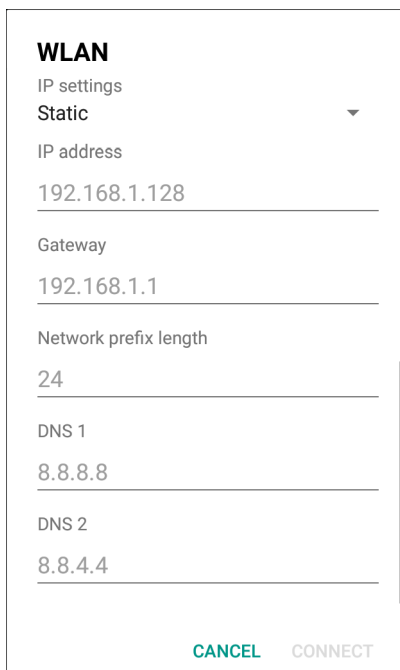
Configuring the Device to Use a Static IP Address

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. In the network dialog box, touch a network.
2. Touch **Advanced options**.
3. Touch **IP settings** and select **Static**.

Figure 24 Static IP Settings



WLAN
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
CANCEL CONNECT

Add network

Show password

Advanced options

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

CANCEL SAVE

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

Wi-Fi Preferences

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

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

Additional Wi-Fi Settings



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

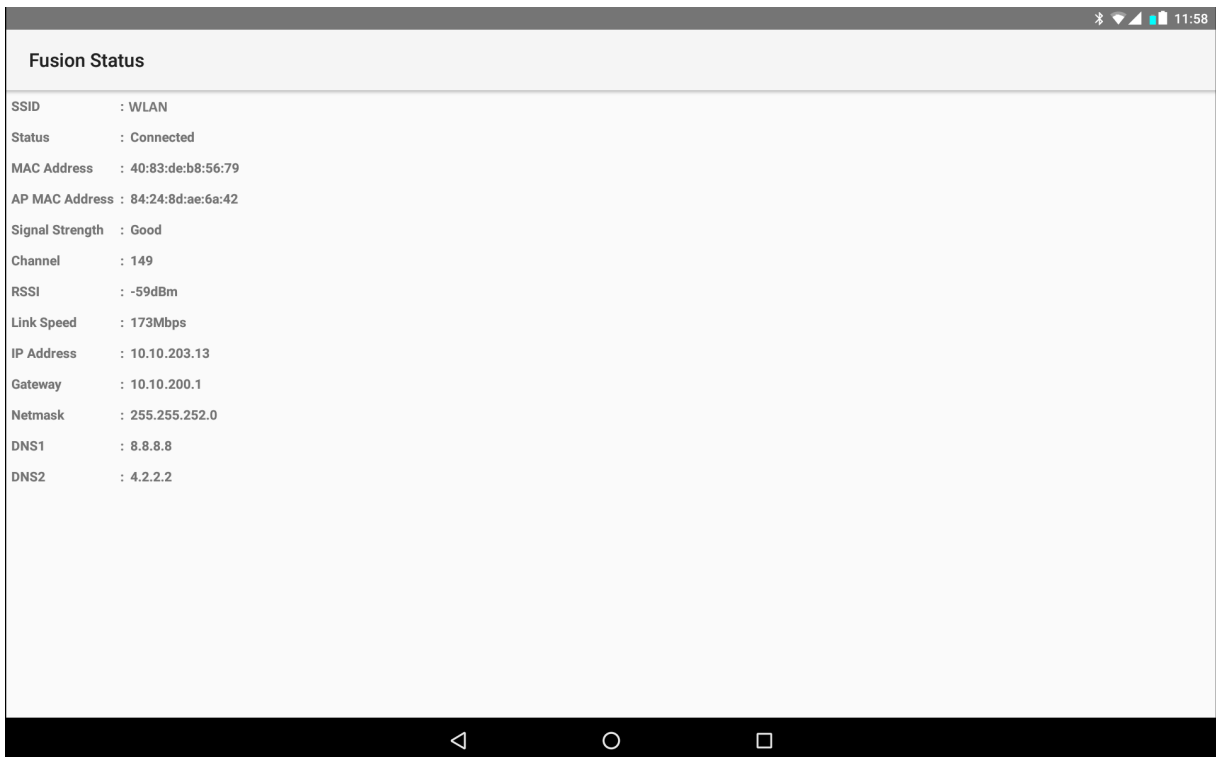
Use the **Additional Settings** to configure additional Wi-Fi settings. To view the additional Wi-Fi settings, scroll to the bottom of the **Wi-Fi** screen and touch **Wi-Fi Preferences > Advanced > Additional settings**.

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

Figure 25 Fusion Logger Screen



Figure 26 Fusion Status Screen

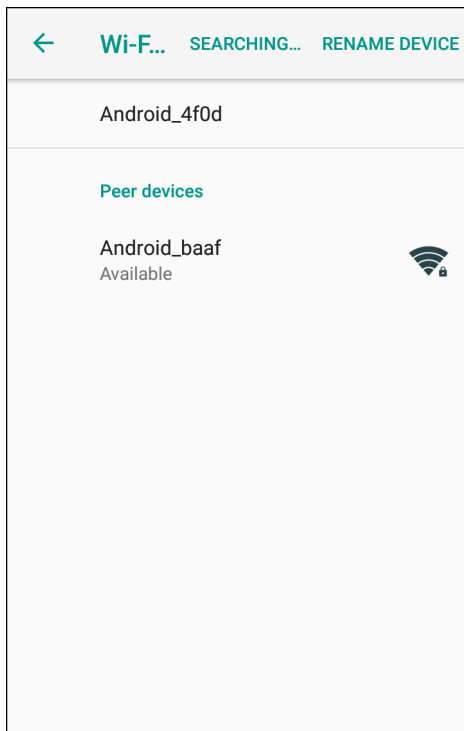


Wi-Fi Direct

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

1. Swipe down from the status bar and then touch .
2. Touch **Wi-Fi > Wi-Fi preferences > Advanced > Wi-Fi Direct**. The device begins searching for another Wi-Fi Direct device.


Figure 27 Wi-Fi Direct Screen



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

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 on page 42](#) for more information.
 - **PIN** - Enter a numeric PIN to unlock screen. See [Setting Screen Lock Using PIN on page 40](#) for more information.
 - **Password** - Enter a password to unlock screen. See [Setting Screen Unlock Using Password on page 41](#) 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.

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


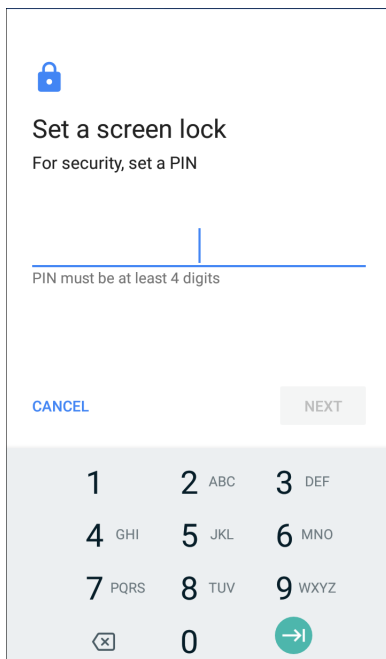

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. To require a PIN upon device start up select **Yes**, or select **No** not to require a PIN.

Figure 28 PIN Screen



The screenshot shows the 'Set a screen lock' screen. At the top, there is a blue padlock icon, followed by the text 'Set a screen lock' and 'For security, set a PIN'. Below this is a horizontal line representing the PIN input field, with a vertical cursor at the end. Underneath the line, it says 'PIN must be at least 4 digits'. At the bottom left, there is a 'CANCEL' button in blue text. At the bottom right, there is a 'NEXT' button in grey text. Below the buttons is a numeric keypad with digits 1 through 9, 0, a backspace icon (X), and a green arrow icon pointing right.

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


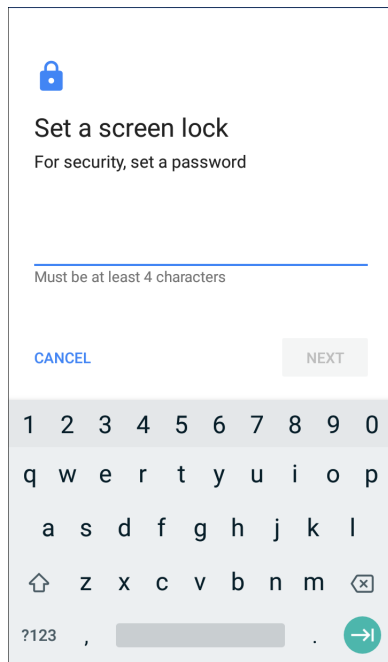

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Password**.
5. To require a password upon device start up select **Yes**, or select **No** not to require a password.
6. Touch in the text field.

Figure 29 Password Screen



7. Enter a password (between 4 and 16 characters) then touch **Next**.
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


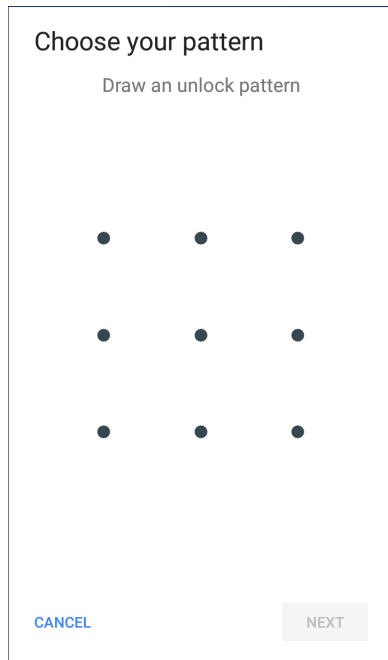
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Pattern**.
5. To require a pattern upon device start up select **Yes**, or select **No** not to require a pattern.


Figure 30 Choose Your Pattern Screen



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

Showing Passwords

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

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

Accounts



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

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



Language Usage

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

Changing the Language Setting

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

Adding Words to the Dictionary

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

Keyboard Settings

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

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

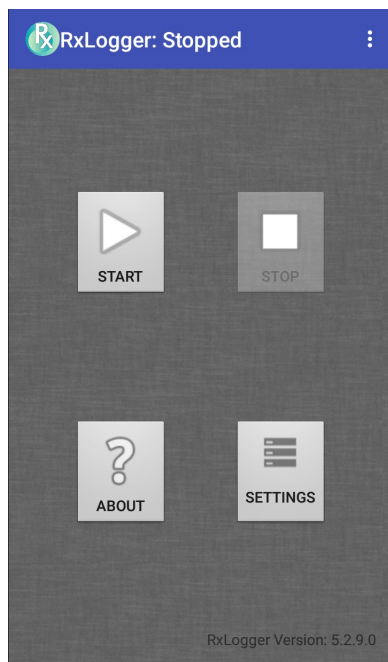
PTT Express Configuration

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

RxLogger

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

Figure 31 RxLogger



RxLogger Configuration

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

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

Figure 32 RxLogger Configuration Screen

SAVE	CANCEL
RxLogger Settings	
ANRModule	
KernelModule	
LogcatModule	
LTSMModule	
RamoopsModule	
ResourceModule	
SnapshotModule	
TCPDumpModule	
TombstoneModule	

RxLogger Settings

The RxLogger Settings module provides additional RxLogger settings.

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

ANR Module

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

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

Kernal Module

The Kernel Module captures kmsg from the system.

- **Enable Module** - Enables logging for this kernal module.
- **Log path** - Specifies the high level log path for storage of all kernal logs. This setting applies globally to all kernal buffers.
- **Kernal Log filename** - Specifies the base log filename for this kernal buffer. The current file count is appended to this name.
- **Max Kernal log file size** - Specifies the maximum size, in megabytes, of an individual log file.
- **Kernal Log interval** - Sets the interval, in seconds, on which to flush the log buffer to the file.

- **Kernal Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Enable System Timestamp in Kernal Log** - Enables system timestamps in kernal logs.
- **System Timestamp Interval** - Sets the interval, in seconds, between system timestamps.
- **Enable Logcat Integration override** - Enables logcat integration overrides.

Logcat Module

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

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

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

LTS Module

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

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

Ramoops Module

The Ramoops Module captures the last kmsg from the device.

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

- **Ramoops file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the log size option.

Resource Module

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

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

Snapshot Module

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

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

- **Usage stats** - Enables dumping of detailed usage information for each package on the device. This includes the number of starts and duration of each run.

TCPDump Module

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

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

Tombstone Module

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



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

Configuration File

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



Enabling Logging

To enable logging:

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

Disabling Logging

To disable logging:

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

Extracting Log Files

1. Connect the device to a host computer using an USB connection.

2. Using a file explorer, navigate to the **RxLogger** folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

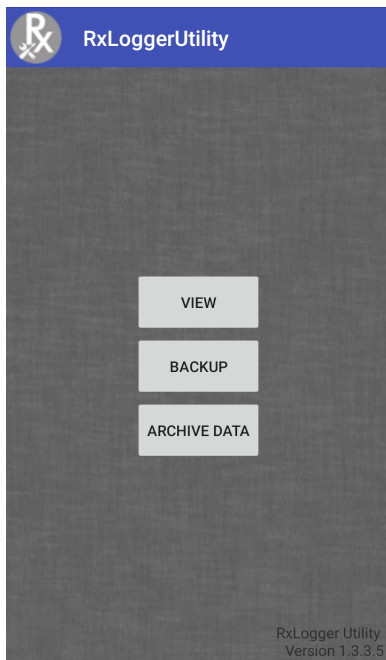
RxLogger Utility

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

App View

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

Figure 33 App View

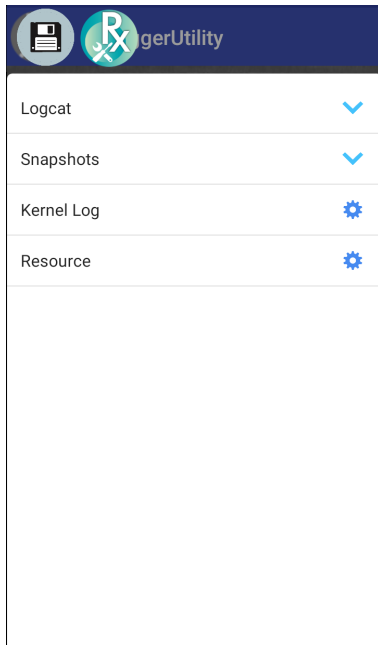


Viewing Logs

To view logs:

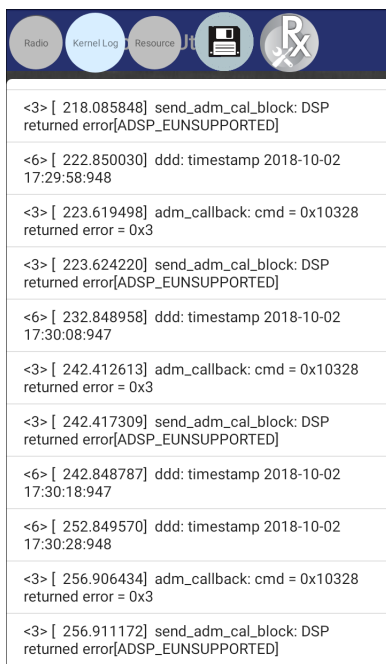
1. Touch the Main Chat Head icon. The Overlay View screen appears.

Figure 34 Overlay View Screen



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

Figure 35 Log File

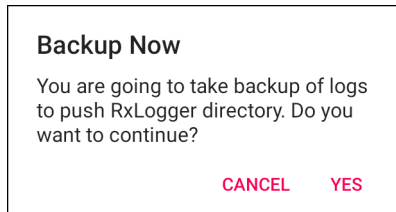


Backup

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

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

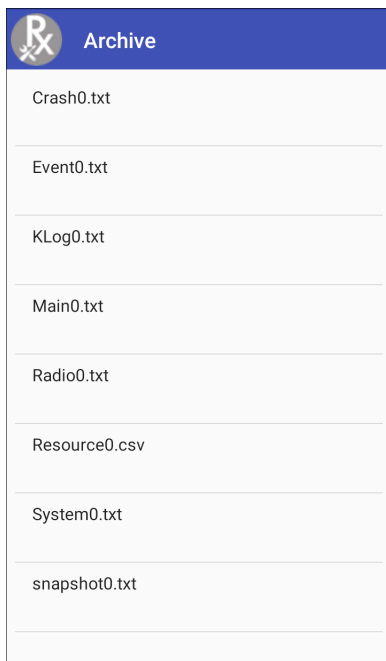
Figure 36 Backup Message



Archive Data

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

Figure 37 Archive



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

Overlay View

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

Initiating the Main Chat Head

To initiate the Main Chat Head:

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

Removing the Main Chat Head

To remove the Main Chat Head icon:

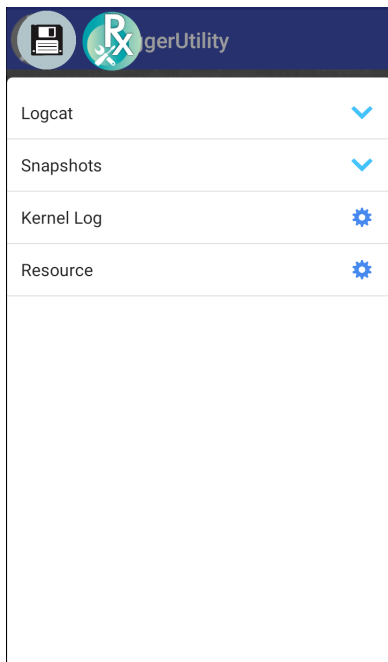
1. Touch and drag the icon. A circle with an X appears.
2. Move the icon over the circle and then release.

Viewing Logs

To view logs:

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

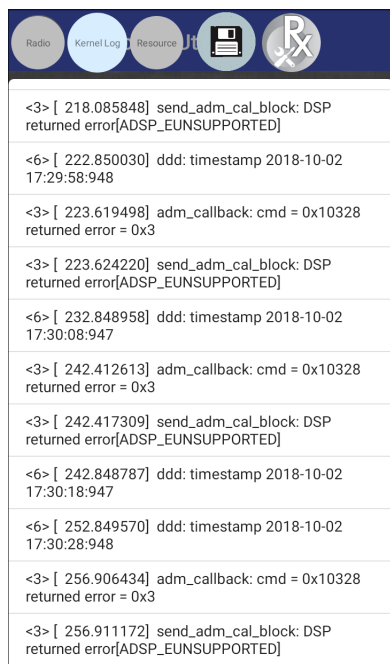
Figure 38 Overlay View Screen



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

4. Touch a Sub Chat Head to display the log contents.

Figure 39 Log File




Removing a Sub Chat Head Icon

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


Backing Up In Overlay View

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

The Backup icon is always available in Overlay View.

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

About Phone

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

- **Status** - Touch to display the following:
 - **IP address** - Displays the IP address of the device.
 - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
 - **Ethernet MAC address** - Displays the Ethernet driver MAC address.
 - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
 - **Serial number** - Displays the serial number of the device.
 - **MSM serial number** - Displays the serial number of the MSM.
 - **Up time** - Displays the time that the device has been running since being turned on.

- **SW components** - Lists filenames and versions for various software on the device.
 - Audio
 - Acoustics
 - MX
 - Hardware ID
 - NFC
 - Scanner
 - Touch
 - Build Date
 - Device Update Version
 - Baseline
 - Secure Boot Status
 - ABL ARB Version
 - Remaining Reboot Count to Lock
- **Legal information** - Opens a screen to view legal information about the software included on the device.
 - Third-party Licenses
 - Google Legal
 - System WebView Licenses
 - Wallpapers
 - Zebra EULA
- **Model** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Android security patch level** - Displays the security patch level date.
- **Baseband version** - Displays WAN radio firmware version (WWAN only).
- **Kernel version** - Displays the kernel version.
- **Build Fingerprint** - Defines Device Manufacturer, Model, Android version and Build version together in one location.
- **Build number** - Displays the software build number.

USB/Ethernet Communication

Introduction

This chapter describes the use and configurations of the USB ports and the Ethernet connection.

The CC6000 includes two USB-2 ports for external peripherals, and one USB-C that can be used for OTG or an external monitor.

The CC600 includes one USB-C that can be used as an OTG port or to connect to an external monitor or USB peripherals (which can be connected simultaneously using a splitter).

Transferring Files with a Host Computer via USB

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

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

Transferring Files

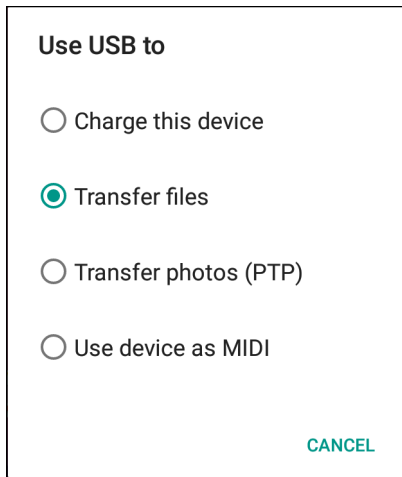


NOTE: Use Transfer files to copy files between the device (internal memory or microSD card) and the host computer.

1. Connect a USB cable to the device.

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

Figure 40 Use USB to Dialog Box



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

Transferring Photos

To transfer photos using Photo Transfer Protocol:



NOTE: Use Photo Transfer Protocol (PTP) to copy photos from either the microSD card or internal memory to the host computer.

1. Connect USB cable to the device. (See [Features on page 16](#) for communication ports.)
2. Pull down the Notification panel and touch **USB charging this device**.
3. Touch **Transfer photos (PTP)**.
4. On the host computer, open a file explorer application.
5. Open the **SD card** or the **Internal storage** folder.
6. Copy or delete photos as required.

Disconnect from the Host Computer


To disconnect the device from the host computer:



CAUTION: Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.

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

USB/Ethernet Communication

For POE (Ethernet) communication, connect an Ethernet cable to the  port.

For USB communication, connect a USB cable to the  port.

Ethernet Settings

The following settings can be configured when using Ethernet communication:

- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings



NOTE: Ethernet is on is the default for the device.

To configure the Ethernet connection:


1. Connect one end of the Ethernet cable to the POE port on the device.
2. Connect the other end to an active Ethernet jack or hub.
3. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
4. Touch **Network & Internet**.
5. Touch **Ethernet**.
6. Slide the switch to the **ON** position.
7. Touch and hold **Eth0** until the menu appears.
8. Touch **Modify Proxy**.
9. Touch the **Proxy** drop-down list and select **Manual**.

Figure 41 Ethernet Proxy Settings

<··> eth0
 Proxy
 Manual ▾
 Proxy hostname
 proxy.example.com
 Proxy port
 8080
 Bypass proxy for
 example.com,mycomp.test.com,|
 CANCEL MODIFY

10. In the **Proxy hostname** field, enter the proxy server address.


11. In the **Proxy port** field, enter the proxy server port number.



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

12. In the **Bypass proxy for** text box, enter addresses for web sites that do not require to go through the proxy server. Use the separator “|” between addresses.

13. Touch **MODIFY**.

14. Touch .

Configuring Ethernet Static IP Address

To configure the Ethernet Static IP Address:



1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch **Network & Internet**.
3. Touch **Ethernet**.
4. Slide the switch to the **ON** position.
5. Touch **Eth0**.
6. Touch the **IP settings** drop-down list and select **Static**.

Figure 42 Static IP Settings

 **eth0**

Proxy
None

IP settings
Static

IP address
192.168.1.128

Gateway
192.168.1.1

Netmask
255.255.255.0

DNS 1
8.8.8.8

DNS 2
4.4.4.4



CANCEL CONNECT

7. In the **IP** address field, enter the proxy server address.

8. If required, in the **Gateway** field, enter a gateway address for the device.

9. If required, in the **Netmask** field, enter the network mask address
10. If required, in the **DNS address** fields, enter a Domain Name System (DNS) addresses.
11. Touch **CONNECT**.
12. Touch .

Establishing Ethernet Connection

1. Swipe down with two fingers from the status bar to open the quick access panel and then touch .
2. Touch **Network & Internet**.
3. Touch **Ethernet**.
4. Insert the device into a slot.
5. Slide the Ethernet switch to the **ON** position.
The  icon appears in the Status bar.
6. Touch **Eth0** to view Ethernet connection details.

DataWedge

Introduction

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

Basic Scanning

Scanning can be performed using the CC600 and CC6000 Customer Concierge or an imager such as the DS22X8 or DS81X8.

Barcode Capture with an Imager

To capture barcode data with the CC600/CC6000 Customer Concierge:

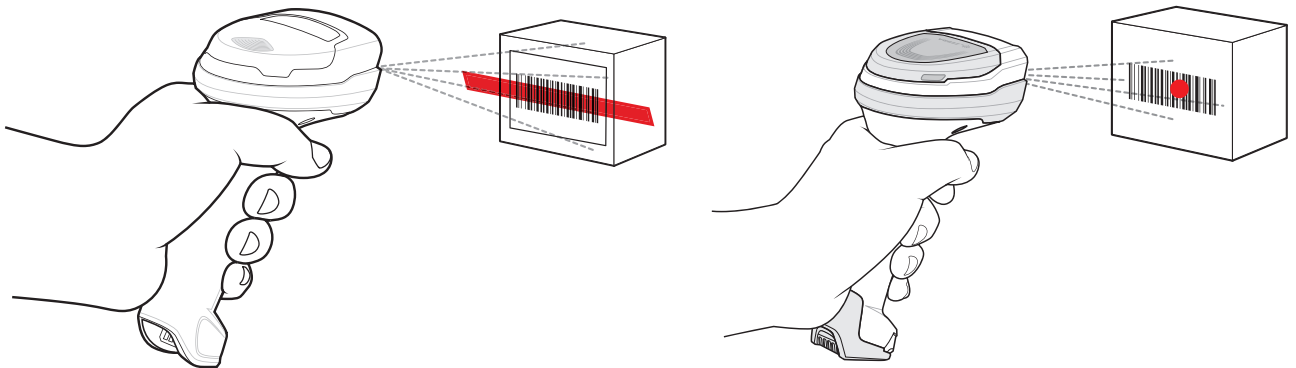
1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Place the barcode in the field of view of the device's scan window. Ensure the barcode is within the scanner's aiming pattern.
3. The LEDs light green and a beep sounds, by default, to indicate the barcode was decoded successfully. Note that when the device is in Pick List Mode, the device does not decode the barcode until the center of the illuminated line or dot touches the barcode.

To capture barcode data with the DS22X8 or DS81X8 imager:

1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Press and hold the trigger until either:
 - a. The imaging scanner reads the bar code. The imaging scanner beeps, the LED flashes, and the scan line turns off.
 - or
 - b. The imaging scanner does not read the bar code and the scan line turns off.

Note that when the device is in Pick List Mode, the device does not decode the barcode until the center of the illuminated line or dot touches the barcode.

Figure 43 Aiming Pattern on Bar Code - DS22X8 and DS81X8



3. Release the trigger.
4. The barcode content data appears in the text field.

Profiles

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

Profile information consists of:

- Associated application
- 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.



IMPORTANT: 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.

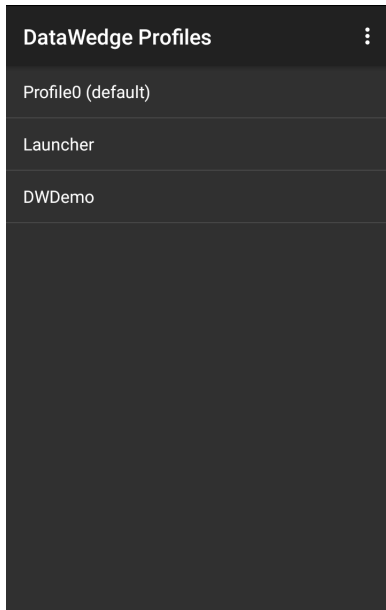
Profiles Screen

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 44 DataWedge Profiles Screen



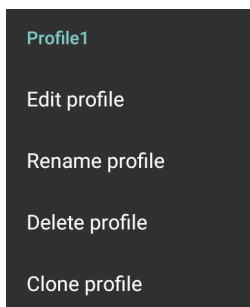
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

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 45 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


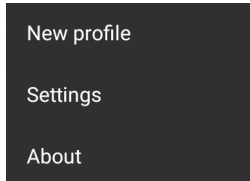


Touch  to open the options menu.

Figure 46 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:



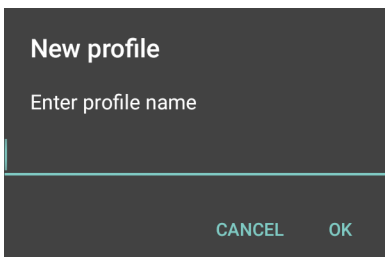
1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **New profile**.
4. In the **New profile** dialog box, enter a name for the new profile. It is recommended that profile names be unique and made up of only alpha-numeric characters (A-Z, a-z, 0-9).

Figure 47 New Profile Name Dialog Box



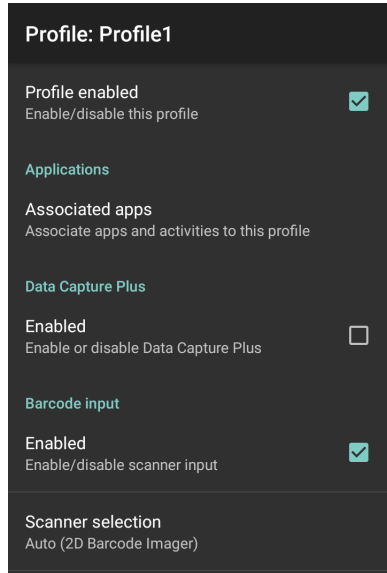
5. Touch **OK**.

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 48 Profile Configuration Screen



The configuration screen lists the following sections:

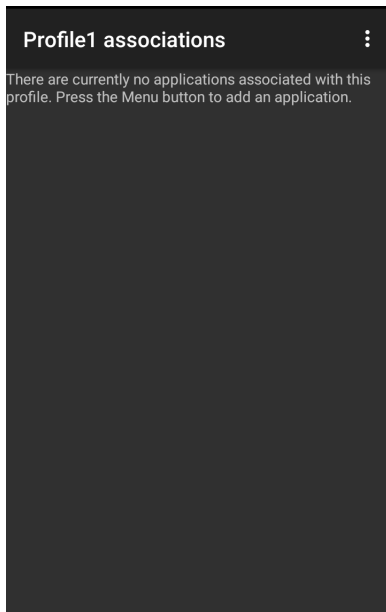
- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode Input
- Keystroke output
- Intent Output
- Voice Output
- IP Output.

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.

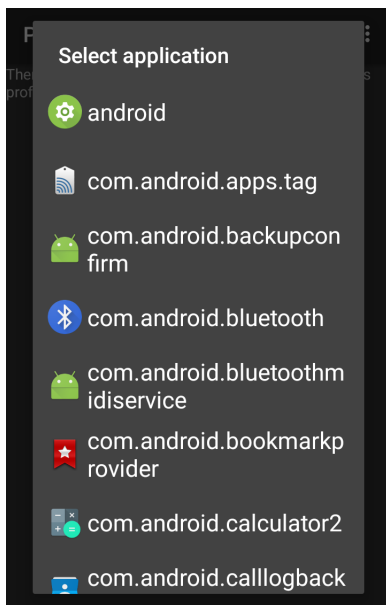
1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.

Figure 49 Associated Apps Screen



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

Figure 50 Select Application Menu

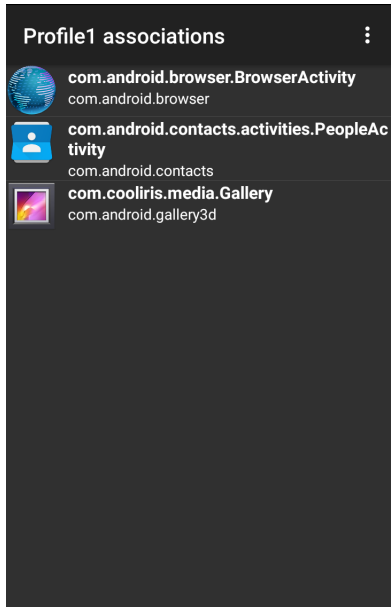


4. In the **Select application** screen, select the desired application from the list.
5. In the **Select activity** menu, selecting the activity adds that application/activity combination to the associated application list for that profile. Selecting * as the activity results in all activities within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

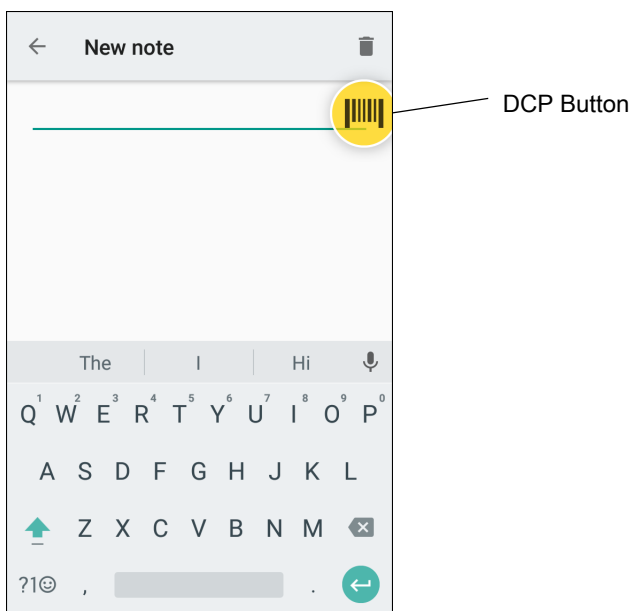
Figure 51 Selected Application/Activity



Data Capture Plus

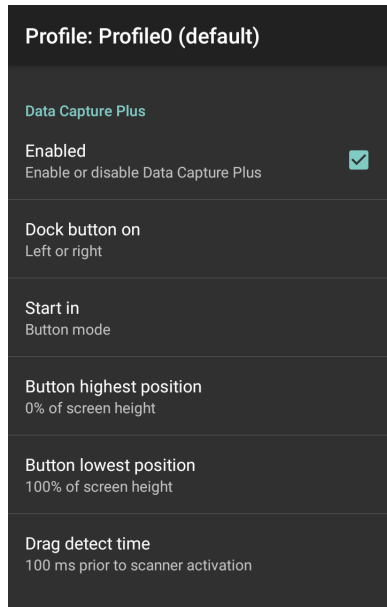
Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching a designated part of the screen. A variable screen overlay acts like a scan button.

Figure 52 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 53 Data Capture Panel Settings



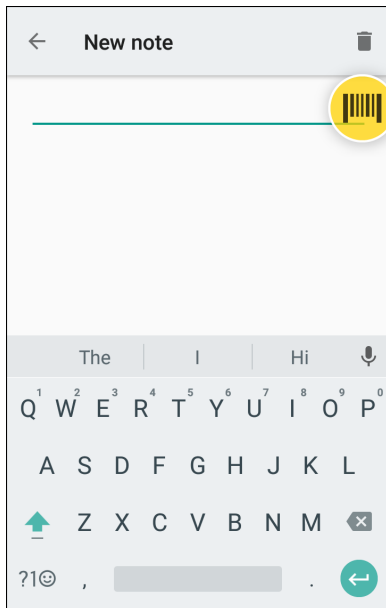
- **Enable** - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
 - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
 - **Left only** - Places the button on left edge of the screen.
 - **Right 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 54 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.
- **Camera Scanner** - Scanning is performed with the rear-facing camera.
- **2D Barcode Imager** - Scanning is performed using the 2D Imager.
- **Bluetooth Scanner** - Scanning is performed using the optional Bluetooth scanner.
- **RS6000 Bluetooth Scanner** - Scanning is performed using the RS6000 Bluetooth scanner.
- **DS3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.
- **LI3678 Bluetooth Scanner** - Scanning is performed using the DS3678 Bluetooth scanner.

Auto Switch to Default on Event

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

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

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

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



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

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

Configure Scanner Settings

Select Configure Scanner Settings to set the following:

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

Decoders

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

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




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

Table 5 *Supported Decoders*

Decoders	Internal Imager SE4710-SR / SE4850-ER / SE2100	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
Australian Postal	O	O	O	O	O	--
Aztec	X	X	X	X	X	--
Canadian Postal	O	--	O	--	--	--
Chinese 2 of 5	O	O	O	O	O	O
Codabar	X	X	X	X	X	X
Code 11	O	O	O	O	O	O
Code 128	X	X	X	X	X	X
Code 39	X	X	X	X	X	X
Code 93	O	O	O	O	O	O
Composite AB	O	O	O	O	O	--
Composite C	O	O	O	O	O	--
Discrete 2 of 5	O	O	O	O	O	O
Datamatrix	X	X	X	X	X	--
Dutch Postal	O	O	O	O	O	--
EAN13	X	X	X	X	X	X
EAN8	X	X	X	X	X	X
GS1 DataBar	X	X	X	X	X	X
GS1 DataBar Expanded	X	X	X	X	X	X
GS1 DataBar Limited	O	O	O	O	O	O
GS1 Datamatrix	O	--	O	O	O	--
GS1 QRCode	O	--	O	O	O	--
HAN XIN	O	--	O	O	O	--
Key X = Enabled O = Disabled -- = Not Supported						

Table 5 Supported Decoders (Continued)

Decoders	Internal Imager SE4710-SR / SE4850-ER / SE2100	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
Interleaved 2 of 5	O	O	O	O	O	O
Japanese Postal	O	O	O	O	O	--
Korean 3 of 5	O	O	O	O	O	O
MAIL MARK	X	--	X	X	X	--
Matrix 2 of 5	O	O	O	O	O	O
Maxicode	X	X	X	X	X	--
MicroPDF	O	O	O	O	O	--
MicroQR	O	O	O	O	O	--
MSI	O	O	O	O	O	O
PDF417	X	X	X	X	X	--
QR Code	X	X	X	X	X	--
Decoder Signature	O	O	O	O	--	--
TLC 39	O	O	O	O	O	O
Trioptic 39	O	O	O	O	O	O
UK Postal	O	O	O	O	O	--
UPCA	X	X	X	X	X	X
UPCE0	X	X	X	X	X	X
UPCE1	O	O	O	O	O	O
US4state	O	O	O	O	O	--
US4state FICS	O	O	O	O	O	--
US Planet	O	O	O	O	O	--
US Postnet	O	O	O	O	O	--
Key X = Enabled O = Disabled -- = Not Supported						

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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 14). See [Decode Lengths on page 79](#) for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

GS1 DataBar Limited

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

HAN XIN

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

Interleaved 2 of 5

- **Check Digit**
 - **No Check Digit** - A check digit is not used. (default)
 - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
 - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
- **Length1** - Use to set decode lengths (default - 14). See [Decode Lengths on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 10). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.
- **Length2** - Use to set decode lengths (default - 0). See [Decode Lengths on page 79](#) 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 on page 79](#) for more information.

- **Length 2** - Use to set decode lengths (default - 55). See [Decode Lengths on page 79](#) for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).

Trioptic 39

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

UK Postal

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

UPCA

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

UPCE0

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

UPCE1

- **Convert UPCE1 To UPCA** - Enable this to convert UPCE1 decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable this to transmit UPCE1 decoded data as UPCE1 data, without conversion (default - disabled).

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

There are three options for transmitting a UPCE1 preamble:

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

US Planet

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

Decode Lengths

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

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

UPC EAN Params

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



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

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar barcodes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC barcodes. (default - disabled)
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **Bookland Format** - If Bookland EAN is enabled, select one of the following formats for Bookland data:
 - **Format ISBN-10** - The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
 - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).

- **Coupon Report Mode** - Traditional coupon symbols are composed of two barcode: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded barcode. The new format offers more options for purchase values (up to \$999.999) and supports complex discount offers as a second purchase requirement. An interim coupon symbol also exists that contain both types of barcodes: UPC/EAN and Databar Expanded. This format accommodates both retailers that do not recognize or use the additional information included in the new coupon symbol, as well as those who can process new coupon symbols.
 - **Old Coupon Report Mode** - Scanning an old coupon symbol reports both UPC and Code 128, scanning 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 (e.g., UPC-A, EAN-8, EAN-13). Enable this parameter to transmit a barcode only when both the left and right blocks are successfully decoded within one laser scan. Enable this option when barcodes 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.
 - **Supplementals Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the barcode the

number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.

- **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the barcode starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN barcode not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN barcode not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN barcode 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
- **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.

Reader Params

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



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

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

The preferred character set and its preference order is configurable to the user through the **Auto Character Set Preferred Order** menu. Users can change the order by dragging the icon for that menu

item. To delete an item, long press on an item and the **Delete** option will appear. To add a new item, tap the menu icon at top right corner and options to add UTF-8 and GB2312 will appear.

- **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
- **GB2312** - Character set of the People's Republic of China, used for simplified Chinese characters.
- **Auto Character Set Failure Option** - If the system cannot find a character set from the preferred list that can be used to successfully decode the data, the character set selected in **Auto Character Set Failure Option** is used to decode the data and send to the user. If **NONE** is used, Null data is returned as string data.
 - **NONE**
 - **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
 - **ISO-8859-1** - Part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
 - **Shift_JIS** - ended for Western European languages.
 - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
 - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.
- **Presentation Parameters** - select Barcode Input for Scene Detection Qualifier.
 - **Proximity Sensor Input** - enables Presentation mode only after a proximity event.
 - **None** - enables Default Presentation Mode.
- **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** - Not applicable.
 - **Disable**
 - **Enable** (default).
- **Beam Width** - Beam Width is applicable only with linear scanners.
 - **Narrow**
 - **Normal** (default)
 - **Wide**
- **Aim mode** - Turns the scanner illumination on or off.
 - **On** - Illumination on (default).
 - **Off** - Illumination 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 by selecting trigger, presentation or continuous read.
 - **Trigger** - A trigger event activates decode processing, which continues until the trigger event ends or a valid decode occurs (default).
 - **Presentation** - Enables presentation mode scanning.
 - **Continuous Read** - Select the soft trigger to start a continuous read of the same bar code. 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 within the illuminated scan dot. 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.

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 barcode 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).

Keep enabled on suspend

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

Voice Input

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. DataWedge is currently not capturing data for 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.

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

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.
- **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 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.
- **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 on page 93](#) for more information.
- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
 - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
 - **Prefix to data** - Add characters to the beginning of the data when sent.
 - **Suffix to data** - Add characters to the end of the data when sent.
 - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
 - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
 - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Output

Allows configuration of the Intent Output Plug-in for the profile. The Intent Output Plug-in allows the captured data to be sent to an application in the form of an implicit Intent. Refer to the Android Developer web site for more information, <http://developer.android.com>.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).
- **Intent delivery** - Select the method by which the intent is delivered:
 - Send via StartActivity
 - Send via startService (default)
 - Broadcast intent
- **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 on page 93](#) 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 e.g. 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.

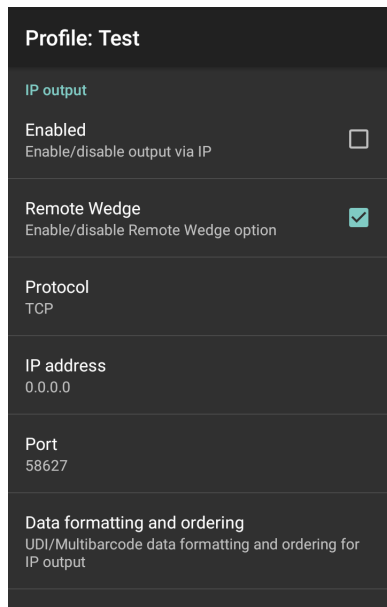
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol 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 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 on page 93](#) 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 55 IP Output Screen

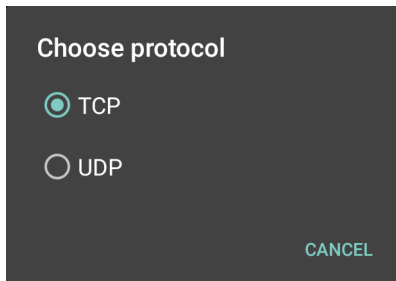


Using IP Output with IPWedge

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

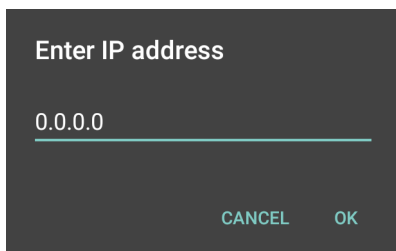
1. In **IP Output**, touch **Enabled**.
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is enabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).

Figure 56 Protocol Selection



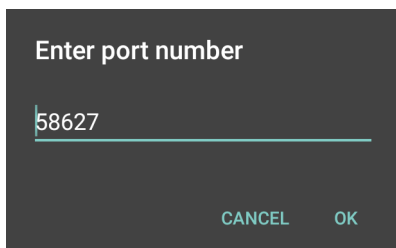
5. Touch **IP Address**.
6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

Figure 57 IP Address Entry



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

Figure 58 Port Number Entry



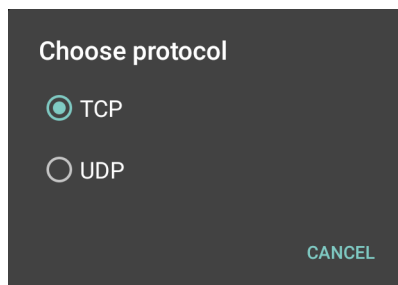
9. Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

Using IP Output without IPWedge

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

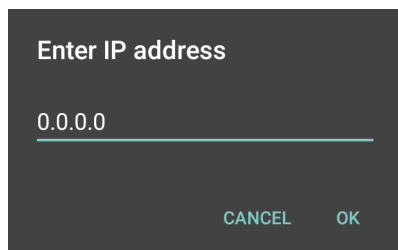
1. In **IP Output**, touch **Enabled**.
A check appears in the checkbox.
2. Ensure **Remote Wedge** option is disabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

Figure 59 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.

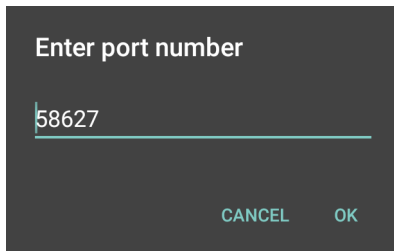
Figure 60 IP Address Entry



7. Touch **Port**.

- In the **Enter port number** dialog box, enter the port number that the host computer application is listening on.

Figure 61 Port Number Entry



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


Generating Advanced Data Formatting Rules

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

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

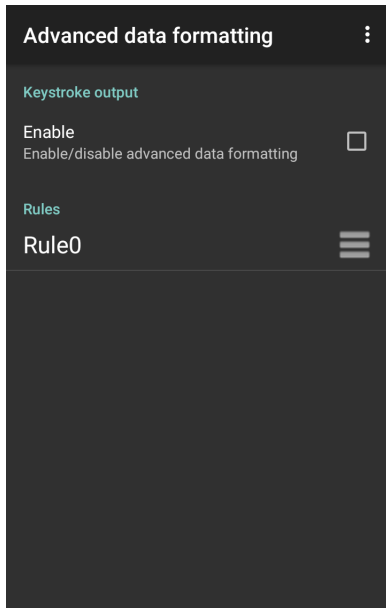
Configuring ADF Plug-in

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

- Swipe up from the bottom of the screen and touch .
- Touch a DataWedge profile.

3. In **Keystroke Output**, touch **Advanced data formatting**.

Figure 62 Advanced Data Formatting Screen



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

Creating a Rule



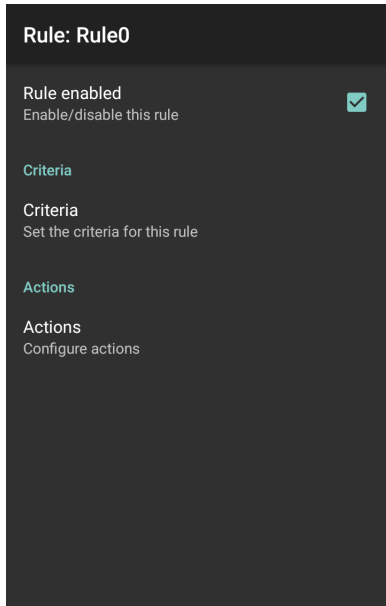
NOTE: By default, **Rule0**, is the only rule in the Rules list.

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 63 Rule List Screen

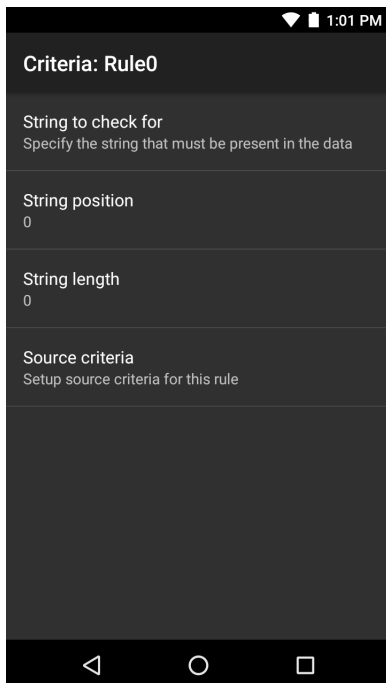


2. Touch the **Rule enabled** checkbox to enable the current rule.

Defining Criteria

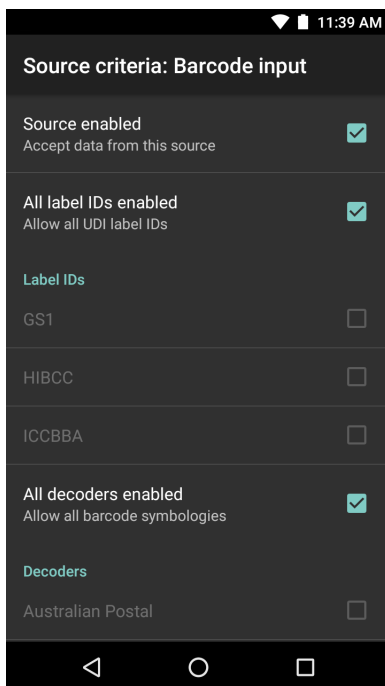
1. Touch **Criteria**.

Figure 64 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 65 Barcode Input Screen






14. For general barcode inputs, touch the **All decoders enabled** checkbox to select all barcode 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.
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 6 *ADF Supported Actions*

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

Table 6 ADF Supported Actions (Continued)

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

Deleting an Action

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

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

When a user scans a barcode with the following criteria:




- Code 39 barcode.

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

Modify the data as follows:

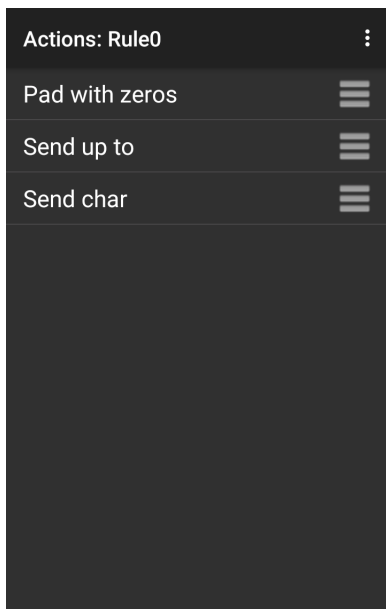
- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

To create an ADF rule for the above example:

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

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

Figure 66 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 67 Sample Barcode



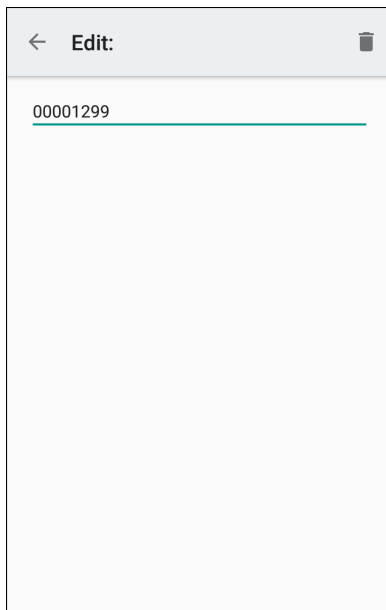
48. Press and hold the scan button.

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

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

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

Figure 68 Formatted Data



DataWedge Settings


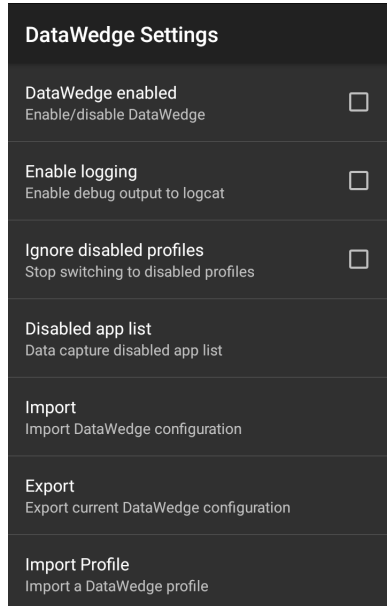


The DataWedge Settings screen provides access to general, non-profile related options. Touch  > **Settings**.

Figure 69 DataWedge Settings Window



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



Importing a Configuration File

1. Copy the configuration file to the microSD card `/Android/data/com.symbol.datawedge/files` folder.
2. Swipe up from the bottom of the screen and touch .
3. Touch .
4. Touch **Settings**.
5. Touch **Import**.

6. Touch **filename to import**.

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



Exporting a Configuration File

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



Importing a Profile File



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



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

Exporting a Profile

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

Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **Restore**.
5. Touch **Yes**.

Configuration and Profile File Management

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

After making configuration or profile changes, export the new configuration or profile to the root of the On-device Storage. The configuration file created is automatically named `datawedge.db`. The profile file created is automatically named `dwprofile_x.db`, where `x` is the profile name. The files can then 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.


Capture Data and Taking a Photo in the Same Application

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

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

Disable DataWedge on Device and Mass Deploy

To disable DataWedge and deploy onto multiple devices:

1. Swipe up from the bottom of the Home screen and touch **DataWedge**.
2. Touch .
3. Touch **Settings**.
4. Unselect the **DataWedge enabled** check box.
5. Export the DataWedge configuration. See Exporting a Configuration File on page 103 for instructions. See Configuration and Profile File Management on page 104 for instructions for using the auto import feature.



DataWedge APIs

DataWedge APIs operate primarily through Android intents - specific commands that can be used by other applications to control data capture without the need to directly access the DataWedge UI. For more information, see <http://techdocs.zebra.com/datawedge/6-8/guide/api/>

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.

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 (e.g. 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 (e.g. 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 barcodes to be scanned. Activity B only requires Code 128 barcodes to be scanned. Profile EAN13 is configured to only scan EAN13 barcodes 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 (e.g. 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**

Imager as Camera

Use the standard Android SDK Camera API functions to operate the imager scanner as a camera. When using the imager scanner as a camera, the following Camera API functions are supported:

- **Camera.open(ID)** - Set ID to 100 to open the Imager Scanner as a camera instance.
- **Camera.release()** - Release the Imager Scanner opened using camera API.
- **Camera.setPreviewDisplay(surfaceHolder)** - Add SurfaceView via SurfaceHolder to show preview.
- **Camera.SetPreviewCallback(PreviewCallback)** - Set previewCallback to get preview data.
- **Camera.startPreview()** - Starting Imager Scanner preview via SurfaceView.
- **Camera.stopPreview()** - Stopping Imager Scanner preview showing in SurfaceView.
- **Camera.getCameraInfo(CameraID, CameraInfo)** – Get camera information on camera ID. CameraInfo has the following members:
 - orientation
 - facing
 - canDisableShutterSound

Use the Zebra Mx architecture to decode barcodes with the imager scanner when the imager as camera feature is disabled. When the imager as camera feature is enabled the imager can not decode barcodes and capture images at the same time.

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.

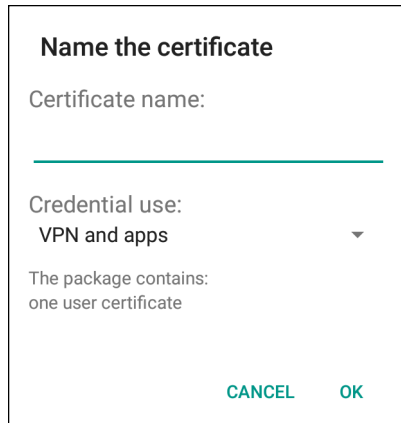
Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory. See [USB/Ethernet Communication](#) for information about connecting the device to a host computer and copying files.
2. Swipe down from the Status bar to open the Quick Access panel and then touch .
3. Touch **Security & Location > Encryption & Credentials**.
4. Touch **Install from storage**.

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


Figure 70 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 microSD card 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 & Location > Encryption & Credentials**.
 - **Trusted credentials** - Touch to display the trusted system and user credentials.
 - **Install from storage** - Touch to install a secure certificate from the microSD card 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 Eclipse IDE. Development can take place on a Microsoft® Windows®, Mac® OS X®, or Linux® operating system.

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

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

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

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

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

Touch **System > About Phone**. 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, supporting Android Lollipop, KitKat®, and Jelly Bean operating systems, and built on the MX 4.3/4.4/5.x/6.0 platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a barcode, 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 barcode, 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 time. The message **You are now a developer!** appears.
5. Touch .
6. Touch **Developer options**.
7. Slide the **USB debugging** switch to the **ON** position.
8. Touch **OK**.
9. Connect the device to the host computer using the Rugged Charge/USB Cable.
The **Allow USB debugging?** dialog box appears on the device.
10. On the device, touch **OK**.
11. On the host computer, navigate to the `platform-tools` folder.

12. Type `adb devices`.

The following displays:

List of devices attached

XXXXXXXXXXXXXXXXX device (where XXXXXXXXXXXXXXXXXXXX is the device number).



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

13. Touch .

Application Installation

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

- USB connection, see [Installing Applications Using the USB Connection on page 121](#).
- Android Debug Bridge, see [Installing Applications Using the Android Debug Bridge on page 122](#).
- microSD Card, see [Installing Applications Using a microSD Card on page 123](#)
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

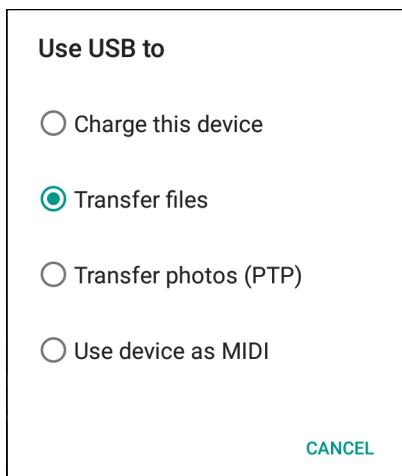
Installing Applications Using the USB Connection



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

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

Figure 71 Use USB Dialog Box



3. Touch **Transfer files**.
4. On the host computer, open a **Files** application.
5. On the host computer, copy the application .apk file from the host computer to the device.



CAUTION: Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.


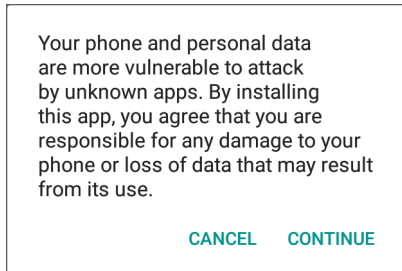
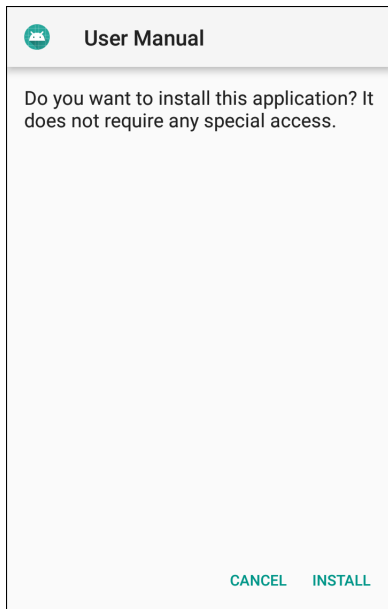
6. Disconnect the device from the host computer.
7. Touch Home, then Swipe the screen up and select  to view files on the microSD card or Internal Storage.
8. Locate the application .apk file.
9. Touch the application file.

Figure 72 Install App Permission Dialog Box



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

Figure 73 Accept Installation Screen



11. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
12. Touch **Open** to open the application or **Done** to exit the installation process. The application appears in the App list.


Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.



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

Ensure that the ADB drivers are installed on the host computer. See [ADB USB Setup on page 120](#).

1. Connect the device to a host computer using USB.
2. Swipe down from the Status bar to open the Quick Access panel and then touch .
3. Touch **System > Developer options**.
4. Slide the switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Touch **OK**.
7. On the host computer, open a command prompt window and use the adb command:
`adb install <application>`
 where: <application> = the path and filename of the apk file.
8. Disconnect the device from the host computer.

Installing Applications Using a microSD Card



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



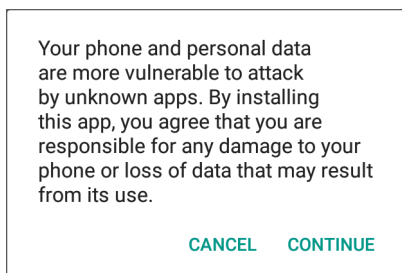
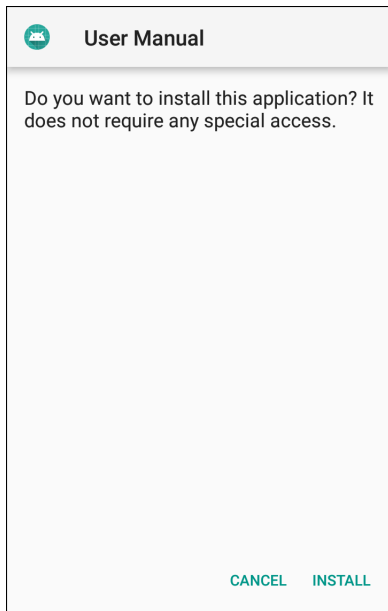
1. Connect the device to a host computer using USB.
2. Copy the application APK file from the host computer to the microSD card.
3. Remove the microSD card from the host computer.
4. Insert the microSD card into the device.
5. Touch Home, then Swipe the screen up and select  to view files on the microSD card.
6. Touch  > **SD card**.
7. Locate the application .apk file.
8. Touch the application file.

Figure 74 Install App Permission Dialog Box



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

Figure 75 Accept Installation Screen



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

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

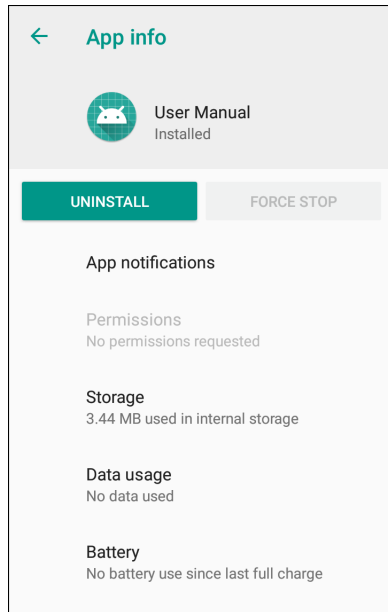
Uninstalling an Application

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 76 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 microSD card 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 microSD Card

1. Copy the System Update zip file to the root of the microSD card.
 - Copy the zip file to a microSD card using a host computer and then installing the microSD card into the device (see [Inserting microSD Card on page 21](#) for more information).
 - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. Disconnect the device from the host computer.
2. Press and hold the Reset button until the Restart option appears. Release the Reset button when the option appears. The device will restart if the button is held down for longer than 3 seconds.
3. Touch **Restart**.


4. Press and hold the Number 1 button. System Recovery screen will appear.
5. Press the Number 2 button to navigate to **Apply upgrade from SD card..**
6. Press the Number 1 button.
7. Use the Number 1 and Number 2 buttons to navigate to the System Update file.
8. Use the Number 2 button to navigate to the System Update file.
9. Press the Number 1 button. The System Update installs and then the device returns to the Recovery screen.
10. Press the Number 1 button to reboot the device.



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

Using ADB

To update the system using ADB:

1. Connect the device to the Rugged Charge/USB cable.
2. Connect the cable to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
4. Touch **System > Developer options**.
5. Slide the switch to the **ON** position.
6. If **USB Debugging** is not **ON** touch **USB Debugging**. 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 Number 2 button to navigate to **Apply upgrade from ADB**.
12. On the host computer command prompt window type:
adb sideload <file>
where: <file> = the path and filename of the zip file.
13. Press **Enter**. The System Update installs (progress appears as percentage in the Command Prompt window) and then the Recovery screen appears.


14. Press the Number 1 button to reboot the device.



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

Verify System Update Installation

To check that the system update installed properly:

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

Performing an Enterprise Reset

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

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

Perform Enterprise Reset using either a microSD card 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 microSD Card

1. Copy the Enterprise Reset zip file to the root of the microSD card.
 - Copy the zip file to a microSD card using a host computer and then installing the microSD card into the device (see [Inserting microSD Card on page 21](#)).
 - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. Disconnect the device from the host computer.
2. Press and hold the Reset button until you get Restart option, release Reset button as you get option.
3. Touch **Restart**.
4. Press and hold the Number 1 button. System Recovery screen will appear.
5. Press the Number 2 button to navigate to Apply upgrade from SD card.
6. Press the Number 1 button. The System Update installs and then the device returns to the Recovery screen.
7. Use the Number 2 button to navigate to the System Update file.

8. Press the Number 1 button. The System Update installs and then the device returns to the Recovery screen.
9. Press the Number 1 button to reboot the device.

Using ADB

To perform an Enterprise Reset using ADB:

1. Connect the device to the Rugged Charge/USB cable.
2. Connect the cable to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
4. Touch **System > Developer options**.
5. Slide the switch to the **ON** position.
6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and type:

```
adb devices.
```

The following displays:

```
List of devices attached
```

```
XXXXXXXXXXXXXXXXX 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 Number 1 and Number 2 buttons to navigate to **apply from adb**.
12. On the host computer command prompt window type:

```
adb sideload <file>
```

where: <file> = the path and filename of the zip file.
13. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.

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 on page 125](#) 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 microSD Card

1. Copy the Factory Reset zip file to the root of the microSD card.
 - Copy the zip file to a microSD card using a host computer and then installing the microSD card into the device (see [Inserting microSD Card on page 21](#)).
 - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. Disconnect the device from the host computer.
2. Switch to recovery mode by pressing and holding the #1 button in the back for 3 seconds while cycling power to the device.
3. Press the Number 1 and Number 2 buttons to navigate to the **apply update from sdcard**.

Using this option, users can perform an OS upgrade using full OTA packages, Diff OTA packages or install Reset Packages from an SD card.

Using ADB

To perform an Factory Reset using ADB:

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

12. Type:

```
adb reboot recovery
```



13. Press Enter. The System Recovery screen appears.
14. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.
15. On the host computer command prompt window type:


```
adb sideload <file>
```

 where: <file> = the path and filename of the zip file.
16. Press Enter. The Factory Reset package installs and then the Recovery screen appears.

Storage

The device contains four types of file storage:

- Random Access Memory (RAM)
- Internal storage
- External storage (microSD card)
- 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.


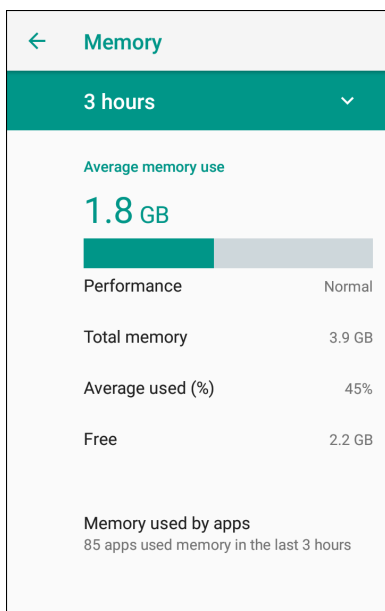
1. To view the amount of free and used memory, swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **System > Developer options > Memory**.

Figure 77 Memory Screen



The screen displays the amount of used and free RAM.

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:


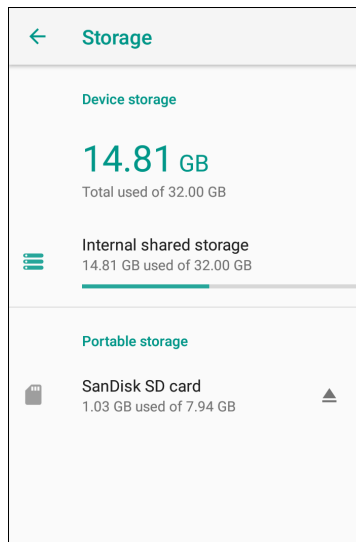
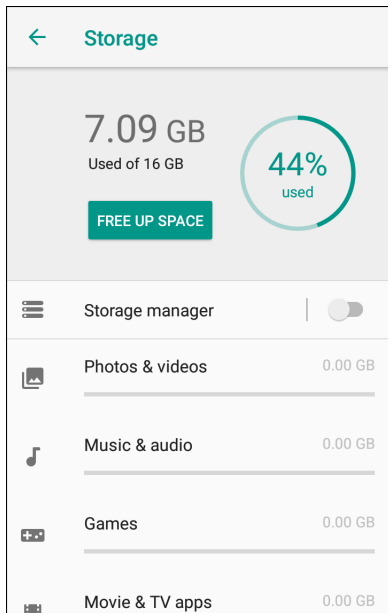
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Storage**.

Figure 78 Storage Screen



- **Internal Storage** - Displays the total amount of space on internal storage and amount used.

Touch **Internal shared storage** to display a the amount of storage used by apps, photos, videos, audio and other files.

Figure 79 Internal Storage Screen

External Storage

The device can have a removable microSD card. The microSD card 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 microSD card:


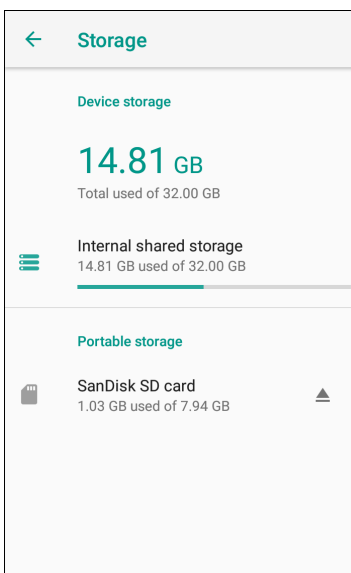
1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Storage**.

Figure 80 Storage Screen

Portable storage displays the total amount of space on the installed microSD card and the amount used.

To unmount the microSD card, touch .

Touch **SD card** to view the contents of the card.

Formatting a microSD Card

To format an installed microSD card as portable storage:


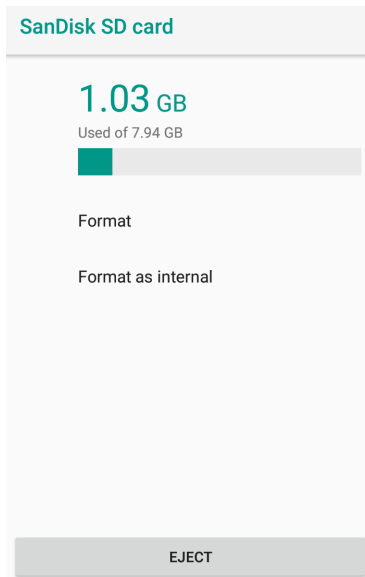
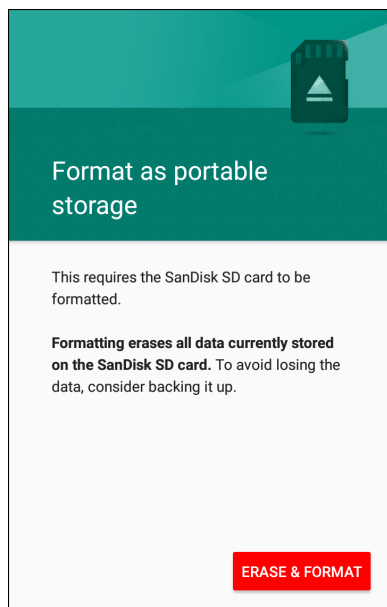
1. Touch **SD card**.
2. Touch  > **Storage settings**.

Figure 81 SD Card Settings Screen



3. Touch **Format**.

Figure 82 Format Screen



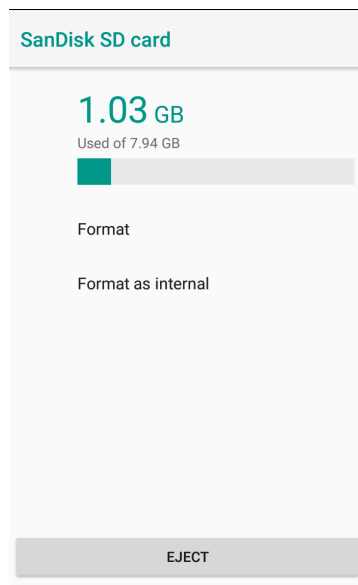
4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.

Formatting as Internal Memory

You can format a microSD card as internal memory to increase the actual amount of the device's internal memory. Once formatted, the microSD card can only be read by this device. To format an installed microSD card as internal memory:

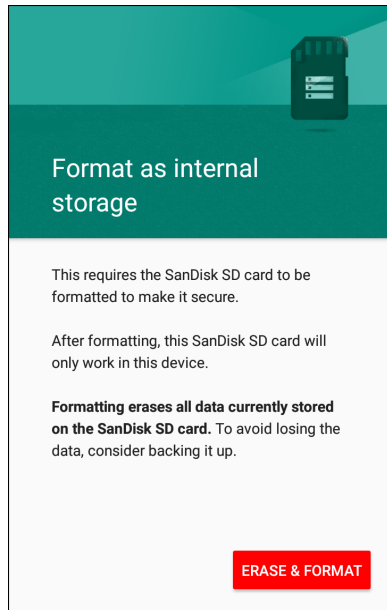
1. Touch **SD card**.
2. Touch **:** > **Storage settings**.

Figure 83 SD Card Settings Screen



3. Touch **Format as internal**.

Figure 84 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.

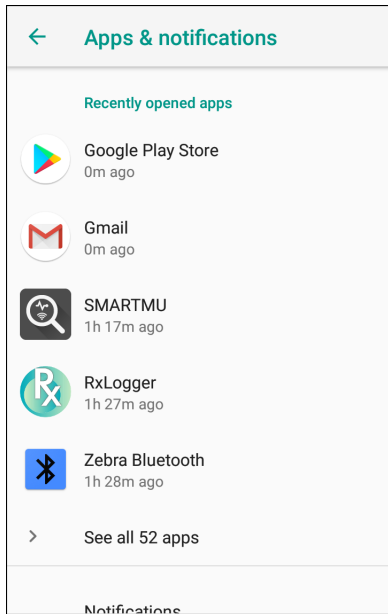
App Management

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 .

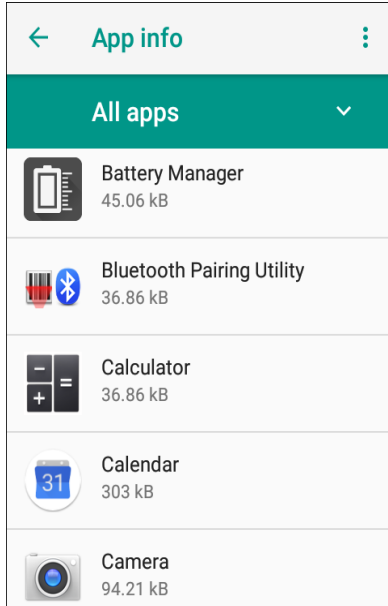
2. Touch **Apps & notifications**.

Figure 85 Apps & Notifications Screen



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

Figure 86 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 on page 124](#) 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.
- **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 microSD card or Internal storage in the Download directory. Use the Downloads app to view, open, or delete downloaded items.



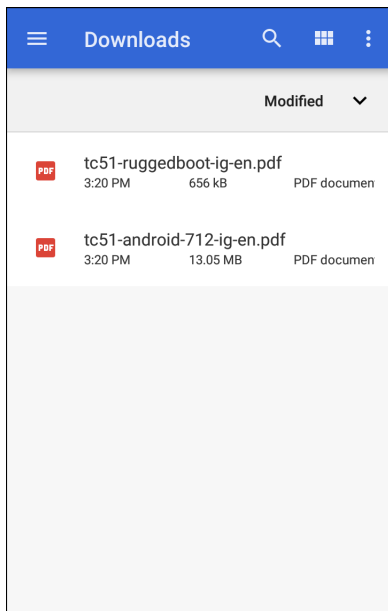

1. Swipe the screen up and touch .
2. Touch  > **Downloads**.

Figure 87 Files - Downloads Screen



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

Maintenance and Troubleshooting

Introduction

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

Maintaining the Device

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

- In order to avoid scratching the screen, use plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the device screen.
- The touch-sensitive screen of the device is glass. Do not drop the device or subject it to strong impact.
- Protect the device from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store the device in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the device. If the surface of the device screen becomes soiled, clean it with a soft cloth moistened with an approved cleanser.

Cleaning Instructions



CAUTION: Always wear eye protection.

Read warning label on alcohol product before using.

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



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

Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, bleach/sodium hypochlorite¹ (see important note below), hydrogen peroxide, ammonium chloride or mild dish soap.



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

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

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

Harmful Ingredients

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

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

Device Cleaning Instructions

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



NOTE: For thorough cleaning, it is recommended to first remove all accessory attachments, if applicable.

Special Cleaning Notes

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

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



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

Cleaning Materials Required

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

Cleaning Frequency

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

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

Cleaning the Device

Housing

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

Display

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

Camera and Exit Window

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

Troubleshooting

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

Table 7 *Troubleshooting the Device*

Problem	Cause	Solution
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	Device disconnected from host computer during communication.	Reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software was incorrectly installed or configured.	Perform setup.
During data communication over Wi-Fi, no data transmitted, or transmitted data was incomplete.	Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
	You moved out of range of an access point.	Move closer to an access point.
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	Bluetooth radio is not on.	Turn on the Bluetooth radio.
	You moved out of range of another Bluetooth device.	Move within 10 meters (32.8 feet) of the other device.
No sound.	Volume setting is low or turned off.	Adjust the volume.
Device shuts off.	Device is inactive.	The display turns off after a period of inactivity. Set this period to 15 seconds, 30 seconds, 1, 2, 5, 10 or 30 minutes.
Tapping the window buttons or icons does not activate the corresponding feature.	The device is not responding.	Reset the device.
A message appears stating that the device memory is full.	Too many files stored on the device.	Delete unused memos and records. If necessary, save these records on the host computer (or use an SD card for additional memory).
	Too many applications installed on the device.	Remove user-installed applications on the device to recover memory. Select ⚙️ > Storage > FREE UP SPACE > REVIEW RECENT ITEMS . Select the unused program(s) and tap FREE UP .

Table 7 *Troubleshooting the Device (Continued)*

Problem	Cause	Solution
The device does not decode with reading barcode.	Scanning application is not loaded.	Load a scanning application on the device or enable DataWedge. See the system administrator.
	Unreadable barcode.	Ensure the symbol is not defaced.
	Distance between exit window and barcode is incorrect.	Place the device within proper scanning range.
	Device is not programmed for the barcode.	Program the device to accept the type of barcode being scanned. Refer to the EMDK or DataWedge application.
	Device is not programmed to generate a beep.	If the device does not beep on a good decode, set the application to generate a beep on good decode.
Device cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (32.8 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
Cannot unlock device.	User enters incorrect password.	If the user enters an incorrect password eight times, the user is requested to enter a code before trying again. If the user forgot the password, contact system administrator.

Technical Specifications

Introduction

This chapter provides technical specifications and decode distances for the CC600 and CC6000.

Technical Specifications

CC6000

Table 8 *CC6000 Technical Specifications*

Item	Description
Physical Characteristics	
Dimensions	Landscape: 10.9 in. x 7.9 in. x 1.4 in. 27.8 cm x 20.1 cm x 3.6 cm Portrait: 7.2 in. x 11.6 in. x 1.4 in. 18.3 cm x 29.6 cm x 3.6 cm
Weight	2.16 lbs./980g
Display	10.1 inch PCAP multi-touch
Active Screen Area	217 mm W x 136 mm H
Aspect Ratio	16:10
Resolution	1280x800 at 60 Hz
Keypad	Virtual
Connectivity	USB host: 2 Full Size USB 2.0 Type A ports for accessory USB OTG: 1 USB-C OTG Ethernet Gigabit compatible: RJ45 External Audio In: 3.5 mm connector
Audio	Audio Two microphones; two front firing speakers (2W total)
Expansion Capabilities	Micro SD card slot, supports class 2 to class 10 and UHS-1 SD cards
Power	Enterprise grade power supply: 5.4VDC/3A; 110/220V Support for integrated 802.3at Power-over-Ethernet (PoE)

Technical Specifications

Table 8 CC6000 Technical Specifications (Continued)

Item	Description
Performance Characteristics	
Display Brightness	300 nits
CPU	Qualcomm Snapdragon™ 660
OS	Android Oreo, Google GMS
Memory	RAM: 4GB Internal Storage: 32GB
User Environment	
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Management	
Management Tools	Integrates with industry standard Mobile Device Management (MDM) solutions to configure settings and provide remote software updates
Data Capture/Output	
Integrated Scanner	1D/2D Zebra SE4710 decoded scanner
Front Camera	5 MP
Video	1080p
Networks	
WLAN	Dual band 802.11 a/b/g/n/ac/d/h/r/k/w/i (2.4 GHz and 5.2 GHz support)
WPAN	Bluetooth 5.0; integrated antenna
Ethernet	Gigabit Ethernet on RJ45 interface, with activity LEDs
Peripherals and Accessories	
Accessories	Country specific AC line cord. Additional accessories can be integrated using USB and Bluetooth interface
Mounting Options	Integrated standard VESA mount; conforms to the VESA 100 mm x 100 mm mounting standard for attachment of third party, off-the-shelf mounting solutions; four (4) M4 x 8 mm max insert distance
2D Imager Engine (SE4710) Specifications	
Field of View	Horizontal - 42.0° Vertical - 28.0°
Image Resolution	1280 horizontal X 800 vertical pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 1,000 ft. candles (10,764 lux)
Focal Distance	From front of engine: 19.4 cm (7.6 in.)
Aiming Element	610 nm amber LED dot
Illumination System	Red LED

CC600

Table 9 CC600 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions	6.6 in. x 4.6 in. x 1.4 in. 16.9 cm x 11.6 cm x 3.5 cm
Weight	0.70 lbs./320 g
Display	5.0 inch PCAP multi-touch
Active Screen Area	110 mm W x 62 mm H
Aspect Ratio	16:10
Resolution	1280x720 at 60 Hz
Keypad	Virtual
Connectivity	USB OTG: 1 USB-C OTG Ethernet Gigabit compatible: RJ45
Audio	Two microphones, one front firing speaker (2W total)
Expansion Capabilities	Micro SD card slot, supports class 2 to class 10 and UHS-1 SD cards
Power	Enterprise grade power supply: 5.4VDC/3A; 110/220V Support for integrated 802.3at Power-over-Ethernet (PoE)
Performance Characteristics	
Display Brightness	480 nits
CPU	Qualcomm Snapdragon™ 660
OS	Android Oreo, Google GMS
Memory	RAM: 4GB Internal Storage: 32GB
User Environment	
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Management	
Management Tools	Integrates with industry standard Mobile Device Management (MDM) solutions to configure settings and provide remote software updates
Data Capture/Output	
Integrated Scanner	1D/2D Zebra SE2100 scanner
Networks	
WLAN	Dual band 802.11 a/b/g/n/ac/d/h/r/k/w/i (2.4 GHz and 5.2 GHz support)
WPAN	Bluetooth 5.0; integrated antenna
Ethernet	Gigabit Ethernet on RJ45 interface, with activity LEDs

Technical Specifications

Table 9 *CC600 Technical Specifications (Continued)*

Item	Description
Peripherals and Accessories	
Accessories	Additional accessories can be integrated using USB and Bluetooth interface
Mounting Options	Integrated standard VESA mount; conforms to the VESA 75 mm x 75 mm mounting standard for attachment of third party, off-the-shelf mounting solutions; four (4) M4 x 8 mm max insert distance
2D Imager Engine (SE2100) Specifications	
Field of View	Horizontal - 41.5° Vertical - 31.7°
Image Resolution	640 horizontal x 480 vertical pixels
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Sunlight: 1,000 ft. candles (10,764 lux)
Focal Distance	From front of engine: 10.7 cm (4.2 inches)
Aiming Element	None
Illumination System	Ultra white LED

Table 10 *Data Capture Supported Symbologies*

Item	Description
1D Barcodes	Code 128, EAN-8, EAN-13, GS1 DataBar Expanded, GS1 128, GS1 DataBar Coupon, UPCA, Interleaved 2 of 5, UPC Coupon Code
2D Barcodes	PDF-417, QR Code, Digimarc, DotCode (CC6000 only)

Decode Distances

CC6000 - SE4710 Scan Engine

Table 11 lists the typical distances for selected barcode densities when scanning with the CC6000. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

Table 11 CC6000 - SE4710 Decode Ranges

Barcode Type	Near Distance	Far Distance
	Typical	Typical
4 mil Code 39	3.3 in / 8.4 cm	8.8 in / 22.4 cm
5 mil Code 128	2.8 in / 7.1 cm	8.2 in / 20.8 cm
5 mil Code 39	2.0 in / 5.08 cm	13.5 in / 34.3 cm
5mil PDF417	3.1 in / 7.9 cm	7.5 in / 19.0 cm
10 mil Data Matrix	2.9 in / 7.4 cm	10.1 in / 25.7 cm
100% UPCA	1.8 in / 4.6 cm*	24.0 in / 60.9 cm
20.0mil Code 39	2.0 in / 5.08 cm*	26 in / 66.0 cm

*Limited by width of barcode in field of view.

Note: Photographic quality barcode at 15° tilt pitch angle under 30 fcd ambient illumination.

CC600 - SE2100 Scan Engine

Table 12 lists the typical distances for selected barcode densities when scanning with the CC600. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

Table 12 *CC600 - SE2100 Decode Ranges*

Barcode Type	Near Distance	Far Distance
	Typical	Typical
5 mil Code 128	2.0 in / 51mm	4.8 in / 122 mm
5 mil Code 39	1.7 in / 43 mm	5.8 in / 147 mm
6.6 mil PDF417	1.6 in / 41 mm	4.9 in / 124 mm
10 mil Data Matrix	1.2 in / 30 mm	4.9 in / 124 mm
100% UPCA	2.0 in / 51 mm	10.6 in / 269 mm
20.0 mil Code 39	2.1 in / 53 mm*	13.6 in / 345 mm
10.0 mil QR Code	1.1 in / 28 mm	5.2 in / 132 mm
*Limited by width of barcode in field of view.		
Note: Photographic quality barcode at 15° tilt pitch angle under 30 fcd ambient illumination.		

Index

A

advanced data formatting rules	93
approved cleanser	138
approved cleanser active ingredients	138
apps	
RxLogger	44
RxLogger Utility	50

B

barcode input	70
enabled	70

C

cleaning	138, 139
camera and exit window	140
display	140
frequency	139
housing	140
instructions	138
materials	139
cleaning instructions	139

D

data capture plus	68
datawedge	
advanced data formatting rules	93
APIs	105
associating applications	66
auto import	104
auto switch to default on event	70
barcode input	70
basic scanning	61
configuration and profile file management	104
configuring ADF plug-in	93
creating a new profile	65
data capture plus	68
decoders	71
disabling	65

enterprise folder	104
exporting a configuration file	103
importing a configuration file	102
input plugins	63
intent output	87
intent overview	88
introduction	61
IP output	89
keep enabled on suspend	85
keystroke output	86
options menu	65
output plug-ins	63
plug-ins	63
process plug-ins	63
profile configuration	66
profile context menu	64
profile0	62
profiles	62
profiles screen	64
programming notes	105
reader params	81
reporting	105
scan params	84
scanner selection	70
settings	102
UDI params	85
UPC EAN params	79
voice input	85
decode ranges	147, 148
decoder params	
Codabar	74
Code 11	74
Code 128	74
Code 39	75
Code 93	76
Composite AB	76
decode lengths	79
Discrete 2 of 5	76
GS1 DataBar Limited	76
HAN XIN	77
Interleaved 2 of 5	77
Matrix 2 of 5	77

MSI	77	configuration file	49
Trioptic 39	78	disable logging	49
UK Postal	78	enable logging	49
UPCA	78	extract log files	49
UPCE0	78	Utility	50
UPCE1	78		
US Planet	79		
decoders	71		
disconnect host computer	57		
F		S	
feature descriptions		scan params	84
touch screen	20	settings	
file transfer	57	datawedge	102
		software version	12, 13
		symbolgies	146
G		T	
Google		touch screen	20
account setup	28	transferring files using USB	56
		troubleshooting	141
H		U	
harmful ingredients	139	UDI params	85
		UPC EAN params	79
		USB	56
M		V	
maintenance	138	voice input	85
approved cleanser active ingredients	138		
clean camera and exit window	140	W	
clean display	140	Wi-Fi direct	39
clean housing	140		
cleaning frequency	139		
cleaning instructions	138		
cleaning materials required	139		
device cleaning instructions	139		
harmful ingredients	139		
maintaining the device	138		
special cleaning notes	139		
mounting the device	21		
N			
notational conventions	14		
P			
photo transfer	57		
R			
reader params	81		
RxLogger	44		
configuration	44		

