

# CC600 and CC6000

Customer Concierge



**ZEBRA**

## **Product Reference Guide**

2024/05/31

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. ©2024 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: [zebra.com/informationpolicy](https://zebra.com/informationpolicy).

COPYRIGHTS: [zebra.com/copyright](https://zebra.com/copyright).

PATENTS: [ip.zebra.com](https://ip.zebra.com).

WARRANTY: [zebra.com/warranty](https://zebra.com/warranty).

END USER LICENSE AGREEMENT: [zebra.com/eula](https://zebra.com/eula).

## Terms of Use

### Proprietary Statement

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

### Product Improvements

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

### Liability Disclaimer

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

### Limitation of Liability

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

# Contents

<b>About this Guide.....</b>	<b>10</b>
Configurations.....	10
Notational Conventions.....	11
Icon Conventions.....	11
Service Information.....	12
Determining Software Versions.....	12
Determining the Serial Number.....	12
 <b>Getting Started.....</b>	 <b>13</b>
Unpacking the Device.....	13
CC6000 Features.....	14
CC600 Features.....	17
Mounting Brackets.....	20
Measurements.....	24
Setting Up the Device.....	26
Installing a microSD Card (Optional).....	26
Mounting the Device.....	27
Resetting the Device.....	31
 <b>Using the Device.....</b>	 <b>32</b>
Home Screen.....	32
Status Bar.....	33
Managing Notifications.....	36
Opening the Quick Access Panel.....	37
Editing the Quick Access Tiles.....	40

Unlocking the Screen.....	40
USB Communication.....	41
Transferring Files.....	41
Transferring Photos.....	41
Disconnecting from the Host Computer.....	41
<b>Settings.....</b>	<b>42</b>
Accessing Settings.....	42
Display Settings.....	42
Setting the Screen Brightness Manually.....	42
Setting Night Light.....	42
Setting Screen Timeout.....	43
Setting Lock Screen Notifications.....	43
Setting Font Size.....	44
Setting Display Size.....	44
Setting the Date and Time.....	44
General Sound Setting.....	45
Sound Options.....	45
Remapping a Button.....	45
Remappable Keys.....	46
Setting Screen Lock.....	47
Setting Screen Lock Using PIN.....	47
Setting Screen Lock Using Password.....	47
Setting Screen Lock Using Pattern.....	48
Keyboards.....	48
Keyboard Configuration.....	48
Using the Android and Gboard Keyboards.....	49
Enterprise Keyboard.....	49
Language Usage.....	50
Changing the Language Setting.....	50
Adding Words to the Dictionary.....	50
Notifications.....	51
Setting App Notifications.....	51

<b>Applications.....</b>	<b>54</b>
Installed Applications.....	54
Accessing Apps.....	55
Switching Between Recent Apps.....	55
Camera.....	56
Taking Photos.....	56
Recording Videos.....	57
Photo Settings.....	59
Video Settings.....	60
DWDemo.....	60
DWDemo Icons.....	60
Selecting a Scanner.....	61
PTT Express Voice Client.....	61
PTT Express User Interface.....	62
PTT Audible Indicators.....	62
PTT Notification Icons.....	63
Enabling PTT Communication.....	63
Selecting a Talk Group.....	63
PTT Communication.....	63
Disabling PTT Communication.....	64
Rxlogger.....	64
RxLogger Configuration.....	64
Configuration File.....	65
Enabling Logging.....	65
Disabling Logging.....	65
Extracting Log Files.....	65
Backing Up Data.....	65
RxLogger Utility.....	65
<b>Data Capture.....</b>	<b>67</b>
Imaging.....	67
Linear Imager.....	67
Operational Modes.....	68
Scanning Considerations.....	68

Scanning with Internal Imager (SE2100).....	69
Scanning with Internal Imager (SE4710).....	70
Scanning with the RS507/RS507X Hands-Free Imager.....	72
Scanning with the RS6000 Bluetooth Ring Scanner.....	75
Scanning with the RS5100 Ring Scanner.....	77
Scanning with the DS3678 Bluetooth Scanner.....	79
Scanning with the LI3678 Linear Imager.....	81
Scanning with the DS2278 Digital Scanner.....	82
Scanning with the DS8178 Digital Scanner.....	83
Pairing a Bluetooth Ring Scanner.....	84
Pairing in SSI Mode Using Near Field Communication.....	85
Pairing in HID Mode Using Near Field Communication.....	85
Pairing Using Simple Serial Interface.....	86
Pairing Using Bluetooth Human Interface Device.....	87
Pairing a Bluetooth Scanner.....	88
Pairing Using Simple Serial Interface.....	88
Pairing Using Bluetooth Human Interface Device.....	89
DataWedge.....	90
Enabling DataWedge.....	90
Disabling DataWedge.....	90
Supported Decoders.....	91
SE2100 Internal Imager Supported Decoders.....	91
SE4850-ER Internal Imager Supported Decoders.....	91
RS507/RS507x Supported Decoders.....	92
RS6000 Supported Decoders.....	93
RS5100 Supported Decoders.....	94
DS2278 Supported Decoders.....	95
DS3678 Supported Decoders.....	95
LI3678 Supported Decoders.....	96
DS8178 Supported Decoders.....	97
<b>Wireless.....</b>	<b>99</b>
Wireless Local Area Networks.....	99
Connecting to a Wi-Fi Network.....	100

Removing a Wi-Fi Network.....	101
WLAN Configuration.....	101
Configuring a Secure Wi-Fi Network.....	101
Manually Adding A Wi-Fi Network.....	102
Configuring for a Proxy Server.....	104
Configuring the Device to Use a Static IP Address.....	104
Wi-Fi Preferences.....	105
Additional Wi-Fi Settings.....	105
Wi-Fi Direct.....	106
Bluetooth.....	106
Adaptive Frequency Hopping.....	107
Security.....	107
Bluetooth Profiles.....	108
Bluetooth Power States.....	109
Bluetooth Radio Power.....	109
Discovering Bluetooth Device(s).....	110
Changing the Bluetooth Name.....	110
Connecting to a Bluetooth Device.....	110
Selecting Profiles on the Bluetooth Device.....	111
Unpairing a Bluetooth Device.....	111
Cast.....	111
Near Field Communications.....	111
Reading NFC Cards.....	112
Sharing Information Using NFC.....	112
Enterprise NFC Settings.....	113
<b>Accessories.....</b>	<b>115</b>
Device Accessories.....	115
Headset (CC6000 Only).....	116
USB cable.....	116
<b>Application Deployment.....</b>	<b>117</b>
Android Security.....	117

Secure Certificates.....	117
Installing a Secure Certificate.....	117
Configuring Credential Storage Settings.....	118
Android Development Tools.....	118
Android Development Workstation.....	118
Enabling Developer Options.....	119
EMDK for Android.....	119
StageNow for Android.....	119
GMS Restricted.....	120
ADB USB Setup.....	120
Enabling USB Debugging.....	120
Entering Android Recovery Manually.....	121
Application Installation Methods.....	121
Installing Applications Using the USB Connection.....	121
Installing Applications Using the Android Debug Bridge.....	122
Installing Applications Using Wireless ADB.....	122
Installing Applications Using a microSD Card.....	124
Uninstalling an Application.....	124
Android System Update.....	125
Performing a System Update Using microSD Card.....	125
Performing a System Update Using ADB.....	125
Verifying System Update Installation.....	126
Android Enterprise Reset.....	126
Performing an Enterprise Reset From Device Settings.....	126
Performing an Enterprise Reset Using microSD Card.....	127
Performing an Enterprise Reset Using ADB.....	127
Android Factory Reset.....	128
Performing a Factory Reset Using microSD Card.....	128
Performing a Factory Reset Using ADB.....	129
Android Storage.....	130
Random Access Memory.....	130
Internal Storage.....	131
External Storage.....	131
Enterprise Folder.....	132

Managing Apps.....	132
App Details.....	133
Managing Downloads.....	133
<b>Maintenance and Troubleshooting.....</b>	<b>134</b>
Maintaining the Device.....	134
Cleaning Instructions.....	134
Approved Cleanser Active Ingredients.....	135
Harmful Ingredients.....	135
Device Cleaning Instructions.....	135
Special Cleaning Notes.....	135
Cleaning Materials Required.....	135
Cleaning Frequency.....	136
Cleaning the Device.....	136
Housing.....	136
Display.....	136
Camera and Exit Window.....	136
Troubleshooting the Device.....	137
<b>Technical Specifications.....</b>	<b>139</b>
Data Capture Supported Symbologies.....	139
CC6000 - SE4710 Scan Engine.....	139
CC600 - SE2100 Scan Engine.....	140

# About this Guide

This guide provides information about using the CC600 and CC6000 Customer Concierge interactive kiosk and accessories. Some screens shown in this guide may differ from the actual screens shown on the device.

This guide includes Android operating system (OS) 11 and above. Android 11 is the baseline, and updated OS releases are indicated in the content where applicable.

## Configurations

This guide covers all the CC600 and CC6000 configurations.

**Table 1** CC600 Device Configurations

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

**Table 2** CC6000 Device Configurations

Configuration	Description	Orientation	Front Camera	Scan Engine	Operating System
CC6000-10-3200LCWW	10 inch, 32 GB, Imager, Worldwide Configuration	Landscape	No	SE4710	Android
CC6000-10-3200PCWW	10 inch, 32 GB, Imager, Worldwide Configuration	Portrait	Yes	SE4710	Android
CC6000-10-3200LCNA	10 inch, 32 GB, Imager, North America Configuration	Landscape	Yes	SE4710	Android

**Table 2** CC6000 Device Configurations (Continued)

Configuration	Description	Orientation	Front Camera	Scan Engine	Operating System
CC6000-10-3200PCNA	10 inch, 32 GB, Imager, North America Configuration	Portrait	Yes	SE4710	Android
CC6000-10-3200LNNA	10 inch, 32 GB, Imager, North America Configuration	Landscape	No	SE4710	Android

## Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

## Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.



**NOTE:** The text here indicates information that is supplemental for the user to know and that is not required to complete a task.



**IMPORTANT:** The text here indicates information that is important for the user to know.



**CAUTION:** If the precaution is not heeded, the user could receive a minor or moderate injury.



**WARNING:** If danger is not avoided, the user CAN be seriously injured or killed.



**DANGER:** If danger is not avoided, the user WILL be seriously injured or killed.

## Service Information

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

When contacting support, please have the following information available:

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


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

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

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


## Determining Software Versions

Before contacting Customer Support, determine the current software version on your device.

1. Swipe down from the Status bar with two fingers to open the Quick Access panel, and then touch .
2. Touch **About phone**.
3. Scroll to view the following information:
  - Software components
  - Legal information
  - Model & hardware
  - Android version
  - Build number

## Determining the Serial Number

Before contacting Customer Support, determine the serial number of your device.

1. Swipe down from the Status bar with two fingers to open the Quick Access panel, and then touch .
2. Touch **About phone**.
3. Touch **Model & hardware**.

# Getting Started

This section provides information to get the device up and running for the first time.

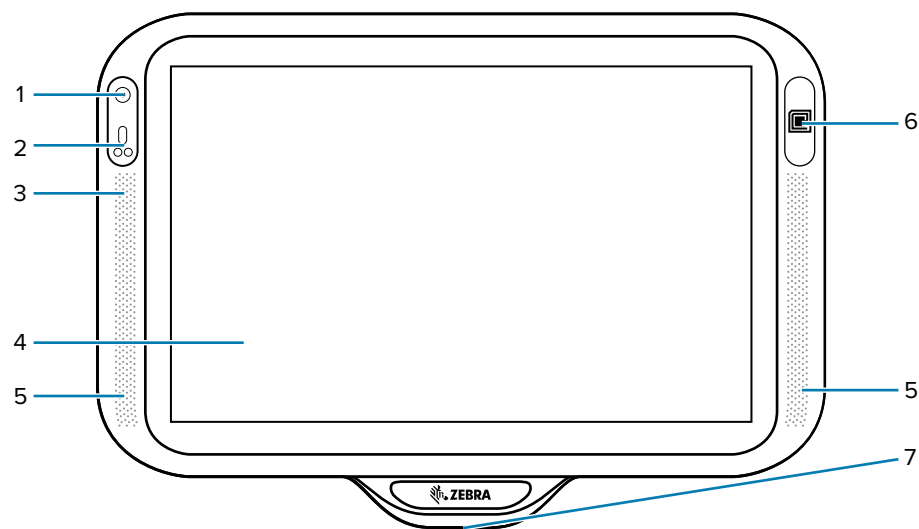
## Unpacking the Device



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

# CC6000 Features

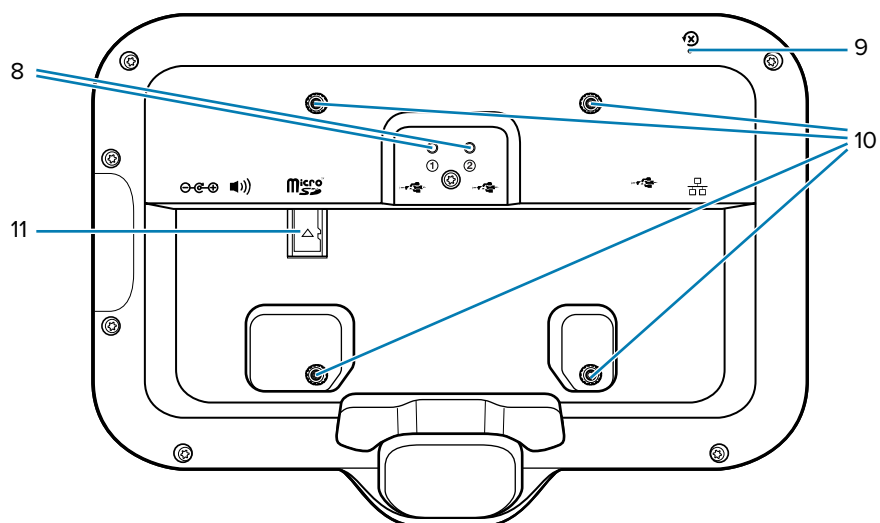
Although the orientations differ, the features on the CC6000 landscape and portrait devices are the same.

Figure 1 CC6000 Front View



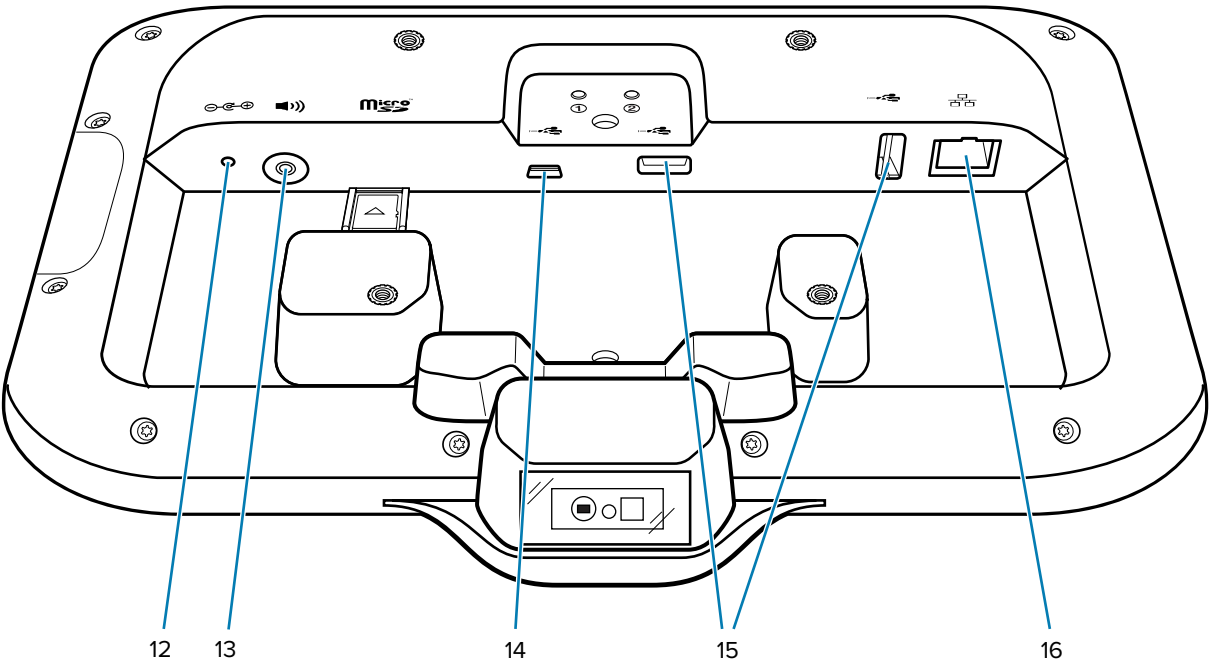
Number	Item	Function
1	Front-facing camera	Captures still photos and videos.  <b>NOTE:</b> Select CC6000 devices only.
2	Proximity sensor	Identifies the proximity of a user for turning up the display.
3	Microphone	Use for communications in Speakerphone mode.
4	Touch screen and display	Displays all information needed to operate the device.
5	Speaker	Provides audio output for video and music playback. Provides audio in speaker-phone mode.
6	NFC antenna	Reads NFC tags. (CC6000 Only)
7	Exit window (scanner)	Provides data capture using the imager and reads a barcode.  <b>NOTE:</b> To read a barcode, a scan-enabled app is required on the device.

**Figure 2** CC6000 Back View



Number	Item	Function
8	Volume up/down button	Increase and decrease audio volume (programmable).
9	Reset button	Press and hold to reset the device. See <a href="#">Resetting the Device</a> on page 31 for more information.
10	Mounting bracket screw holders	Use for mounting the device to a wall or other flat surface. See <a href="#">Mounting the Device</a> on page 27.
11	Micro SD card slot	Installs a micro secure digital (SD) card.

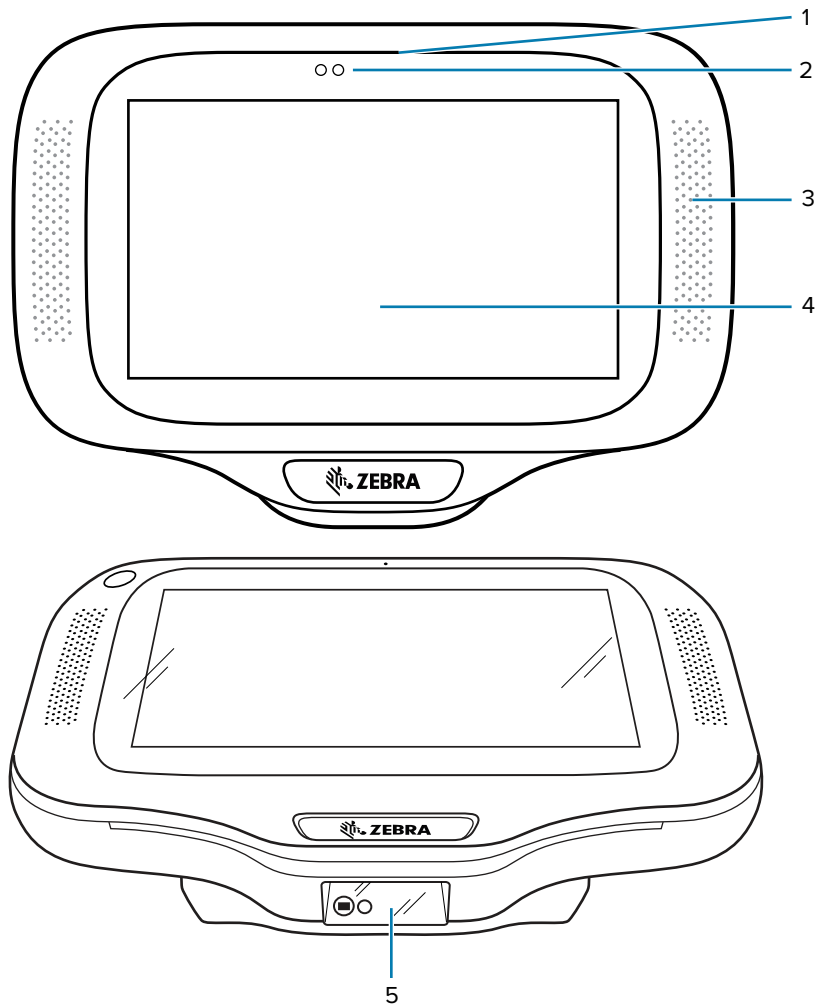
**Figure 3** CC6000 Power and Cable Ports




Number	Item	Function
12	Power port	Connects the power supply.
13	Audio port	For audio output to a headset.
14	USB C port (used for external display or OTG)	Designated for USB-C port utilization.
15	USB A port	Designated for USB-A port utilization.
16	External with POE	Designated for the integrated Power-over-Ethernet (PoE).

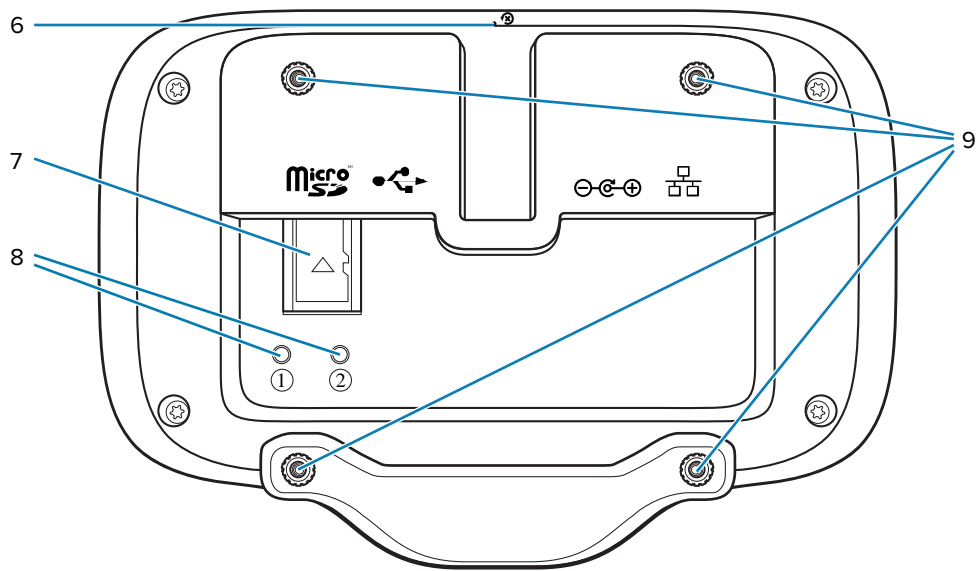
## CC600 Features

**Figure 4** CC600 Front View



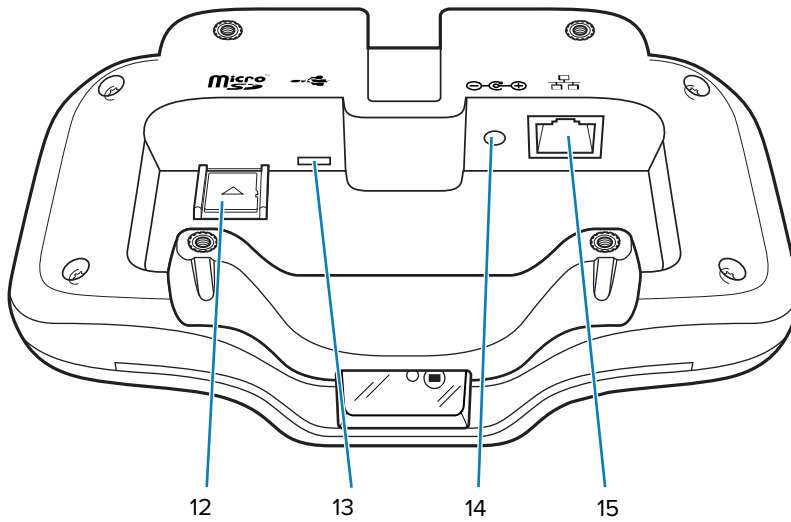
Number	Item	Function
1	Microphone	Use for communications in Speakerphone mode.
2	Proximity sensor	Identifies the proximity of a user for turning up the display.
3	Speaker	Provides audio output for video and music playback. Provides audio in speaker-phone mode.
4	Touch screen and display	Displays all information needed to operate the device.
5	Exit window (scanner)	Provides data capture using the imager and reads a barcode.  <b>NOTE:</b> To read a barcode, a scan-enabled app is required on the device.

**Figure 5** CC600 Back View



Number	Item	Function
6	Reset button	Press and hold to reset the device. See <a href="#">Resetting the Device</a> on page 31 for more information.
7	Micro SD card slot	Installs a micro secure digital (SD) card.
8	Volume up/ down button	Increase and decrease audio volume (programmable).
9	Mounting bracket screw holders	Use for mounting the device to a wall or other flat surface. See <a href="#">Mounting the Device</a> on page 27.

**Figure 6** CC600 Power and Cable Ports



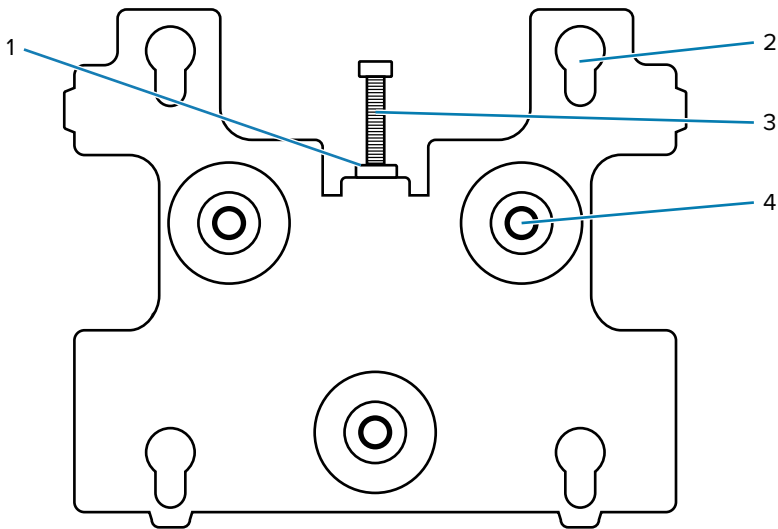
Number	Item	Function
12	Micro SD card slot	Installs a micro secure digital (SD) card.
13	USB C port (used for external display or OTG)	Designated for USB-C port utilization.
14	Power port	Connects the power supply.
15	External with POE	Designated for the integrated Power-over-Ethernet (PoE).

# Mounting Brackets

Each configuration of the device requires the appropriate mounting bracket to mount the device to a wall or other flat surface.

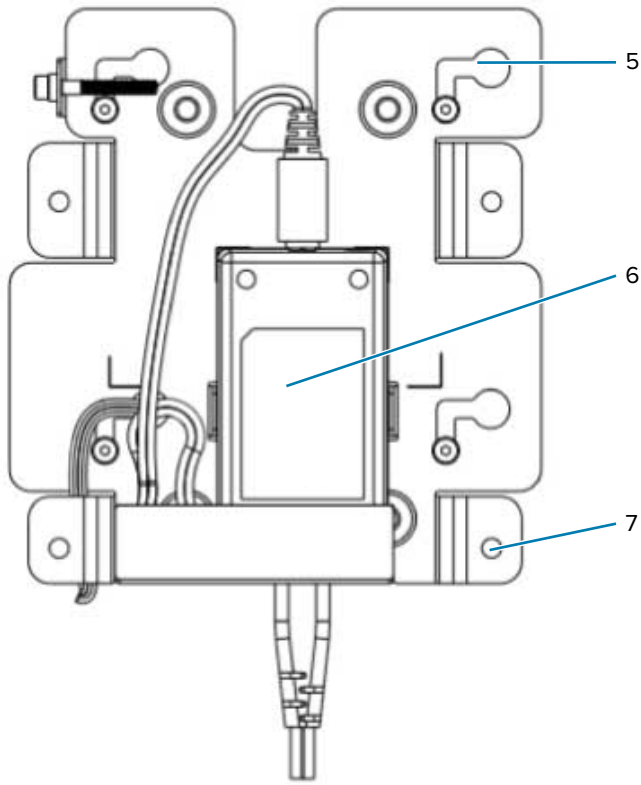
## Brackets

**Figure 7** CC600 Mounting Bracket



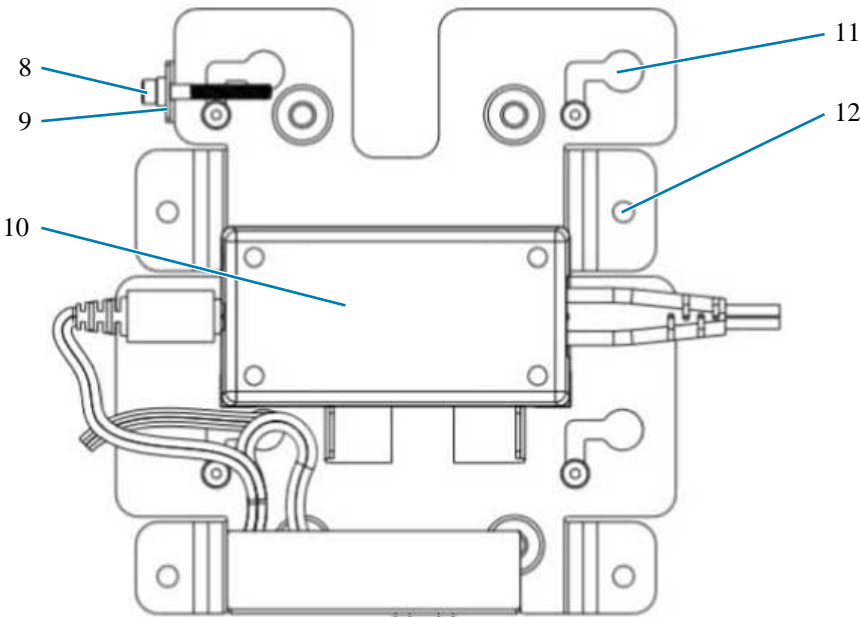
Number	Item
1	Securing screw hole
2	Shoulder screw hole (4)
3	Securing screw
4	Wall screw hole (3)

**Figure 8** CC6000 Mounting Bracket - Portrait Orientation



Number	Item
5	Shoulder screw hole (4)
6	Power supply
7	Wall screw hole (4)

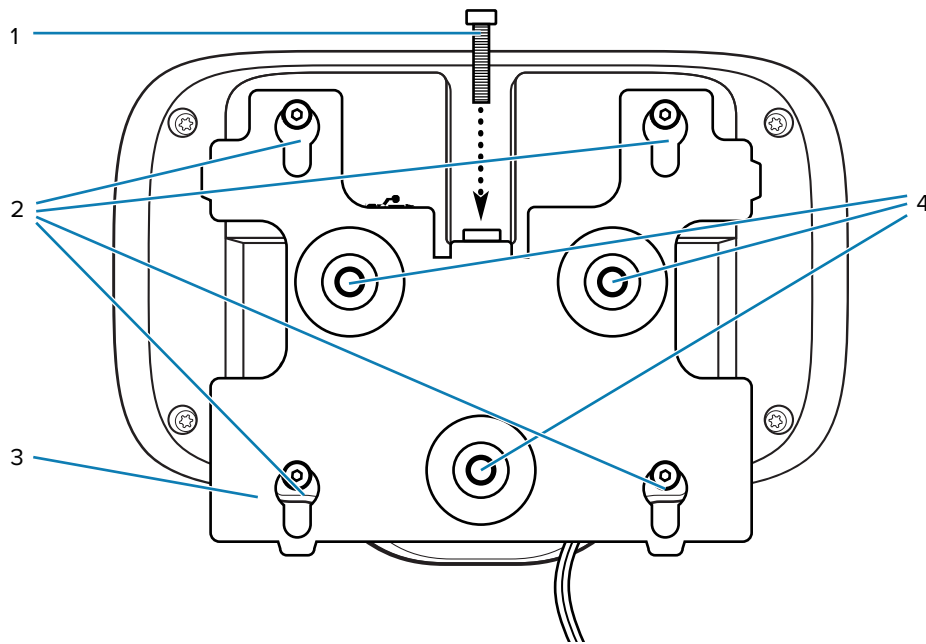
**Figure 9** CC6000 Mounting Bracket (KT-152098-03) - Landscape Orientation



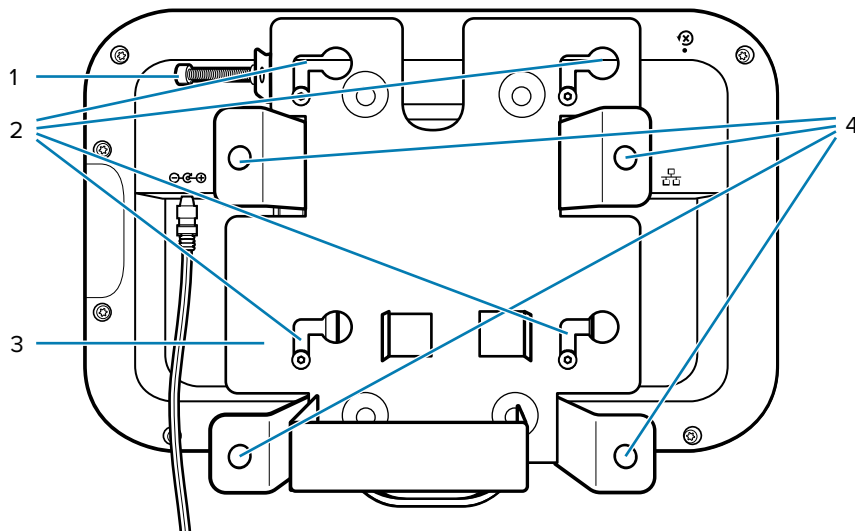
Number	Item
8	Securing screw
9	Securing screw hole
10	Power supply
11	Shoulder screw hole (4)
12	Wall screw hole (4)

## Device and Brackets

**Figure 10** CC600 Back With Bracket View



**Figure 11** CC6000 Back With Bracket View



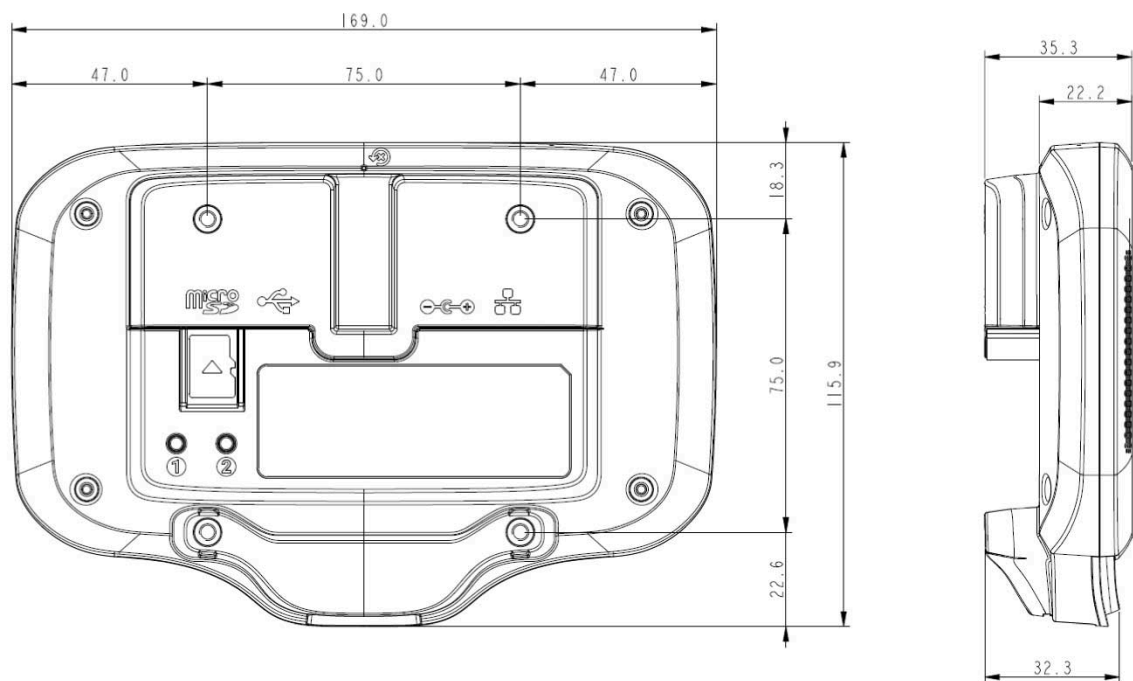
Number	Item
1	Mounting bracket locking screw
2	Mounting bracket screw holders
3	Mounting bracket
4	Wall mount screw holes

## Measurements

The device measurements are in millimeters.

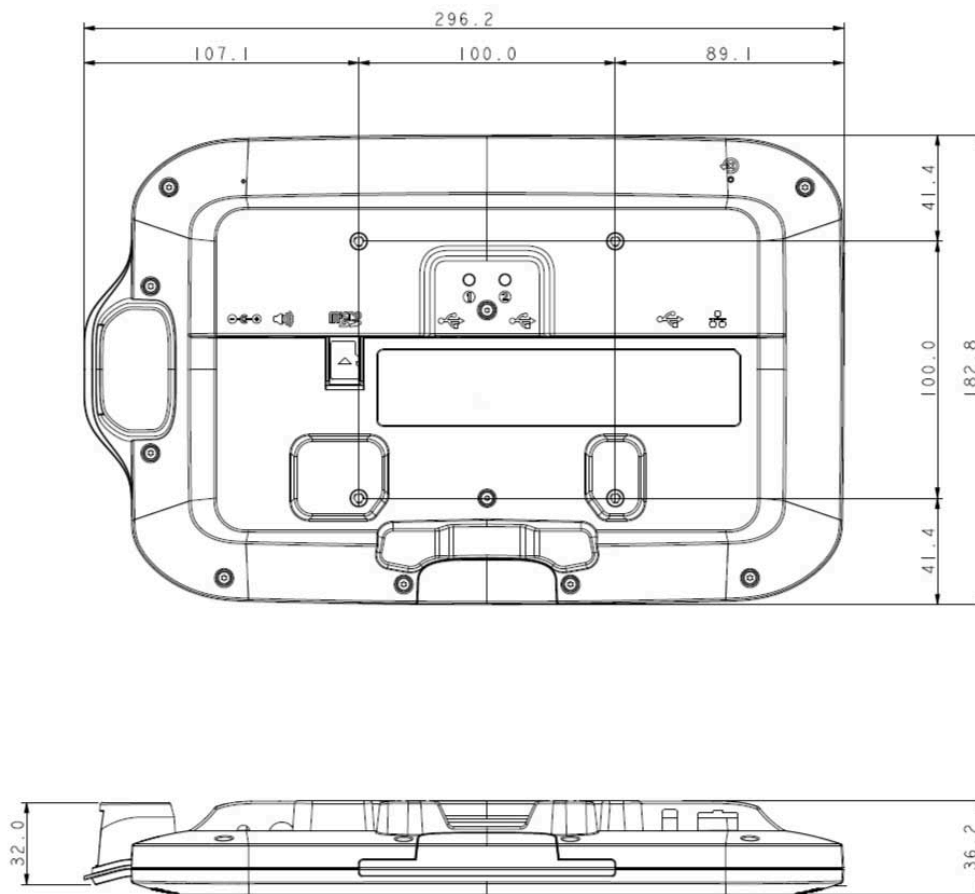
### CC600

**Figure 12** CC600 Measurements



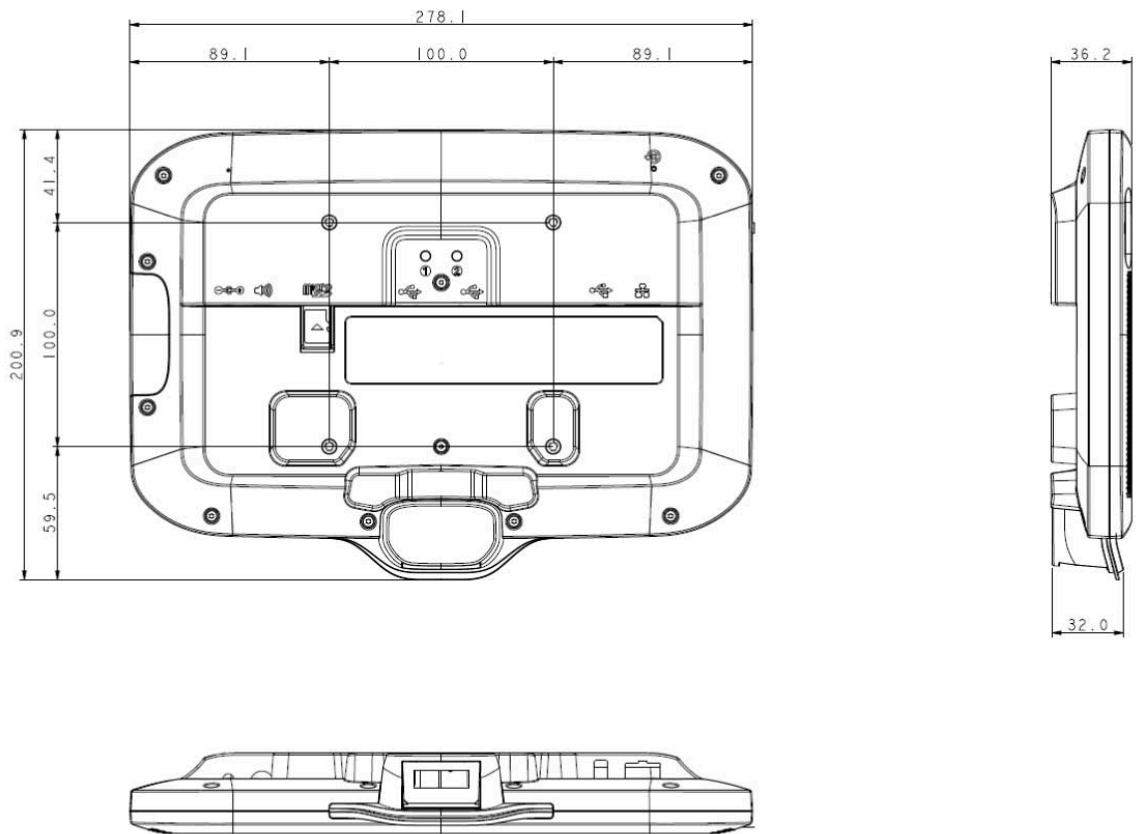
**CC6000 Portrait**

**Figure 13** CC6000 Portrait Measurements



## CC6000 Landscape

**Figure 14** CC6000 Landscape Measurements



## Setting Up the Device

Perform these procedures to start using the device for the first time.

1. Install a micro secure digital (SD) card (optional).
2. Connect the power supply to power on the device.
3. Configure the device.
4. Mount the device with the mounting bracket.
5. Set up a Google account.

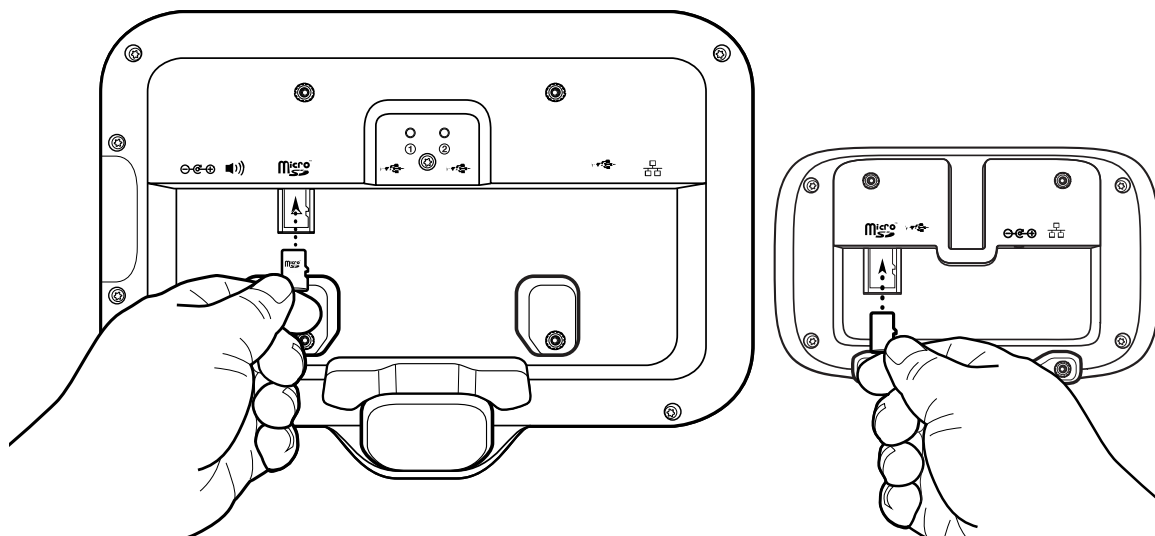
## Installing a microSD Card (Optional)

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.

1. Remove the device from the mounting bracket, if installed.
2. Slide the microSD card, connectors down, into the device.



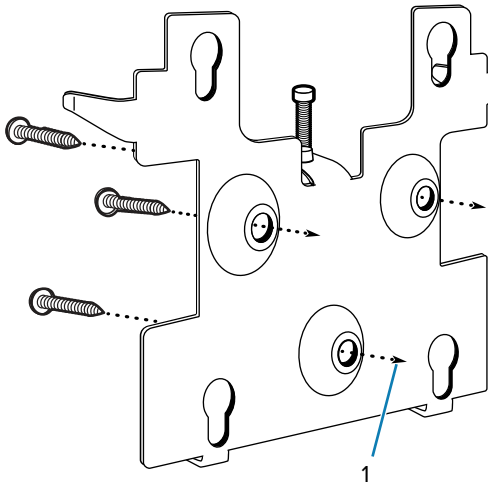
## Mounting the Device

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 5.8 mm (0.228 in.).

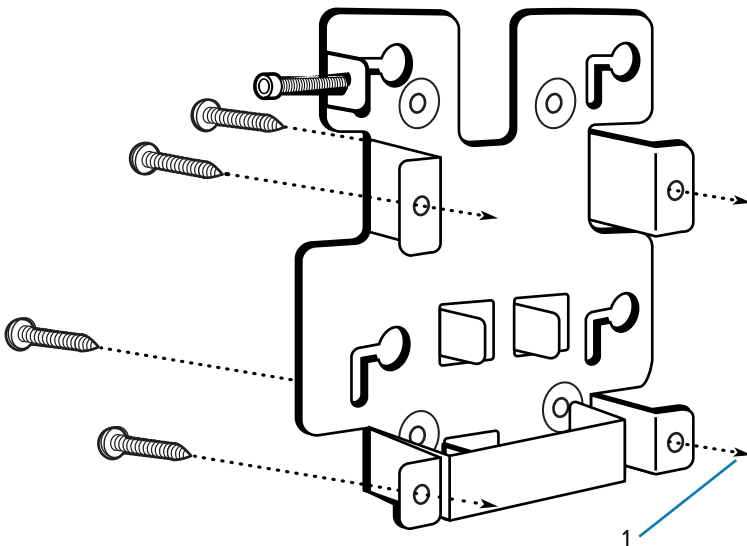
1. Determine the CC600 or CC6000 mounting location.

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 15** Attaching the CC600 Bracket To Wall



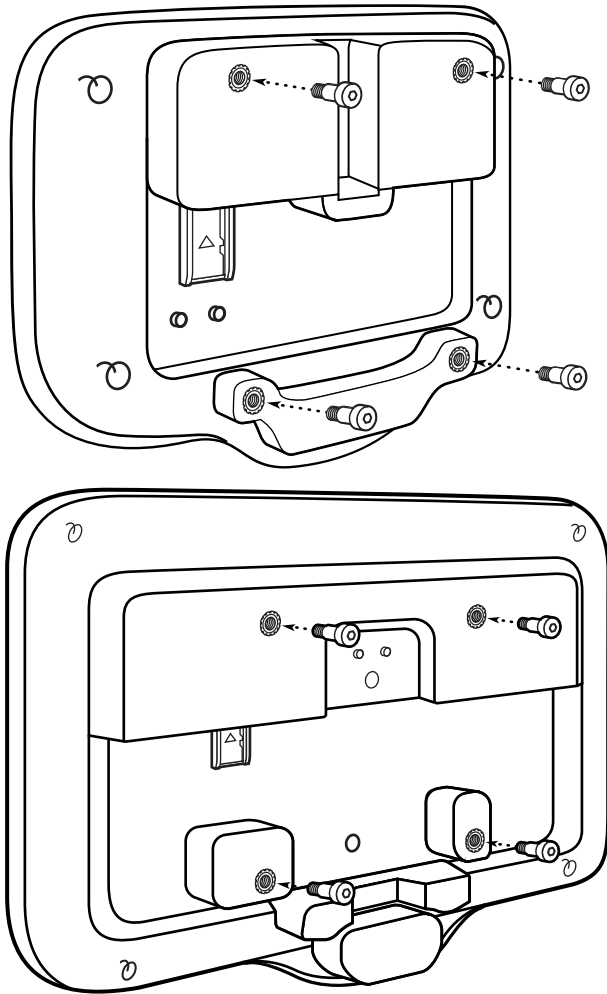
**Figure 16** Attaching the CC6000 Bracket To Wall



1	To wall
---	---------

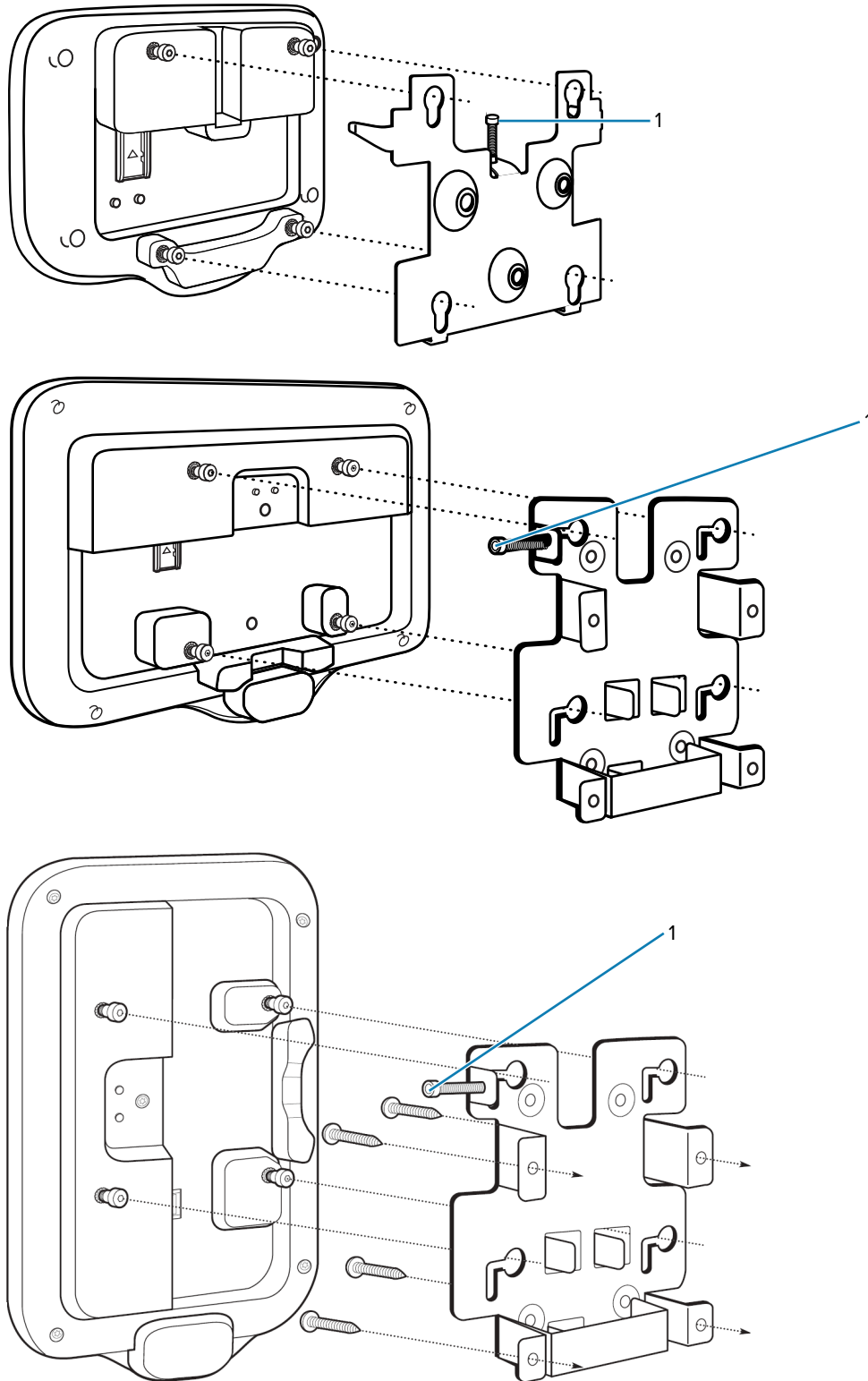
3. Insert the four shoulder screws, also provided, into the mounting holes in the back of the device.

**Figure 17** Inserting Shoulder Screws



4. Connect the power supply to the power port. Connect any additional cables into the appropriate ports shown in [Figure 3 CC6000 Power and Cable Ports](#) and [Figure 6 CC600 Power and Cable Ports](#).

5. Mount the device by placing the shoulder screws through the four keyholes on the mounting plate, and slide the device down to secure it in place.



1	To wall
---	---------

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.

## Resetting the Device

The device has a recessed reset button (see [Figure 5 CC600 Back View](#) and [Figure 2 CC6000 Back View](#)).

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

The device has a recovery console accessible via pressing 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 [Android Enterprise Reset](#) on page 126 for more information).
- Factory reset Full Factory reset (see [Android Factory Reset](#) on page 128 for more information).

The device recovery mode supports the following functions:

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

# Using the Device

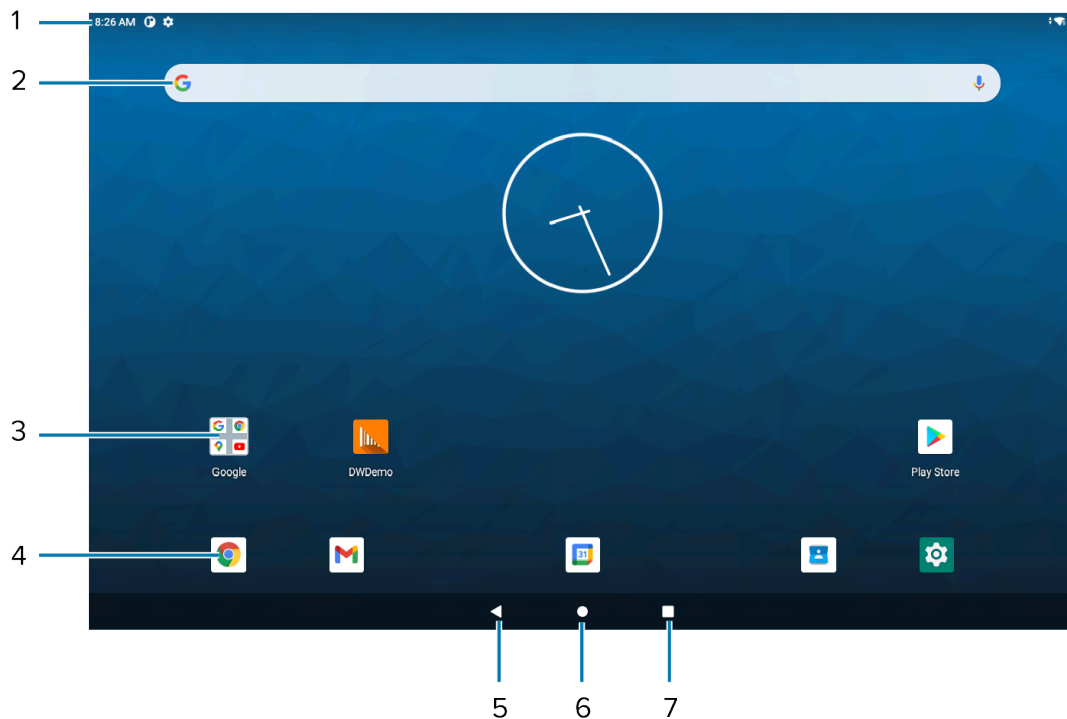
This section explains how to use the device.

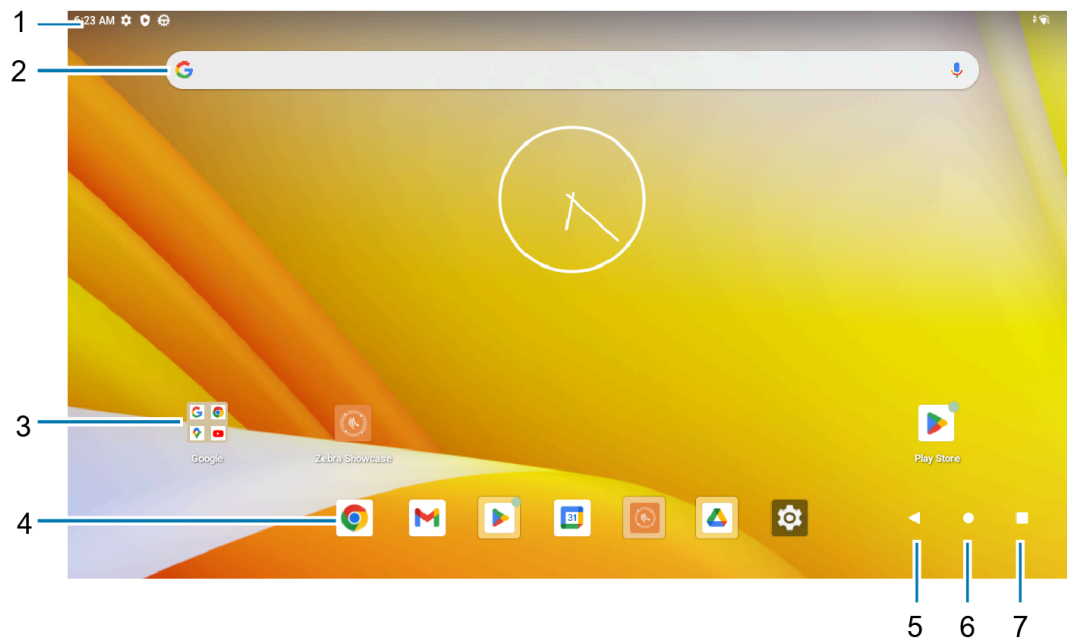
## Home Screen

Turn on the device to display the Home screen. Depending on how your system administrator configured your device, your Home screen may appear differently than the graphics in this section.

After the device goes into Sleep mode, the Home screen displays with the lock icon. Touch the screen and swipe up to unlock. The Home screen provides four additional screens to place widgets and shortcuts. Touch and hold on an icon, and then move it for the option to place the icon on one of the other screens. Swipe the Home screen left or right to view the additional screens.

**Figure 18** Android 11 Home Screen



**Figure 19** Android 13 Home Screen

1	Status bar	Displays the time, status icons (right side), and notification icons (left side).
2	Widgets	Launches stand-alone apps that run on the Home screen.
3	Shortcut icons	Opens apps installed on the device.
4	Folder	Contains apps.
5	Back	Displays the previous screen.
6	Home	Displays the home screen.
7	Recent	Displays recently used applications.

## Status Bar

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

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
















**Figure 20** Notifications and Status Icons

1	Notification icons
2	Status icons

## Notification Icons

Notification icons indicate app events and messages.











**Table 3** Notification Icons

Icon	Description
	More notifications are available for viewing.
	Data is synching.
	Indicates an upcoming event. AOSP devices only.
	Indicates an upcoming event. GMS devices only.
	A problem with sign-in or sync has occurred.
	The device is uploading data.
	Animated: the device is downloading data. Static: the download is complete.
	The device is connected to or disconnected from a virtual private network (VPN).
	Preparing internal storage by checking it for errors.
	USB debugging is enabled on the device.
	A wired headset with a boom module is connected to the device.
	PTT Express Voice client status.
	The RxLogger app is running.
	A Bluetooth scanner is connected to the device.
	A ring scanner is connected to the device in HID mode.

## Status Icons

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

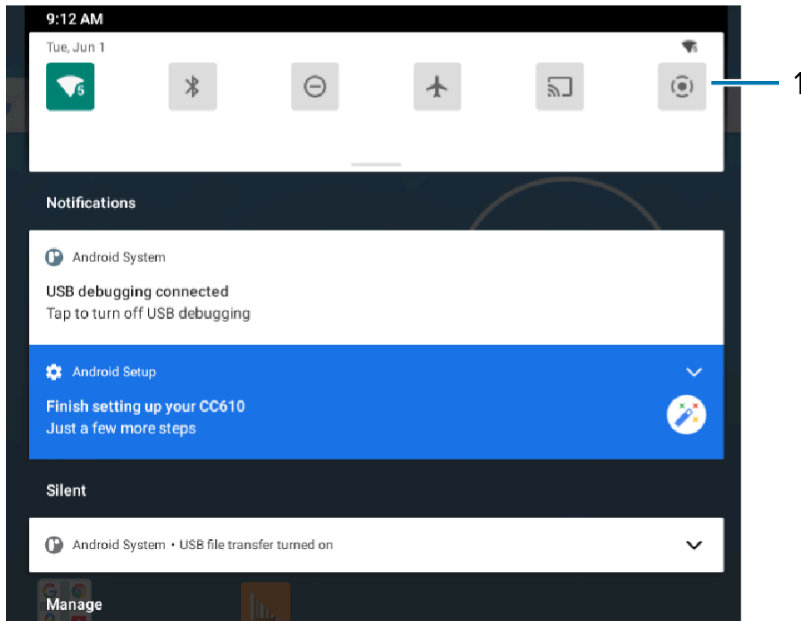
**Table 4** Status Icons

Icon	Description
	Alarm is active.
	All sounds except media and alarms are muted.
	Do Not Disturb mode active.
	Airplane Mode is active. All radios are turned off.
	Bluetooth is on.
	Connected to a Bluetooth device.
	Connected to a Wi-Fi network. Indicates the Wi-Fi version number.
	Not connected to a Wi-Fi network or no Wi-Fi signal.
	Connected to an Ethernet network.
	Indicates that a headset is connected to the device.

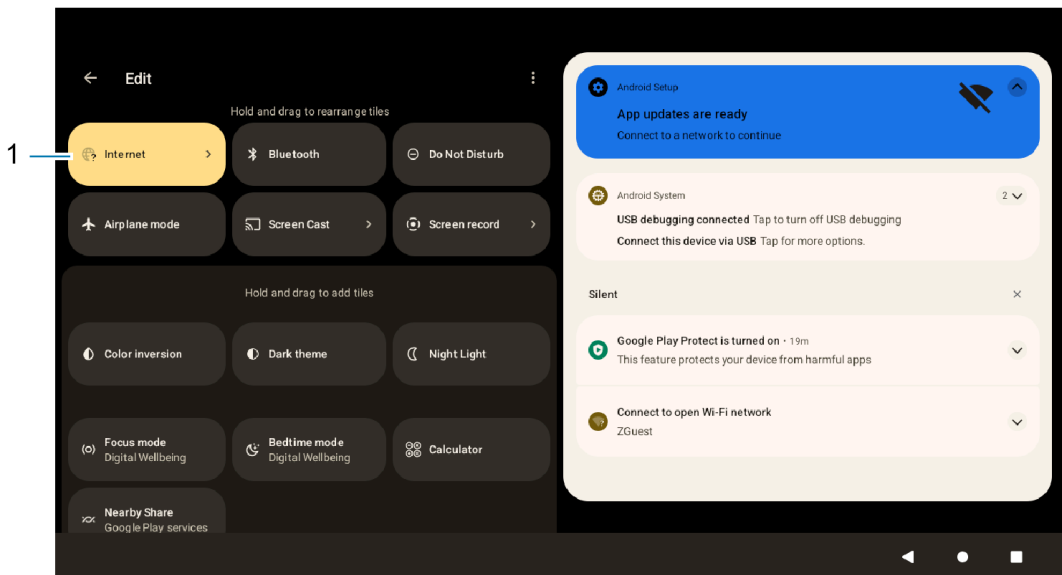
## Managing Notifications

Notification icons report the arrival of new messages, calendar events, alarms, and ongoing events. When a notification occurs, an icon appears in the Status bar with a brief description.

**Figure 21** Android 11 Notification Panel



**Figure 22** Android 13 Notification Panel



1	Quick settings bar
---	--------------------

- To view a list of all notifications, open the Notification panel by dragging the Status bar down from the top of the screen.

- To respond to a notification, open the Notification panel and then touch a notification. The Notification panel closes and the corresponding app opens.
- To manage recent or frequently used notifications, open the Notification panel and then touch Manage notifications. Touch the toggle switch next to an app to turn off all notifications, or touch an app for more notification options.
- To clear all notifications, open the Notification panel and then touch CLEAR ALL. All event-based notifications are removed. Ongoing notifications remain in the list.
- To close the Notification panel, swipe the Notification panel up.

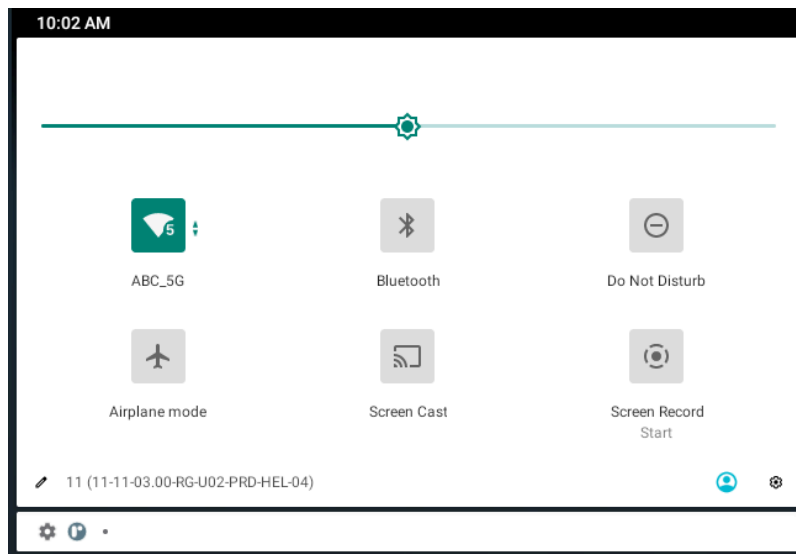
## Opening the Quick Access Panel

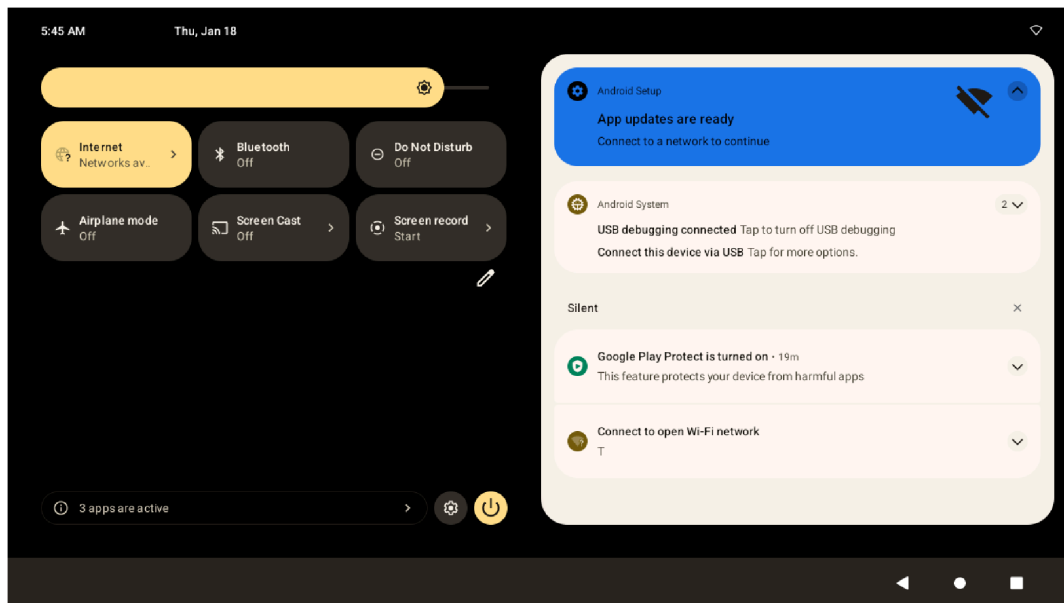
Use the Quick Access panel to access frequently used settings (for example, Airplane mode).



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

**Figure 23** Android 11 Quick Access Panel









**Figure 24** Android 13 Quick Access Panel

- If the device is locked, swipe down once.
- If the device is unlocked, swipe down once with two fingers, or twice with one finger.
- If the Notification panel is open, swipe down from the Quick Settings bar.











## Quick Access Panel Icons

Quick Access panel icons indicate frequently used settings (for example, Airplane mode).

**Table 5** Quick Access Panel Icons

Icon	Description
	Display brightness - Use the slider to decrease or increase the brightness of the screen. (A11 only)
	Display brightness - Use the slider to decrease or increase the brightness of the screen. (A13 only)
	Internet/Wi-Fi network - Turn Wi-Fi on or off. To open Wi-Fi settings, touch the Wi-Fi network name.
	Bluetooth settings - Turn Bluetooth on or off. To open Bluetooth settings, touch Bluetooth.
	Do not disturb - Control how and when to receive notifications.
	Airplane mode - Turn Airplane mode on or off. When Airplane mode is on the device does not connect to Wi-Fi or Bluetooth.

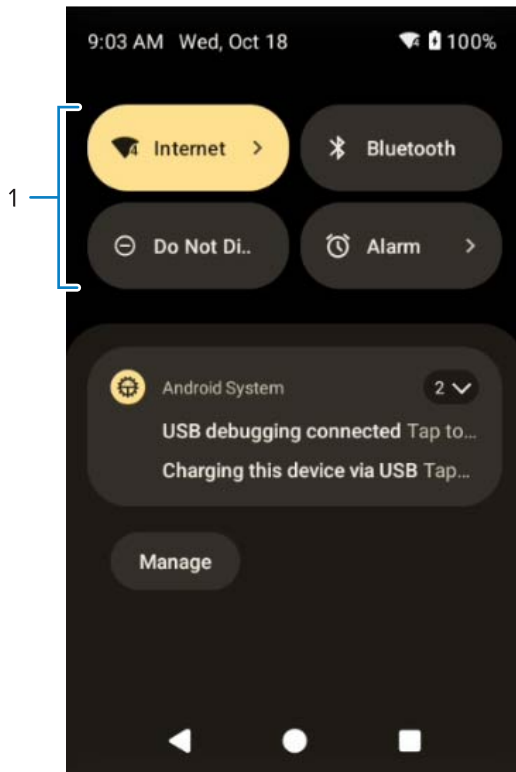
**Table 5** Quick Access Panel Icons (Continued)

Icon	Description
	Night Light - Tint the screen amber to make it easier to look at the screen in dim light. Set Night Light to turn on automatically from sunset to sunrise, or at other times.
	Screen Cast - Share phone content on Chromecast or a television with Chromecast built-in. On the Cast screen, check the "enable wireless display" option, and then touch "cast screen" to display a list of devices. Touch a device in the list to begin casting.
	Dark Theme - Toggles dark theme on and off. Dark themes reduce the luminance emitted by the screen, while meeting minimum color contrast ratios. It helps improve visual ergonomics by reducing eye strain, adjusting brightness to current lighting conditions, and facilitating screen use in dark environments, while conserving battery power.
	Focus mode - Turn on to pause distracting apps. To open Focus mode settings, touch and hold.
	Bedtime mode - Turn grayscale on and off. Grayscale turns the screen black and white, reducing phone distractions and improving battery life.
	Nearby Share - Helps find and interact with services and devices close to the device.
	Invert colors - Invert the display colors.
	Screen Record - Makes a video recording of everything that happens on the screen, with options to include audio and screen touches.
	NFC - Enable or disable NFC communication.
	Calculator - Open the calculator app. (A13 only)

## Editing the Quick Access Tiles

The first four setting tiles from the Quick Access panel become the Quick Access tiles on the Notification panel.

**Figure 25** Notification Panel



1	Quick access tiles
---	--------------------

- Open the Quick Access panel and touch  to edit, add, or remove settings tiles.

## Unlocking the Screen

The screen is locked when the device starts up.



**NOTE:** Use **Screen lock** to protect data on the device. Go to [Setting Screen Lock](#) on page 47 for information on setting up the locking feature.

- When the drive starts up, swipe the screen up to unlock.
  - If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.
  - If the PIN or Password screen unlock feature is enabled, enter the PIN or password after unlocking the screen.
- When the screen is dark, touch the screen.

# USB Communication

Connect the device to a host computer 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

Use the Transfer files option to copy files between the device and the host computer.

1. Connect the device to a host computer using a USB accessory.
2. On the device, pull down the Notification panel and touch **Connect this device via USB**.

By default, **No data transfer** is selected.

3. Touch **File Transfer**.



**NOTE:** After changing the setting to **File Transfer**, and then disconnecting the USB cable, the setting reverts back to **No data transfer**. If the USB cable is reconnected, select **File Transfer** again.

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

## Transferring Photos

Use PTP to copy photos from the device to the host computer.

1. Connect the device to a host computer using a USB accessory.
2. On the device, pull down the Notification panel and touch **Connect this device via USB**.
3. Touch **PTP**.
4. On the host computer, open a file explorer application.
5. Open the **Internal storage** folder.
6. Copy or delete photos as required.

## Disconnecting from the Host Computer



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



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

# Settings

This section describes the settings on the device.

## Accessing Settings

There are multiple ways to access settings on a device.


- Swipe down with two fingers from the top of the Home screen to open the Quick Access panel and touch .
- Double-swipe down from the top of the Home screen to open the Quick Access panel and touch .
- Swipe up from the bottom of the Home screen to open APPS and touch **Settings**.

## Display Settings

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

### Setting the Screen Brightness Manually

Manually set the screen brightness using the touchscreen.

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

### Setting Night Light

The Night Light setting tints the screen amber, making the screen easier to look at in low light.

1. Go to **Settings**.
2. Touch **Display**.
3. Touch **Night Light**.
4. Touch **Schedule**.

5. Select one of the schedule values:
  - None (default)
  - Turns on at custom time
  - Turns on from sunset to sunrise.
6. By default, **Night Light** is disabled.
  - On Android 11, touch **TURN ON NOW** to enable.
  - On Android 13, touch **Use Night Light** to enable.
7. Adjust the tint using the **Intensity** slider.

## Setting Screen Timeout

The screen turns off and goes into Suspend mode after the selected period of inactivity.

1. Go to **Settings**.
2. Touch **Display > Screen timeout**.
3. Select one of the sleep values:
  - **15 seconds**
  - **30 seconds**
  - **1 minute**
  - **2 minutes**
  - **5 minutes**
  - **10 minutes**
  - **30 minutes**
  - **Never** (default)
4. On Android 13, turn on the **Screen** attention switch to prevent your screen from turning off if you are looking at it.

## Setting Lock Screen Notifications

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

1. Go to **Settings**.
2. On Android 11, touch **Display > Advanced**.
3. On Android 13, touch **Display**.
4. Touch **Lock screen**.
5. On Android 11, in the **When to show** section, enable or disable an option using the switch.
6. On Android 13, in the **What to show** and **When to show** section, enable or disable an option using the switch.

## Setting Font Size

Set the size of the font in system apps.

1. Go to **Settings**.
2. On Android 11, touch **Display > Advanced > Font size**.
3. On Android 13, touch **Display > Display size and text**. Use the **Font size** + and - to vary the font size.
4. Touch **Home**.

## Setting Display Size

By default, the display size is set to Default.

1. Go to **Settings**.
2. On Android 11, touch **Display > Advanced > Display size**.
3. On Android 13, touch **Display > Display size and text**. Use the **Display size** + and - to vary the text size.
4. Touch **Home**.

## Setting the Date and Time

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

1. Go to **Settings**.
2. Touch **System > Date & time**.
3. On Android 11, touch **Use network-provided time** to disable automatic date and time synchronization.
4. On Android 13, touch **Set time automatically** to disable automatic date and time synchronization.
5. On Android 11, touch **Use network-provided time zone** to disable automatic time zone synchronization.
6. On Android 13, touch **Set time zone automatically** to disable automatic time zone synchronization.
7. Touch **Date** to select the date in the calendar.
8. Touch **OK**.
9. Touch **Time**.
  - a) Touch the circle, drag to the current hour, and then release.
  - b) Touch the circle, drag to the current minute, and then release.
  - c) Touch **AM** or **PM**.
10. Touch **OK**.
11. Touch **Time zone > Time zone** and select the current time zone from the list. This option may not be available in some locations.
12. Touch **Time zone > Region** to select the current time zone from the list.
13. Touch **Update Interval** to select an interval to synchronize the system time from the network.
14. In **TIME FORMAT**, choose either **Use locale default** or **Use 24-hour format**.

## General Sound Setting

Use the Sound settings to configure media and alarm volumes.

1. Go to **Settings**.
2. On Android 11, touch **Sound**.
3. On Android 13, touch **Sounds & Vibrations**.
4. Touch an option to set sounds.

## Sound Options

- **Media volume** - Controls the music, games, and media volume.
- **Alarm volume** - Controls the alarm clock volume.
- **Notifications volume** - Controls the notification volume.
- **Do Not Disturb** - Mutes some or all sounds and vibrations.
- **Live Caption** - Detects speech on your device and automatically generates captions. (Android 13 only)
- **Media** - Shows the media player in Quick Settings while sound is playing, allowing quick access.
- **Shortcut to prevent ringing** - Select how the shortcut method prevents ringing.
- **Default notification sound** - Select a sound to play for all system notifications.
- **Default alarm sound** - Select a sound to play for alarms.
- **Other sounds and vibrations:**
  - **Screen locking sounds** - Play a sound when locking and unlocking the screen (default – enabled).
  - **Advanced**
    - **Touch sounds** - Play a sound when making screen selections (default – enabled).

## Remapping a Button

Buttons on the device can be programmed to perform different functions or as shortcuts to installed apps. For a list of key names and descriptions, refer to: [techdocs.zebra.com](https://techdocs.zebra.com).

1. Go to **Settings**.
2. Touch **Key Programmer**. A list of programmable buttons displays.
3. Select the button to remap:
  - **VOLUMEUP**
  - **VOLUMEDOWN**
4. Touch the **Shortcut**, the **Keys and Buttons**, or the **Trigger** tabs to list the available functions, applications, and triggers.
5. Touch a function or application shortcut to map to the button.



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

Remappable Keys

Figure 26 CC6000 Key Positions

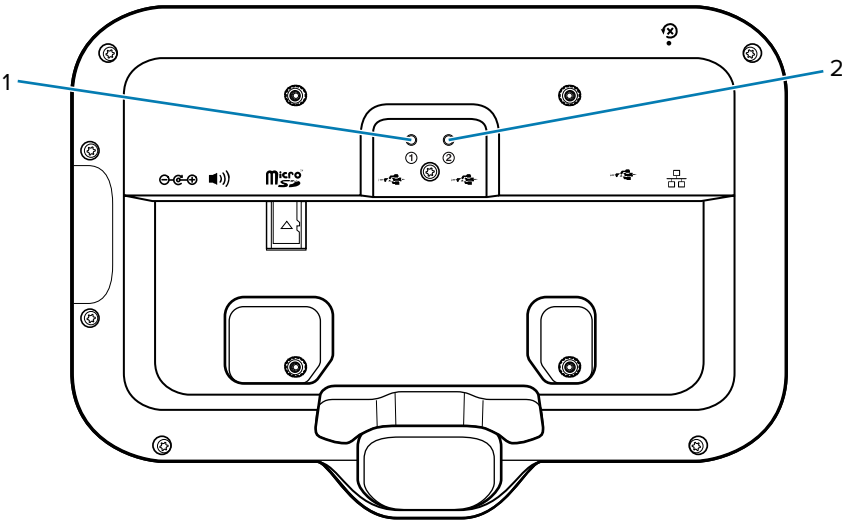


Figure 27 CC600 Key Positions

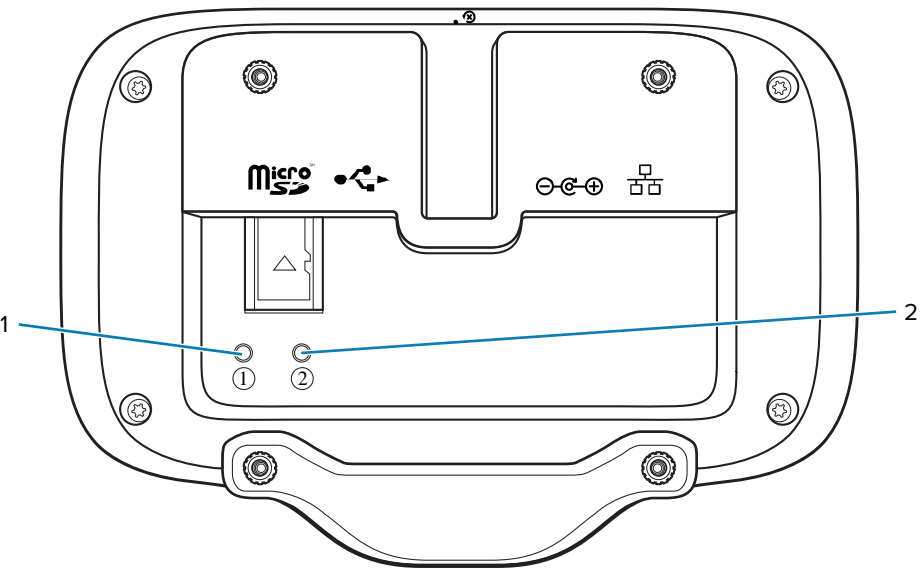



Table 6 Key Positions

Number	Button	Description
1	VOLUME_UP	Volume up button.
2	VOLUME_DOWN	Volume down button.

## Setting Screen Lock

Use the Device security settings to set preferences for locking the screen on an initial boot.

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.

1. Swipe down from the Status bar to open the Quick Access panel and then touch .
2. Touch **Security > Screen lock**.
  - **None** - Disable screen unlock security.
  - **Swipe** - Slide the lock icon to unlock the screen.
  - **PIN** - Enter a numeric PIN to unlock the screen. See [Setting Screen Lock Using PIN](#) on page 47 for more information.
  - **Pattern** - Draw a pattern to unlock the screen. See [Setting Screen Lock Using Pattern](#) on page 48 for more information.
  - **Password** - Enter a password to unlock the screen. See [Setting Screen Lock Using Password](#) on page 47 for more information.

### Setting Screen Lock Using PIN

1. Touch **Settings > Security > PIN**.
2. Select an option whether to require a PIN to start the device.  
Select **Yes** to protect access to data on the device. The device cannot receive notifications until the device starts up.
3. Enter a PIN (minimum four numbers).
4. Touch **Next**.
5. Re-enter PIN.
6. Touch **Confirm**.
7. Select the type of notifications that appear when the screen is locked.
8. Touch **Done**.

The next time the device is powered on, a PIN is required.

### Setting Screen Lock Using Password

1. Touch **Settings > Security > Password**.
2. Select an option whether to require a PIN to start the device.  
Select **Yes** to protect access to data on the device. The device cannot receive notifications until the device starts up.
3. Enter a password (between 4 and 16 characters).
4. Touch **Next**.
5. Re-enter the password.
6. Touch **Confirm**.

7. Select the type of notifications that appear when the screen is locked.
8. Touch **Done**.

The next time the device is powered on, a password is required.

## Setting Screen Lock Using Pattern

1. Touch **Settings** > **Security** > **Pattern**.
2. Select an option whether to require a pattern to start the device.  
Select **Yes** to protect access to data on the device. The device cannot receive notifications until the device starts up.
3. Draw a pattern connecting at least four dots.
4. Touch **Next**.
5. Re-draw the pattern.
6. Touch **Confirm**.
7. Select the type of notifications that appear when the screen is locked.
8. Touch **Done**.

The next time the device is powered on, a pattern is required.

## Keyboards

The device provides multiple keyboard options.

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



**NOTE:** By default, the Enterprise and Virtual Keyboards are disabled. The Enterprise Keyboard is available for download from the [Zebra Support Site](#).

## Keyboard Configuration

This section describes configuring the device's keyboard.

### Enabling Keyboards

1. Go to **Settings**.
2. Touch **System** > **Languages & input** > **On-screen keyboard** > **Manage on-screen keyboards**.
3. Touch a keyboard to enable.

## Switching Between Keyboards

To switch between keyboards, touch in a text box to display the current keyboard.



**NOTE:** By default, the Gboard is enabled. All other virtual keyboards are disabled.

- On the Gboard keyboard, touch and hold (GMS devices only).
- On the Android keyboard, touch, and hold (Non-GMS devices only).
- On the Enterprise keyboard, touch .

## Using the Android and Gboard Keyboards

Use the Android or Gboard keyboards to enter text in a text field.

- To configure the keyboard settings, touch and hold "," (comma) and then select **Android keyboard settings**.

## Edit Text

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

## Entering Numbers, Symbols, and Special Characters

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

## Enterprise Keyboard

The Enterprise Keyboard contains multiple keyboard types.

- Numeric
- Alpha
- Special characters
- Data capture

## Numeric Tab


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

## Alpha Tab

The alpha keyboard is labeled using the language code. For English, the alpha keyboard is labeled **EN**.

## Additional Character Tab

The additional characters keyboard is labeled **#\*/\***.

- Touch  to enter emoji icons in a text message.
- Touch **ABC** to return to the Symbols keyboard.


## Scan Tab

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

# Language Usage

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

## Changing the Language Setting

1. Go to **Settings**.
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.  
The operating system text changes to the selected language.

## Adding Words to the Dictionary

1. Go to **Settings**.
2. On Android 11, touch **System > Languages & input > Advanced > Personal dictionary**.
3. On Android 13, touch **System > Languages & input > Personal dictionary**.
4. If prompted, select the language where this word or phrase is stored.
5. Touch **+** to add a new word or phrase to the dictionary.

6. Enter the word or phrase.
7. In the **Shortcut** text box, enter a shortcut for the word or phrase.

## Notifications

This section describes setting, viewing, and controlling notifications on the device.

### Setting App Notifications

Configure the notifications settings for a specific app.

1. Go to **Settings**.
2. On Android 11, touch **Apps & notifications > App info**.  
If there are no recently opened apps, touch **App info** to open the **App Info** screen.
3. On Android 13, touch **Apps > All Apps**.
4. Select an app.  
Options vary depending on the app selected.

5. On Android 11, select an available option:

- **Open** - Opens the app.
- **Disable** - Turn the app off and hide it. The app no longer appears in the All Apps list. You must re-enable the app to use it.
- **Force Stop** - Turn off the app.
- **Notifications**
  - **All app notifications** - Select to turn all notifications from this app on (default) or off. Touch a notification category to display additional options.
  - **Default** - Allow notifications from this app to make sound or vibrate the device.
  - **Silent** - Do not allow notifications from this app to make sound or vibrate.
  - **Minimize** - In the Notification panel, collapse notifications to one line.
  - **Advanced** - Touch for additional options.
    - **Allow notification dot** - Do not allow this app to add a notification dot to the app icon.
    - **Additional settings in the app** - Open the app settings.
  - **Permissions** - Configure which permissions are allowed or denied for this app.
  - **Storage & cache** - View the amount of storage and cache space used for this app. You can choose to **Clear Storage** and **Clear Cache** for the app to free up storage space on the device.
  - **Mobile data & Wi-Fi** - View the data usage for this app. You can choose to enable Background data usage or allow Unrestricted data usage by this app.
  - **Advanced** - Touch for additional options.
  - **Screen time** - Touch for options to set an App timer that limits the amount of time you can use this app and to Manage notifications.
  - **Open by default** - Modify which links or files the app opens by default.
- **Advanced**
  - **Picture-in-picture** - Allow this app to create a picture-in-picture window when the app is running in the background.
  - **Install unknown apps** - Allow this app to install unknown apps.
  - **Display over other apps** - Allow this app to display over other apps.
  - **Modify system settings** - Allow this app to modify system settings.
- **Store**
  - **App details** - Opens the Google Play Store to display information about the app.

6. On Android 13, touch the switch to turn on or off notifications for this app.

- **Allow notification dot** - Do not allow this app to add a notification dot to the app icon.
- **Additional settings in the app** - Open the app settings.

## Viewing Notifications

1. Go to **Settings**.
2. On Android 11, touch **Apps & Notifications**.

3. On Android 13, touch **Notifications > App Settings**.
4. Scroll down to **Notifications** to view how many apps have notifications turned off.

### Controlling Lock Screen Notifications

Control whether notifications can be seen when the device is locked.

1. Go to **Settings**.
2. On Android 11, touch **Apps & notifications > Notifications**.
3. On Android 13, touch **Notifications**
4. Touch **Notifications on lockscreen** and select one of the following:
  - **Show conversations, default, and silent (default)**
  - **Hide silent conversations and notifications**
  - **Don't show any notifications**








# Applications

Apart from the standard pre-installed Android applications, the following table lists Zebra-specific applications installed on the device.








## Installed Applications

Aside from the common Google apps, the Zebra-specific apps that are installed on the device are described in this section.

**Table 7** Apps

Icon	Description
	<b>Bluetooth Pairing Utility</b> – Use to pair a Zebra Bluetooth scanner with the device by scanning a barcode.
	<b>DataWedge</b> - Enables data capture using the imager.
	<b>DisplayLink Presenter</b> - Use to present the device screen onto a connected monitor.
	<b>DWDemo</b> - Provides a way to demonstrate the data capture features using the imager.
	<b>License Manager</b> - Use to manage software licenses on the device.
	<b>PTT Express</b> - Use to launch PTT Express client for VoIP communication. (Android 11 only)
	<b>StageNow</b> - Allows the device to stage a device for initial use by initiating the deployment of settings, firmware, and software.

**Table 7** Apps (Continued)

Icon	Description
	<b>RxLogger</b> - Use to diagnose device and app issues.
	<b>Settings</b> - Use to configure the device.
	<b>VoD</b> - The Video on Device basic app provides a how-to video for proper device cleaning. For Video on Device licensing information, contact <a href="mailto:learningservices@zebra.com">learningservices@zebra.com</a> .
	<b>Wireless Analyzer</b> - A diagnostic intelligent app. Use to diagnose surrounding area and display network stats, such as coverage hole detection or AP in the vicinity. Refer to the Worry Free Wi-Fi Analyzer Administrator Guide for Android. Only available with Mobility DNA Enterprise License.
	<b>Zebra Bluetooth Settings</b> - Use to configure Bluetooth logging.
	<b>Zebra Data Services</b> - Use to enable or disable Zebra Data Services. Some options are set by the system administrator.
	<b>Zebra Showcase</b> - Provides a way to experience and learn about Zebra's new or existing capabilities. (Android 13 only)

## Accessing Apps

Access all apps installed on the device using the APPS window.

1. On the Home screen, swipe up from the bottom of the screen.
2. Slide the **APPS** window up or down to view more app icons.
3. Touch an icon to open the app.

## Switching Between Recent Apps

1. Touch **Recent**.

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

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

## Camera

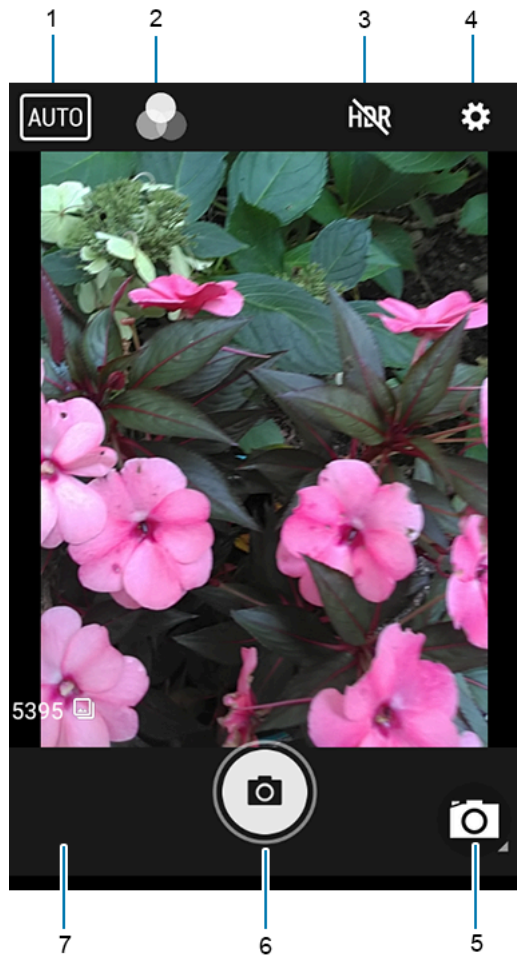
This section provides information for taking photos and recording videos using the integrated digital cameras.



**NOTE:** The device saves photos and videos on the microSD card, if installed and the storage path is changed manually. By default, or if a microSD card is not installed, the device saves photos and videos on internal storage.



### Taking Photos

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



1	Scene mode
2	Color effect
3	High dynamic range
4	Settings
5	Camera mode

6	Shutter button
7	Gallery


2. If necessary, touch the Camera Mode icon and touch .
3. Frame the subject on the screen.
4. To zoom in or out, press two fingers on the display and pinch or expand your fingers. The zoom controls appear on the screen.
5. Touch an area on the screen to focus. The focus circle appears. The two bars turn green when in focus.
6. Touch .

The camera takes a photo and a shutter sound plays.

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



## Recording Videos

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

2. Touch the camera mode menu and touch .




1	Color effect
2	Audio
3	Settings
4	Camera mode
5	Shutter button
6	Gallery






3. Point the camera and frame the scene.
4. To zoom in or out, press two fingers on the display and pinch or expand fingers. The zoom controls appear on the screen.
5. Touch  to start recording.  
The video time remaining appears in the top left of the screen.
6. Touch  to end the recording.

## Photo Settings

In Photo mode, photo settings appear on screen.


Touch  to display the photo settings options.

- **Selfie Flash** - Turns the screen white to help produce a little extra light in dimmer settings. Options: Off (default), or On.
- **Picture size** - Set the size (in pixels) of the photo to: 5M pixels (default), 3M pixels, HD1080, 2M pixels, HD720, 1M pixels, WVGA, VGA, or QVGA.
- **Picture quality** - Set the picture quality setting to: Low, Standard or High (default).
- **Countdown timer** - Set to: Off (default), 2 seconds, 5 seconds or 10 seconds.
- **Storage** – Set location to store the photo to: Phone.
- **Continuous Shot** - Select to take a series of photos quickly while holding the capture button. Off (default) or On.
- **Face Detection** - Select to turn face detection Off (default) or On.
- **ISO** - Set how sensitive the camera is to light. Options: Auto (default), ISO Auto (HJR), ISO100, ISO200, ISO400, ISO800 or ISO1600.
- **Exposure** - Touch to adjust the exposure settings. Options: +2, +1, 0 (default), -1 or -2.
- **White balance** - Select how the camera adjusts colors in different kinds of light, to achieve the most natural-looking colors.





Icon	Description
	<b>Incandescent</b> - Adjust the white balance for incandescent lighting.
	<b>Fluorescent</b> - Adjust the white balance for fluorescent lighting.
	<b>Auto</b> - Adjust the white balance automatically (default).
	<b>Daylight</b> - Adjust the white balance for daylight.
	<b>Cloudy</b> - Adjust the white balance for a cloudy environment.

- **Redeye reduction** - Helps eliminate redeye effect. Options: Disabled (default), or Enable.
- **ZSL** - Set the camera to immediately take a picture when the button is pressed (default – enabled)
- **Selfie Mirror** - Select to save a mirror image of the photo. Options: Disable (default), or Enable.
- **Shutter Sound** - Select to play a shutter sound when taking a photo. Options: Disable (default) or Enable.
- **Anti Banding** - Allows the camera to avoid problems caused by artificial light sources that are not constant. These sources cycle (flicker) fast enough to go unnoticed to the human eye, appearing continuous. The camera's eye (its sensor) can still see this flicker. Options: Auto (default), 60 Hz, 50 Hz, or Off.

## Video Settings

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

- **Video quality** – Set video quality to: HD1080p (default), HD 720p, SD 480p, VGA, CIF, or QVGA.
- **Video duration** – Set to: 30 seconds (MMS), 10 minutes, 30 minutes (default), or no limit.
- **Storage** – Set the location to store the photo to: Phone (default).
- **White balance** - Select how the camera adjusts colors in different kinds of light, to achieve the most natural-looking colors.

Icon	Description
	<b>Incandescent</b> - Adjust the white balance for incandescent lighting.
	<b>Fluorescent</b> - Adjust the white balance for fluorescent lighting.
	<b>Auto</b> - Adjust the white balance automatically (default).
	<b>Daylight</b> - Adjust the white balance for daylight.
	<b>Cloudy</b> - Adjust the white balance for a cloudy environment.

- **Image Stabilization** - Set to reduce blurry videos due to device movement. Options: On or Off (default).

## DWDemo




Use DataWedge Demonstration (DWDemo) to demonstrate data capture functionality. To configure DataWedge, refer to [techdocs.zebra.com/datawedge/](https://techdocs.zebra.com/datawedge/).










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

## DWDemo Icons

**Table 8** DWDemo Icons


Category	Icon	Description
Illumination		Imager illumination is on. Touch to turn illumination off.
Illumination		Imager illumination is off. Touch to turn illumination on.
Data Capture		The data capture function is through the internal imager.

**Table 8** DWDemo Icons (Continued)

Category	Icon	Description
Data Capture		Indicates a USB scanner is connected to the device.
Data Capture		Indicates a USB scanner is not connected to the device.
Data Capture		A Bluetooth scanner is connected.
Data Capture		A Bluetooth scanner is not connected.
Scan Mode		Imager is in picklist mode. Touch to change to normal scan mode.
Scan Mode		Imager is in normal scan mode. Touch to change to picklist mode.
Menu		Opens a menu to view the application information or to set the application DataWedge profile.

## Selecting a Scanner

See the Data Capture section for more information.

1. To select a scanner, touch  > **Settings** > **Scanner Selection**.
2. Touch the on-screen yellow scan button to capture data.

The data appears in the text field below the yellow button.

## PTT Express Voice Client

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



**NOTE:** PTT Express is only pre-installed on Android 11.



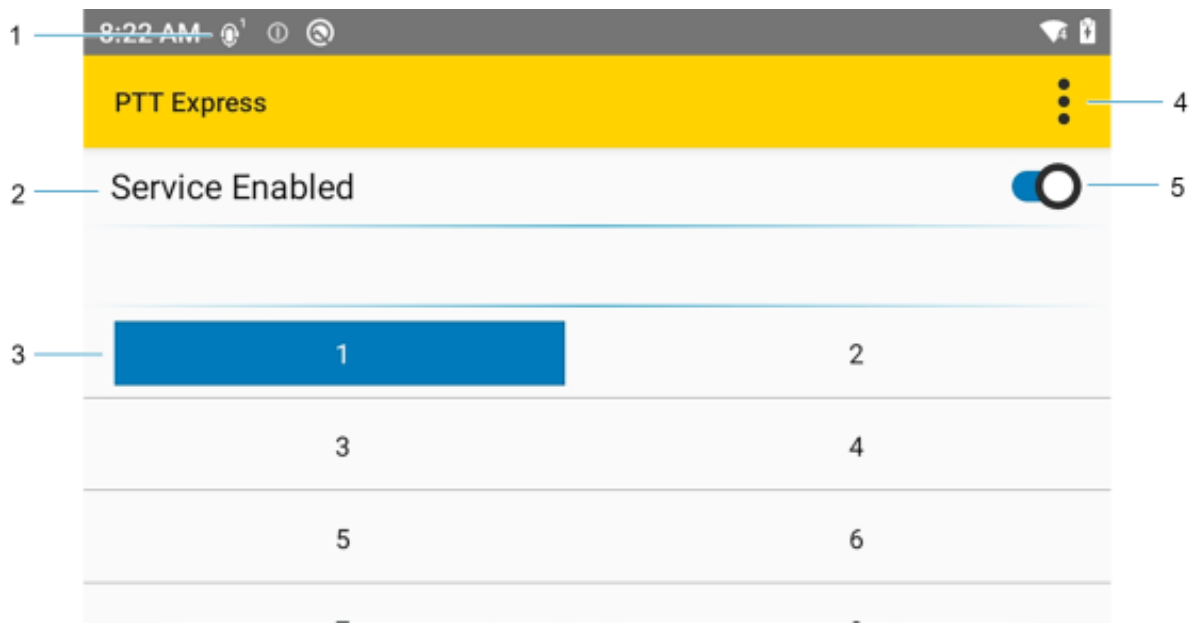
**NOTE:** Requires a PTT Express License.

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

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

## PTT Express User Interface

Use the PTT Express interface for Push-To-Talk communication.



Number	Item	Description
1	Notification icon	Indicates the current state of the PTT Express client.
2	Service indication	Indicates the status of the PTT Express client. Options are: Service Enabled, Service Disabled or Service Unavailable.
3	Talk group	Lists all 32 Talk Groups available for PTT communication.
4	Settings	Opens the PTT Express Settings screen.
5	Enable/disable switch	Turns the PTT service on and off.

## PTT Audible Indicators

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

- **Talk Tone:** Double chirp. Plays when the Talk button is depressed. This is a prompt for you to start talking.
- **Access Tone:** Single beep. Plays when another user just finished a broadcast or response. You can now initiate a Group Broadcast or Private Response.
- **Busy Tone:** Continuous tone. Plays when the Talk button is depressed and another user is already communicating on the same talkgroup. Plays after the maximum allowed talk time is reached (60 seconds).








- **Network Tone:**

- Three increasing pitch beeps. Plays when PTT Express acquires the WLAN connection and the service is enabled.
- Three decreasing pitch beeps. Plays when PTT Express loses the WLAN connection or the service is disabled.


## PTT Notification Icons

Notification icons indicate the current state of the PTT Express Voice client.

**Table 9** PTT Express Icons

Status Icon	Description
	The PTT Express Voice client is disabled.
	The PTT Express Voice client is enabled but not connected to a WLAN.
	The PTT Express Voice client is enabled, connected to a WLAN, and listening on the Talk Group indicated by the number next to the icon.
	The PTT Express Voice client is enabled, connected to a WLAN, and communicating on the Talk Group indicated by the number next to the icon.
	The PTT Express Voice client is enabled, connected to a WLAN, and in a private response.
	The PTT Express Voice client is enabled and muted.
	The PTT Express Voice client is enabled but it is not able to communicate due to a VoIP telephony call in progress.

## Enabling PTT Communication

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

## Selecting a Talk Group

There are 32 Talk Groups that can be selected by PTT Express users. However, only one talk group can be enabled at a time on the device.

- Touch one of the 32 Talk Groups. The selected Talk Group is highlighted.

## PTT Communication

This section describes the default PTT Express client configuration. Refer to the PTT Express V1.2 User Guide for detailed information on using the client.

### Creating Group Call



**NOTE:** When using a wired headset, use only Zebra approved wired headsets with a PTT button.

1. Press and hold the GROUP CALL button (or the Talk button on the headset) and listen for the talk tone.  
If you hear a busy tone, release the button and wait a moment before making another attempt. Ensure that PTT Express and the WLAN are enabled.



**NOTE:** Holding the button for more than 60 seconds (default) drops the call, allowing others to make Group Calls. Release the button when finished talking to allow others to make calls.


2. Start talking after hearing the talk tone.
3. Release the button when finished talking.

### Responding Private Response

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

1. Wait for an access tone.
2. Within 10 seconds, press and hold the PRIVATE CALL button, and listen for the talk tone.
3. If you hear a busy tone, release the button and wait a moment before making another attempt. Ensure that PTT Express and the WLAN are enabled.
4. Start talking after the talk tone plays.
5. Release the button when finished talking.

### Disabling PTT Communication

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

## Rxlogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics, and diagnoses device and application issues.

RxLogger logs the following information: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging, cellular logging, TCP dumps, Bluetooth logging, GPS logging, logcat, FTP push/pull, ANR dumps, etc. All generated logs and files are saved onto flash storage on the device (internal or external).

### RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plug-ins already built-in. For information on configuring RxLogger, refer to [techdocs.zebra.com/rxlogger/](https://techdocs.zebra.com/rxlogger/).


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

## Configuration File


All RxLogger settings are stored in a file on the device, permitting remote configuration and mass deployment of setting files using an enterprise mobile management (EMM) system.

The config.json 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 JSON file on the device. There is no need to stop and restart the RxLogger service because the file change is automatically detected.

## Enabling Logging

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

## Disabling Logging

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

## Extracting Log Files

1. Connect the device to a host computer using a 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.

## Backing Up Data


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  > **BackupNow**.

## 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 using Main Chat Head.

### Initiating 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

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

### Viewing Logs

1. Touch the Main Chat Head icon.  
The RxLogger Utility screen appears.
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.

### 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 backup.

# Data Capture

This section provides information for capturing barcode data using various scanning options.

The device supports data capture using:

- Internal Linear Imager (SE2100)
- Internal Linear Imager (SE4710)
- RS507/RS507X Hands-free Imager
- RS6000 Hands-free Imager
- RS5100 Bluetooth Ring Scanner
- DS3678 Digital Scanner
- LI3678 Linear Scanner
- DS2278 Digital Scanner
- DS8178 Digital Scanner

## Imaging

The device with an integrated 2D imager has the following features:

- Omnidirectional reading of a variety of barcode symbologies, including the most popular linear, postal, PDF417, Digimarc, and 2D matrix code types.
- The ability to capture and download images to a host for a variety of imaging applications.
- Advanced intuitive laser aiming cross-hair and dot aiming for easy point-and-shoot operation.

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

## Linear Imager

The device with integrated linear imager has the following features:

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

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

## Operational Modes

The device with an integrated imager supports three modes of operation.

Activate each mode by pressing **Scan**.

- Decode mode — The device attempts to locate and decode enabled barcodes within its field of view. The imager remains in this mode as long as you hold the scan button, or until it decodes a barcode.



**NOTE:** To enable Picklist Mode, configure in DataWedge or set in an application using an API command.

- Picklist mode — Selectively decode a barcode when more than one barcode is in the device's field of view by moving the aiming crosshair or dot over the required barcode. Use this feature for pick lists containing multiple barcodes and manufacturing or transport labels containing more than one barcode type (either 1D or 2D).



**NOTE:** To enable MultiBarcode Mode, configure in DataWedge or set in an application using an API command.

- MultiBarcode Mode — In this mode, the device attempts to locate and decode a specific number of unique barcodes within its field of view. The device remains in this mode as long as the user holds the scan button, or until it decodes all the barcodes.
  - The device attempts to scan the programmed number of unique barcodes (from 2 through 100). This may be a fixed amount, meaning it scans X unique barcodes, or can be set as a range to scan a different number of unique barcodes each session.
  - If there are duplicate barcodes (same symbology type and data), only one of the duplicate barcodes is decoded and the remainder are ignored. If the label has two duplicate barcodes plus another two different barcodes, a maximum of three barcodes will be decoded from that label; one will be ignored as a duplicate.
  - Barcodes can be of multiple symbology types and still be acquired together. For example, if the specified quantity for a MultiBarcode Mode scan is four, two barcodes can be symbology type Code 128 and the other two can be symbology type Code 39.
  - If the specified number of unique barcodes is not initially in view of the device, the device will not decode any data until the device is moved to capture the additional barcode(s) or time out occurs. If the device field of view contains a number of barcodes greater than the specified quantity, the device randomly decodes barcode(s) until the specified number of unique barcodes is reached. For example, if the count is set to two and eight barcodes are in the field of view, the device decodes the first two unique barcodes it sees, returning the data in random order.
  - MultiBarcode Mode does not support concatenated barcodes.

## Scanning Considerations

Typically, scanning is a simple matter of aim, scan, and decode, with a few quick trial efforts to master it.

However, consider the following to optimize scanning performance:

- Range — Scanners decode optimally over a particular working range — minimum and maximum distances from the barcode. This range varies according to barcode density and scanning device optics. Scan within range for quick and constant decodes; scanning too close or too far away prevents decodes. Move the scanner closer and further away to find the right working range for the barcodes being scanned.

- Angle — Scanning angle is important for quick decodes. When the illumination/flash reflects directly back into the imager, the specular reflection can blind/saturate the imager. To avoid this, scan the barcode so that the beam does not bounce directly back. Do not scan at too sharp an angle; the scanner needs to collect scattered reflections from the scan to make a successful decode. Practice quickly shows what tolerances to work within.
- Hold the device farther away for larger symbols.
- Move the device closer for symbols with bars that are close together.



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

### Scanning with Internal Imager (SE2100)

Use the internal imager to capture barcode data.



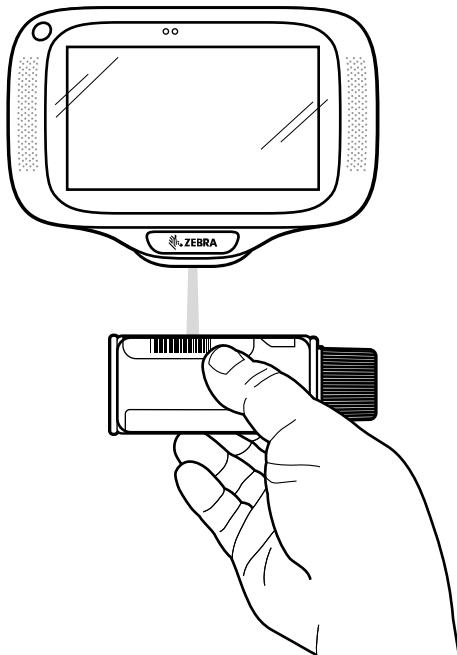
**NOTE:** Configure the imager illumination setting in the DataWedge application.



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

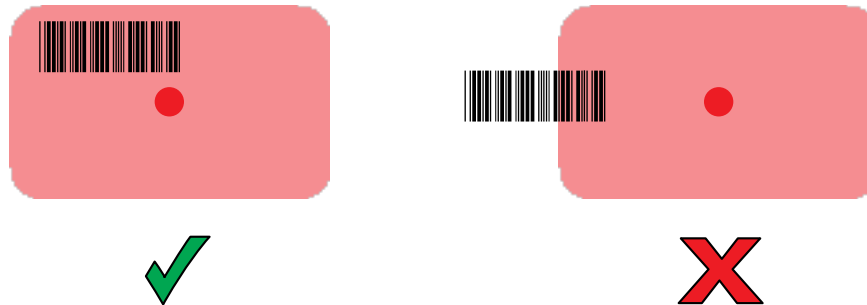
To scan with the internal imager:

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.



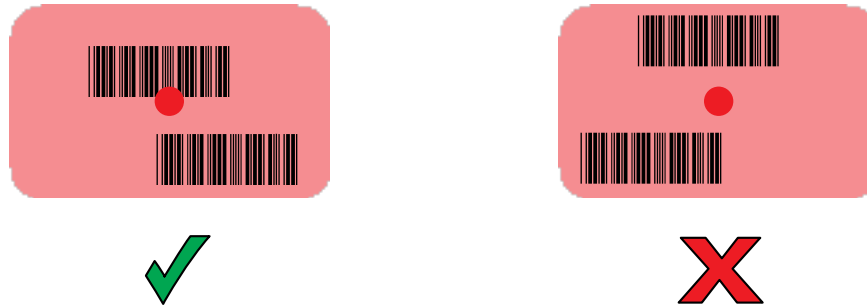
3. Ensure the barcode is within the area formed by the aiming pattern. The aiming dot is used for increased visibility in bright lighting conditions.

**Figure 28** Aiming Pattern



**NOTE:** 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 29** Pick List Mode with Multiple Barcodes



By default, a beep sound indicates that the barcode was decoded successfully. The barcode content data appears in the text field.

## Scanning with Internal Imager (SE4710)

Use the internal imager to capture barcode data.



**NOTE:** Configure the imager illumination setting in the DataWedge application.

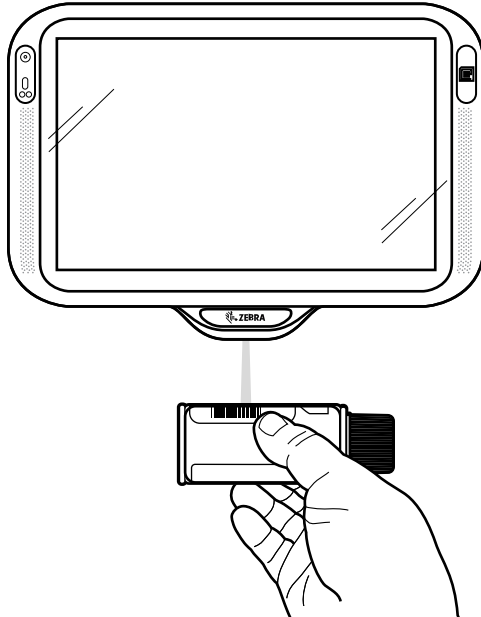


**NOTE:** To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the scanner to decode barcode data and display the barcode content.

To scan with the internal imager:

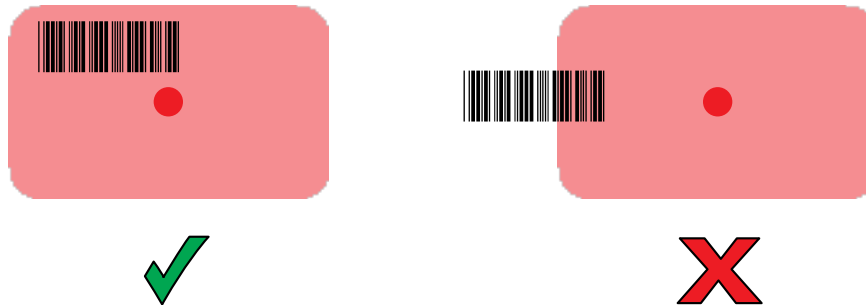
1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).

2. Place the barcode in the field of view of the device's scan window.



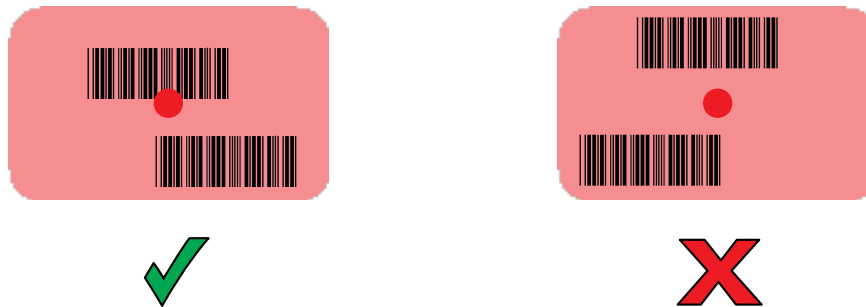
3. Ensure the barcode is within the area formed by the aiming pattern. The aiming dot is used for increased visibility in bright lighting conditions.

**Figure 30** Aiming Pattern



**NOTE:** 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 31** Pick List Mode with Multiple Barcodes

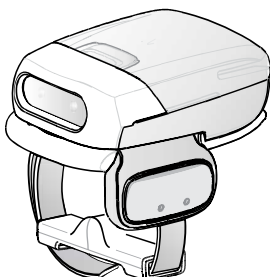


By default, a beep sound indicates that the barcode was decoded successfully. The barcode content data appears in the text field.

## Scanning with the RS507/RS507X Hands-Free Imager

Use the RS507/RS507X Hands-Free Imager to capture barcode data.

**Figure 32** RS507/RS507X Hands-Free Imager



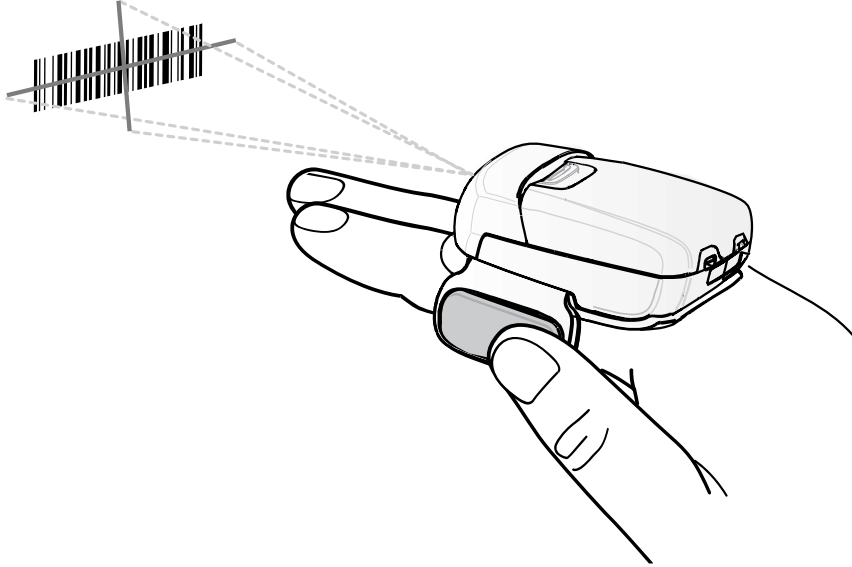
Refer to the RS507/RS507X Hands-free Imager Product Reference Guide for more information.



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

To scan with the RS507/RS507x:

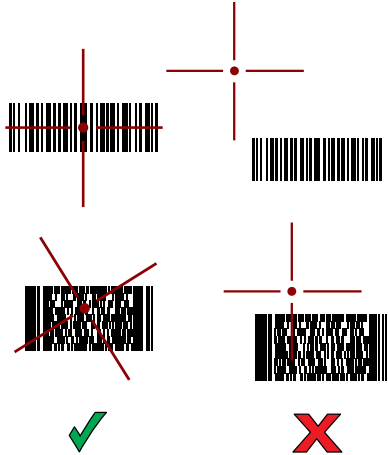
1. Pair the RS507/RS507X with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS507/RS507X at a barcode.



4. Press and hold the trigger.

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

**Figure 33** RS507/RS507X Aiming Pattern



When the RS507/RS507X is in Pick List mode, the RS507/RS507X does not decode the barcode until the center of the crosshair touches the barcode.

**Figure 34** RS507/RS507X Pick List Mode with Multiple Barcodes in Aiming Pattern



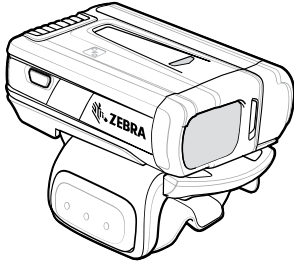
The RS507/RS507X LEDs light green and a beep sounds to indicate the barcode was decoded successfully.

The captured data appears in the text field.

## Scanning with the RS6000 Bluetooth Ring Scanner

Use the RS6000 Bluetooth Ring Scanner to capture barcode data.

**Figure 35** RS6000 Bluetooth Ring Scanner



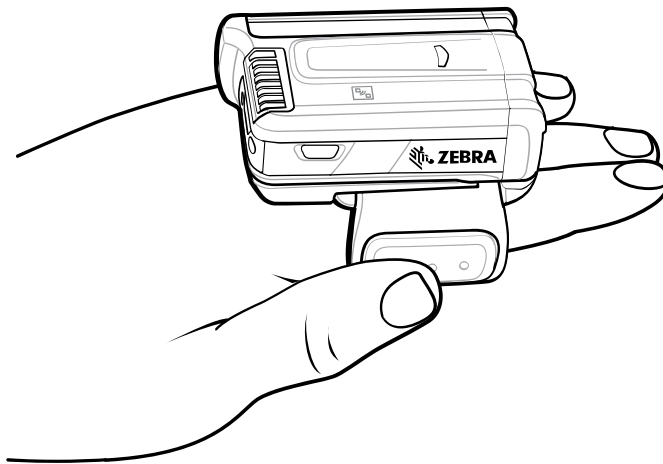
Refer to the RS6000 Bluetooth Ring Scanner Product Reference Guide for more information.



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

To scan with the RS6000:

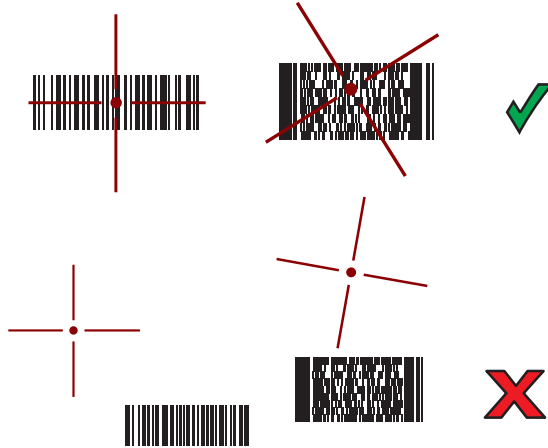
1. Pair the RS6000 with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS6000 at a barcode.



4. Press and hold the trigger.

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

**Figure 36** RS6000 Aiming Pattern



When the RS6000 is in Pick List mode, the RS6000 does not decode the barcode until the center of the crosshair touches the barcode.

**Figure 37** RS6000 Pick List Mode with Multiple Barcodes in Aiming Pattern

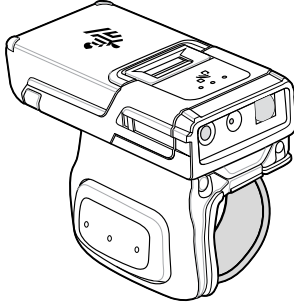


The RS6000 LEDs light green and a beep sounds to indicate the barcode was decoded successfully. The captured data appears in the text field.

## Scanning with the RS5100 Ring Scanner

Use the RS5100 Ring Scanner to capture barcode data.

**Figure 38** RS5100 Ring Scanner



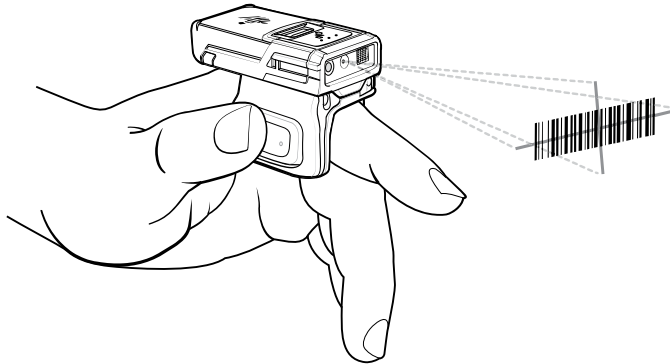
Refer to the RS5100 Ring Scanner Product Reference Guide for more information.



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

To scan with the RS5100:

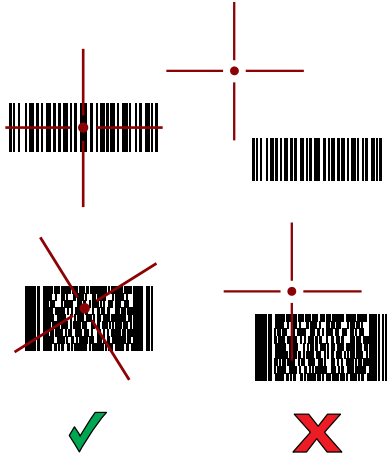
1. Pair the RS5100 with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS5100 at a barcode.



4. Press and hold the trigger.

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

**Figure 39** RS5100 Aiming Pattern



When the RS5100 is in Pick List mode, the RS5100 does not decode the barcode until the center of the crosshair touches the barcode.

**Figure 40** RS5100 Pick List Mode with Multiple Barcodes in Aiming Pattern

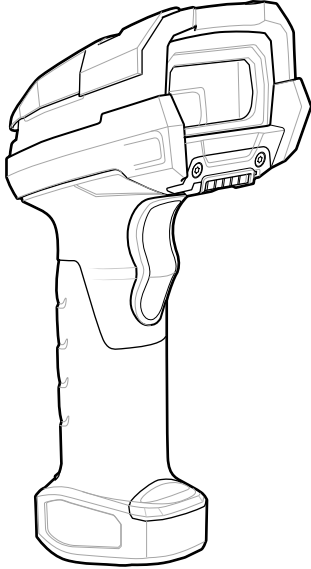


The RS5100 LEDs light green and a beep sounds to indicate the barcode was decoded successfully. The captured data appears in the text field.

## Scanning with the DS3678 Bluetooth Scanner

Use the DS3678 Bluetooth Scanner to capture barcode data.

**Figure 41** DS3678 Digital Scanner



Refer to the DS3678 Product Reference Guide for more information.

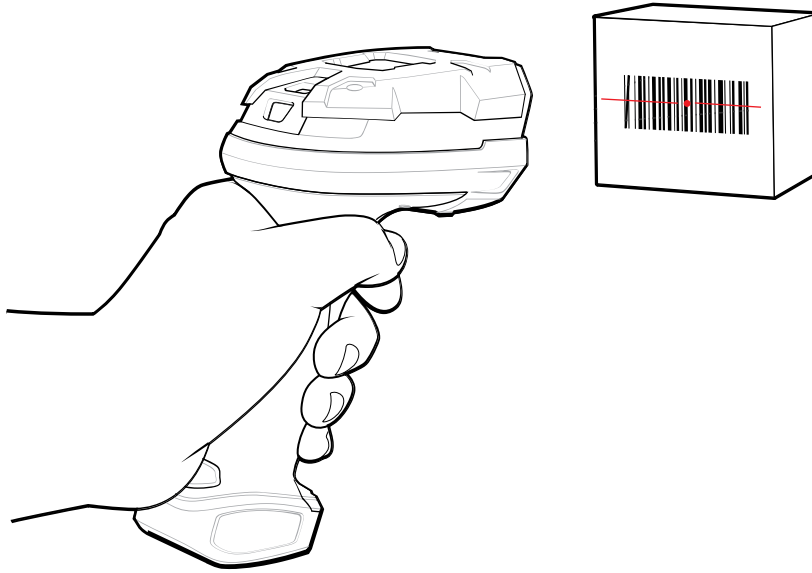


**NOTE:** To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the scanner to decode barcode data and display the barcode content.

To scan with the DS3678 scanner:

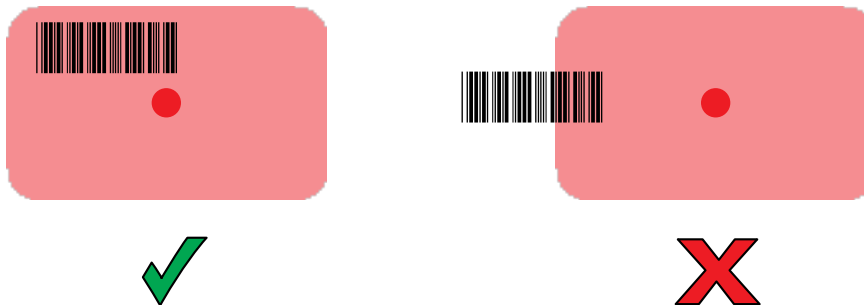
1. Pair the scanner with the device. See [Pairing Bluetooth Scanners](#) for more information.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).

3. Point the scanner at a barcode.



4. Press and hold the trigger.

Ensure the barcode is within the area formed by the aiming pattern. The aiming dot increases visibility in bright lighting conditions.

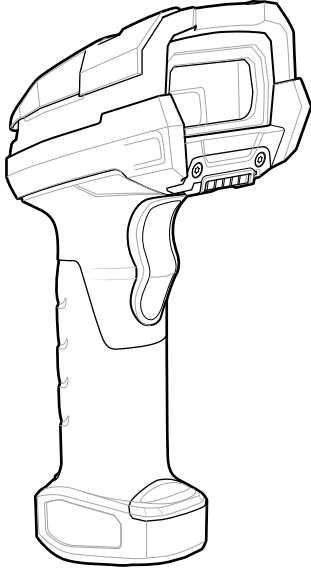


The captured data appears in the text field.

## Scanning with the LI3678 Linear Imager

Use the LI3678 linear imager to capture barcode data.

**Figure 42** LI3678 Bluetooth Scanner



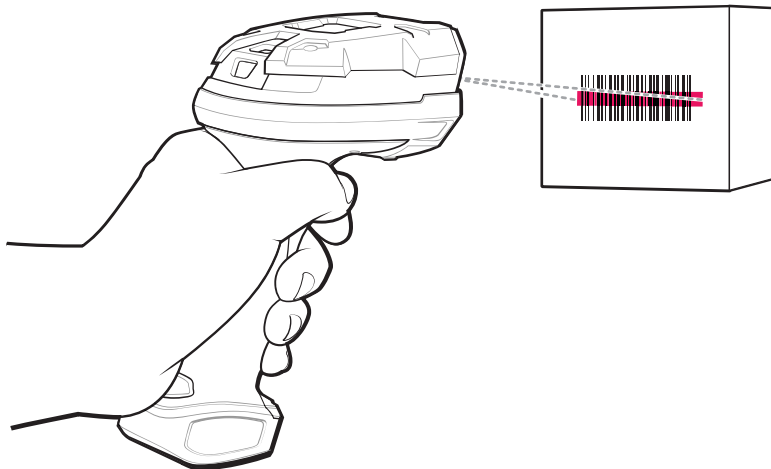
Refer to the LI3678 Product Reference Guide for more information.



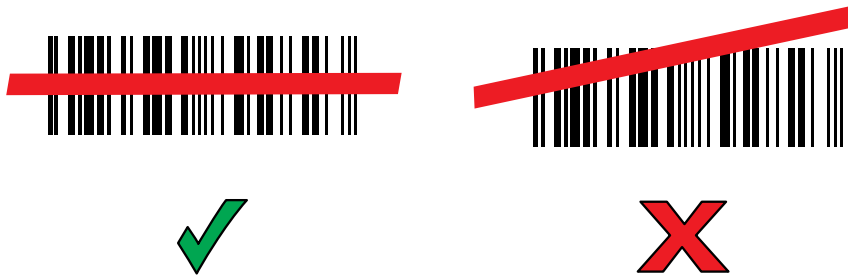
**NOTE:** To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the scanner to decode barcode data and display the barcode content.

To scan with the LI3678:

1. Pair the LI3678 with the device. See [Pairing a Bluetooth Scanner](#) for more information.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the LI3678 at a barcode.
4. Press and hold the trigger.



5. Ensure the aiming pattern covers the barcode.



Upon successful decode, the scanner beeps and the LED displays a single green flash.  
The captured data appears in the text field.

## Scanning with the DS2278 Digital Scanner

Use the DS2278 Digital Scanner to capture barcode data.

**Figure 43** DS2278 Digital Scanner



Refer to the DS2278 Digital Scanner Product Reference Guide for more information.

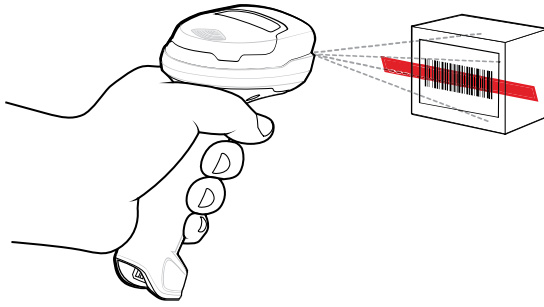


**NOTE:** To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the scanner to decode barcode data and display the barcode content.

To scan with the DS2278:

1. Pair the DS2278 with the device. See [Pairing a Bluetooth Scanner](#) for more information.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).

3. Point the scanner at a barcode.



4. Press and hold the trigger.
5. Ensure the aiming pattern covers the barcode.

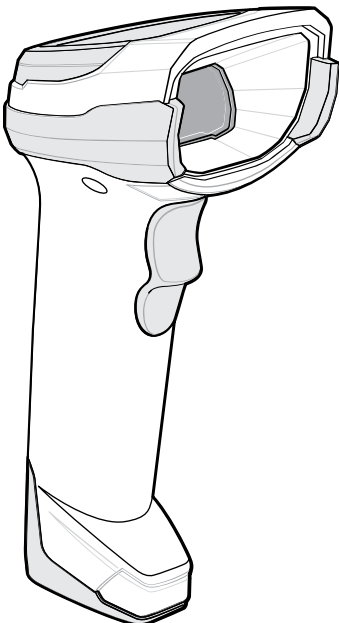


6. Upon successful decode, the scanner beeps and the LED flashes, and the scan line turns off.  
The captured data appears in the text field.

## Scanning with the DS8178 Digital Scanner

Use the DS8178 Bluetooth Scanner to capture barcode data.

**Figure 44** DS8178 Digital Scanner



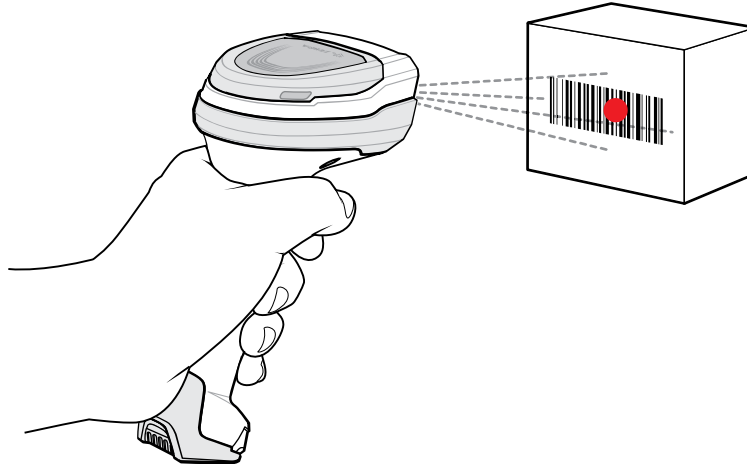
Refer to the DS8178 Digital Scanner Product Reference Guide for more information.



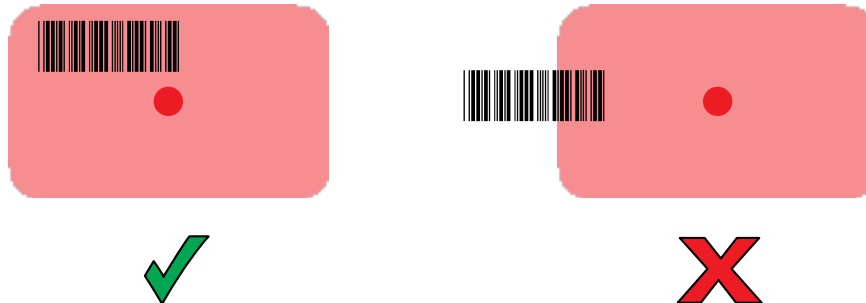
**NOTE:** To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows the user to enable the scanner to decode barcode data and display the barcode content.

To scan with the DS8178 scanner:

1. Pair the scanner with the device. See [Pairing Bluetooth Scanners](#) for more information.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the scanner at a barcode.



4. Press and hold the trigger.
5. Ensure the barcode is within the area formed by the aiming pattern. The aiming dot increases visibility in bright lighting conditions.



6. Upon successful decode, the scanner beeps and the LED flashes, and the scan line turns off. The captured data appears in the text field.

## Pairing a Bluetooth Ring Scanner

Before using a Bluetooth Ring Scanner with the device, connect the device to the Ring Scanner.

To connect the Ring Scanner to the device, use one of the following methods:

- Near Field Communication (NFC) (RS6000 only)



**NOTE:** Applicable to CC6000 only.

- Simple Serial Interface (SSI)
- Bluetooth Human Interface Device (HID) Mode

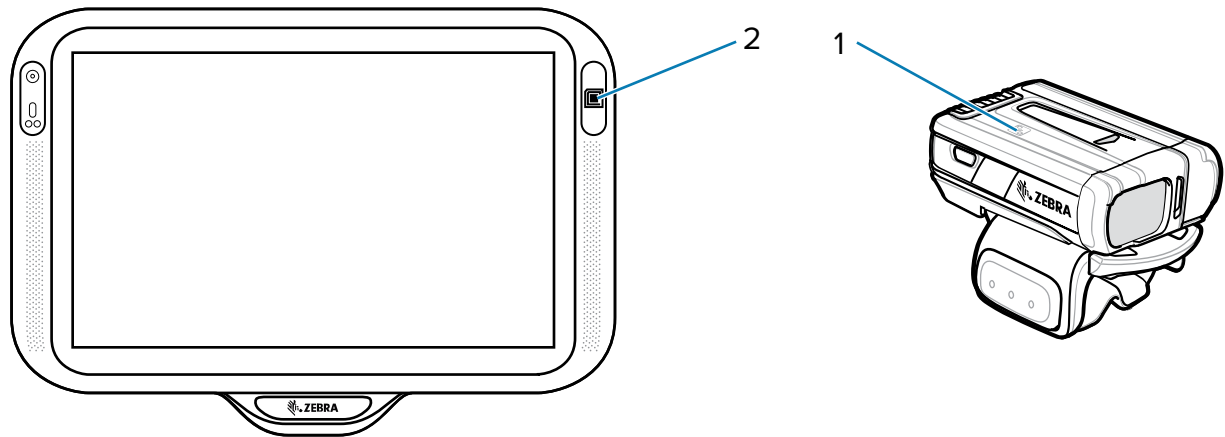
Pairing in SSI Mode Using Near Field Communication

The device provides the ability to pair the RS5100/6100 or RS6000 Ring Scanner in SSI Mode using NFC.



**NOTE:** Applicable to CC6000 with RS5100 or RS6000 only.


1. Ensure that NFC is enabled on the device.
2. Align the NFC icon on the Ring Scanner with the NFC icon on the back of the device.



1	NFC logo
2	NFC antenna

The Status LED blinks blue indicating that the Ring Scanner is attempting to establish a connection with the device. When a connection is established, the Status LED turns off and the Ring Scanner emits a single string of low/high beeps.

A notification appears on the device screen.

The  icon appears in the Status bar.

Pairing in HID Mode Using Near Field Communication

The device provides the ability to pair the RS5100/RS6100 or RS6000 Ring Scanner in HID Mode using NFC.

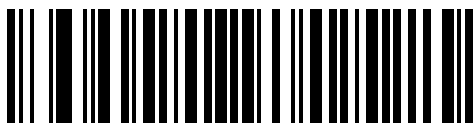


**NOTE:** Applicable to CC6000 with RS5100 and RS6000 imagers only.

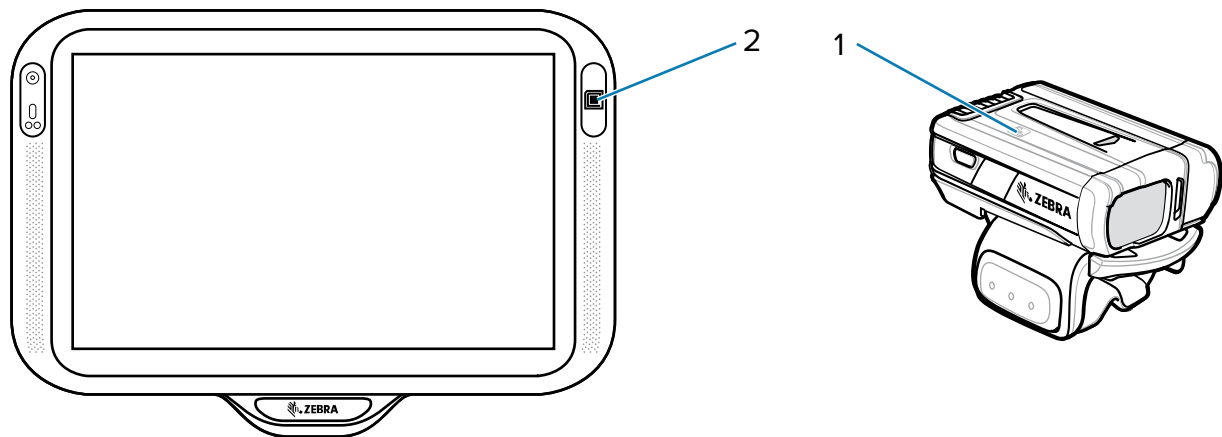
1. Ensure that NFC is enabled on the device.
2. Ensure that Bluetooth is enabled on both devices.
3. Ensure that the Bluetooth device to discover is in discoverable mode.
4. Ensure that the two devices are within 10 meters (32.8 feet) of one another.

- 5. Place the Ring Scanner in Human Interface Device (HID) mode. If the Ring Scanner is already in HID mode, skip to step 6.
  - a) Remove the battery from the Ring Scanner.
  - b) Press and hold the Restore key.
  - c) Install the battery onto the Ring Scanner.
  - d) Keep holding the Restore key for about five seconds until a chirp is heard and the Scan LEDs flash green.
  - e) Scan the barcode below to place the Ring Scanner in HID mode.

**Figure 45** Bluetooth HID Barcode



- 6. Remove the battery from the Ring Scanner.
- 7. Re-install the battery into the Ring Scanner.
- 8. Align the NFC icon on the Ring Scanner with the NFC icon on the device.



1	NFC logo
2	NFC antenna


The Status LED blinks blue indicating that the Ring Scanner is attempting to establish a connection with the device. When a connection is established, the Status LED turns off and the Ring Scanner emits a single string of low/high beeps.

A notification appears on the device screen.

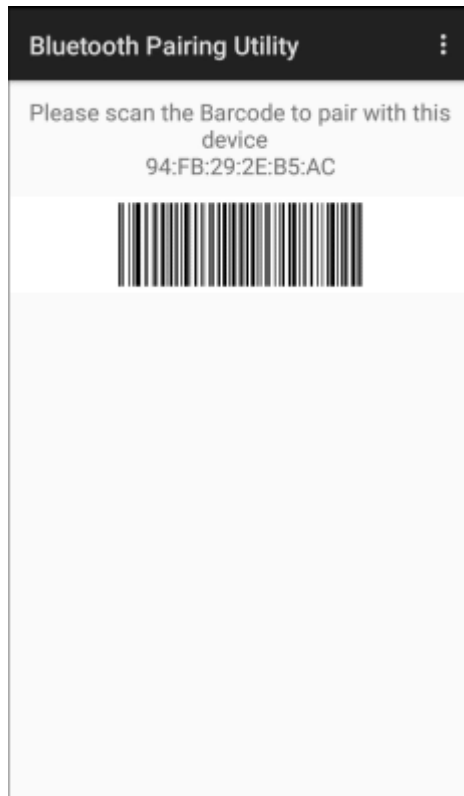
The **A** icon appears in the Status bar.

### Pairing Using Simple Serial Interface

Pair the Ring Scanner to the device using Simple Serial Interface.


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

**Figure 46** Bluetooth Pairing Utility



2. Using the Ring Scanner, scan the barcode on the screen.

The Ring Scanner emits a string of high/low/high/low beeps. The Scan LED flashes green indicating that the Ring Scanner is attempting to establish a connection with the device. When a connection is established, the Scan LED turns off and the Ring Scanner emits one string of low/high beeps.

A notification appears on the Notification panel and the  icon appears in the Status bar.

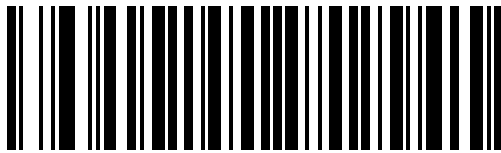
## Pairing Using Bluetooth Human Interface Device

Pair the Ring Scanner to the device using Human Interface Device (HID).

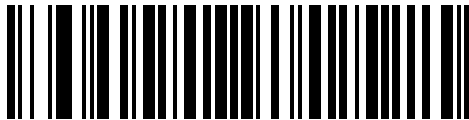
1. Ensure that Bluetooth is enabled on both devices.
2. Ensure that the Bluetooth device to discover is in discoverable mode.
3. Ensure that the two devices are within 10 m (32.8 ft) of one another.


4. Place the Ring Scanner in HID mode. If the Ring Scanner is already in HID mode, skip to step 5.
  - a) Remove the battery from the Ring Scanner.
  - b) Press and hold **Restore**.
  - c) Install the battery onto the Ring Scanner.
  - d) Keep holding the Restore key for about five seconds until a chirp is heard and the Scan LEDs flash green.
  - e) Scan the barcode below to place the Ring Scanner in HID mode.

**Figure 47** RS507 Bluetooth HID Barcode



**Figure 48** RS6000 Bluetooth HID Barcode



5. Remove the battery from the Ring Scanner.
6. Re-install the battery into the Ring Scanner.
7. Swipe down from the Status bar to open the Quick Access panel and then touch .
8. Touch **Bluetooth**.
9. Touch **Pair new device**. The device begins searching for discoverable Bluetooth devices in the area and displays them under **Available devices**.
10. Scroll through the list and select Ring Scanner.

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

A notification appears on the Notification panel and the  icon appears in the Status bar.

## Pairing a Bluetooth Scanner

Before using a Bluetooth scanner with the device, connect the device to the Bluetooth scanner.


Connect the scanner to the device using one of the following methods:

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

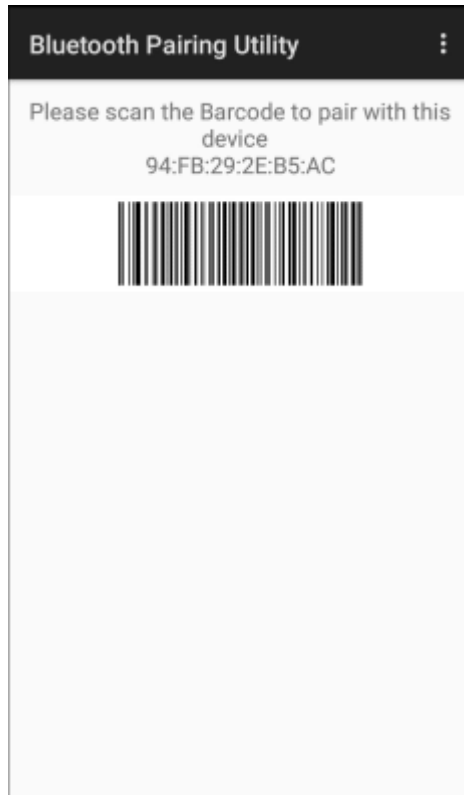
### Pairing Using Simple Serial Interface

Pair the Bluetooth scanner to the device using Simple Serial Interface (SSI).

1. Ensure that the two devices are within 10 meters (32.8 feet) of one another.

2. Install the battery into the scanner.
3. Swipe up from the bottom of the Home screen and touch .

**Figure 49** Bluetooth Pairing Utility



4. Using the Bluetooth scanner, scan the barcode on the screen.

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

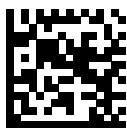
A notification appears on the Notification panel and the  icon appears in the Status bar.


## Pairing Using Bluetooth Human Interface Device

Pair the Bluetooth scanner to the device using HID.

To pair the scanner with the device using HID:

1. Remove the battery from the scanner.
2. Replace the battery.
3. After the scanner reboots, scan the barcode below to place the scanner in HID mode.



4. On the device, swipe down from the Status bar to open the Quick Access panel and then touch .
5. Touch **Bluetooth**.
6. Touch **Pair new device**. The device begins searching for discoverable Bluetooth devices in the area and displays them under **Available devices**.
7. Scroll through the list and select XXXXX xxxxxx, where XXXXX is the scanner and xxxxxx is the serial number.

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

## DataWedge

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

DataWedge allows any app on the device to get data from input sources such as a barcode scanner, MSR, RFID, voice, or serial port and manipulate the data based on options or rules.



Configure DataWedge to:

- Provide data capture services from any app.
- Use a particular scanner, reader, or other peripheral devices.
- Properly format and transmit data to a specific app.

To configure DataWedge, refer to [techdocs.zebra.com/datawedge/](https://techdocs.zebra.com/datawedge/).

## Enabling DataWedge



This procedure provides information on how to enable DataWedge on the device.

1. Swipe up from the bottom of the Home screen and touch .
2. Touch  > **Settings**.
3. Touch the **DataWedge enabled** checkbox.

A blue checkmark appears in the checkbox indicating that DataWedge is enabled.

## Disabling DataWedge

This procedure provides information on how to disable DataWedge on the device.

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

## Supported Decoders

This sections provides the supported decoders for each data capture option.

### SE2100 Internal Imager Supported Decoders

Lists the supported decoders for the SE2100 internal imager.

**Table 10** SE2100 Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	O	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	-O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	—	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, — = Not Supported

### SE4850-ER Internal Imager Supported Decoders

Lists the supported decoders for the SE4850-ER internal imager.

**Table 11** SE4850-ER Internal Imager Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O

**Table 11** SE4850-ER Internal Imager Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	O	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	O	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	X	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, - = Not Supported

## RS507/RS507x Supported Decoders

This section lists the supported decoders for the RS507/RS507x Ring Scanner.

**Table 12** RS507/RS507x Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	-	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	-	Trioptic 39	O

**Table 12** RS507/RS507x Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Code 128	X	GS1 QRCode	-	UK Postal	O
Code 39	O	HAN XIN	-	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	-	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, - = Not Supported

## RS6000 Supported Decoders

This section lists the supported decoders for the RS6000 Ring Scanner.

**Table 13** RS6000-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	O	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	O	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O

**Table 13** RS6000-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, - = Not Supported

## RS5100 Supported Decoders

This section lists the supported decoders for the RS5100 Ring Scanner.

**Table 14** RS5100-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	O	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	O	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, - = Not Supported

## DS2278 Supported Decoders

This section lists the supported decoders for the DS2278 Digital Scanner.

**Table 15** DS2278 Digital Scanner-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	—	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	O
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	—	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, — = Not Supported

## DS3678 Supported Decoders

This section lists the supported decoders for the DS3678 scanner.

**Table 16** DS3678-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	—	GS1 DataBar	X	QR Code	X

**Table 16** DS3678-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	—
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	O	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, — = Not Supported

## LI3678 Supported Decoders

This section lists the supported decoders for the LI3678 scanner.

**Table 17** LI3678-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	—	EAN8	X	MSI	O
Aztec	—	Grid Matrix	O	PDF417	—
Canadian Postal	—	GS1 DataBar	X	QR Code	—
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	—
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	—	Trioptic 39	O
Code 128	X	GS1 QRCode	—	UK Postal	—
Code 39	X	HAN XIN	O	UPCA	X

**Table 17** LI3678-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	—	Japanese Postal	—	UPCE1	O
Composite C	—	Korean 3 of 5	O	US4state	—
Discrete 2 of 5	O	MAIL MARK	—	US4state FICS	—
Datamatrix	—	Matrix 2 of 5	O	US Planet	—
Dutch Postal	—	Maxicode	—	US Postnet	—
DotCode	O	MicroPDF	—		
EAN13	X	MicroQR	—		

Key: X = Enabled, O = Disabled, — = Not Supported

## DS8178 Supported Decoders

This section lists the supported decoders for the DS8178 Digital scanner.

**Table 18** DS8178 Digital Scanner-Supported Decoders

Decoder	Default State	Decoder	Default State	Decoder	Default State
Australian Postal	O	EAN8	X	MSI	O
Aztec	X	Grid Matrix	O	PDF417	X
Canadian Postal	—	GS1 DataBar	X	QR Code	X
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	—
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	O	Trioptic 39	O
Code 128	X	GS1 QRCode	O	UK Postal	O
Code 39	X	HAN XIN	—	UPCA	X
Code 93	O	Interleaved 2 of 5	O	UPCE0	X
Composite AB	O	Japanese Postal	O	UPCE1	O
Composite C	O	Korean 3 of 5	O	US4state	O
Discrete 2 of 5	O	MAIL MARK	X	US4state FICS	O
Datamatrix	X	Matrix 2 of 5	O	US Planet	O
Dutch Postal	O	Maxicode	X	US Postnet	O

**Table 18** DS8178 Digital Scanner-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	O		

Key: X = Enabled, O = Disabled, — = Not Supported

# Wireless

This section provides information on the wireless features of the device.

The following wireless features are available on the device:

- Wireless Local Area Network (WLAN)
- Bluetooth
- Cast
- Near Field Communications (NFC)

## Wireless Local Area Networks

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

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

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

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **Wireless & networks** (Android 11 only) or **Network & internet** (Android 13 only) settings to configure the device to match the security scheme.

The device supports the following WLAN security options:

- None
- Enhanced Open
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)/WPA2 Personal (PSK)
- WPA3-Personal

- WPA/WPA2/WPA3 Enterprise (EAP) (Android 11 only)
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
  - Transport Layer Security (TLS)
  - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.
  - Password (PWD).
  - Lightweight Extensible Authentication Protocol (LEAP).
- WPA/WPA2-Enterprise (Android 13 only)
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
  - Transport Layer Security (TLS)
  - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP) with MSCHAP and MSCHAPv2 authentication, and GTC authentication.
  - Password (PWD).
  - Extensible Authentication Protocol Method for Subscriber Identity Module (SIM)
  - Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA)
  - Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA')
  - Lightweight Extensible Authentication Protocol (LEAP).
- WPA3-Enterprise 192-bit
- WPA3-Enterprise (Android 13 only)
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
  - Transport Layer Security (TLS)
  - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP) with MSCHAP and MSCHAPv2 authentication, and GTC authentication.
  - Password (PWD).
  - Extensible Authentication Protocol Method for Subscriber Identity Module (SIM)
  - Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA)
  - Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA')
  - Lightweight Extensible Authentication Protocol (LEAP).

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

## Connecting to a Wi-Fi Network

1. Go to **Settings**.
2. Touch **Network & internet**.
3. On Android 11, touch **Wi-Fi** to open the **Wi-Fi** screen. The device searches for WLANs in the area and lists them.
4. On Android 13, touch **Internet** to open the **Internet** screen. The device searches for WLANs in the area and lists them.
5. Scroll through the list and select the desired WLAN network.

- For open networks, touch the profile once or press and hold and then select **Connect** or for secure networks, enter the required password or other credentials, then touch **Connect**. See the system administrator for more information.



The device obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the device with a fixed internet protocol (IP) address, see [Configuring the Device to Use a Static IP Address](#) on page 104.

- In the Wi-Fi setting field, **Connected** appears, indicating that the device is connected to the WLAN.

## Wi-Fi Version

When the device is connected to a Wi-Fi network, the Wi-Fi icon on the Status bar indicates the Wi-Fi network version.

**Table 19** Wi-Fi Version Icons

Icon	Description
	Connected to Wi-Fi 5, the 802.11ac standard.
	Connected to Wi-Fi 4, the 802.11n standard.

## Removing a Wi-Fi Network

Remove a remembered or connected Wi-Fi network.

- Go to **Settings**.
- Touch **Network & Internet**.
- On Android 11, touch **Wi-Fi**.
- On Android 13, touch **Internet**.
- Scroll down to the bottom of the list and touch **Saved networks**.
- Touch the name of the network.
- Touch **FORGET**.

## WLAN Configuration

This section provides information on configuring Wi-Fi settings.

### Configuring a Secure Wi-Fi Network

- Go to **Settings**.
- Touch **Network & Internet**.
- On Android 11, touch **Wi-Fi**.
- On Android 13, touch **Internet**.
- Slide the switch to the **ON** position.

6. The device searches for WLANs in the area and lists them on the screen.
7. Scroll through the list and select the desired WLAN network.
8. Touch the desired network. If network security is **Open**, the device automatically connects to the network. For all other network security, a dialog box appears.
9. If network security is **WPA/WPA2-Personal**, **WPA3-Personal**, or **WEP**, enter the required password and then touch **Connect**.
10. If network security is **WPA/WPA2/WPA3 Enterprise**:
  - a) Touch the **EAP method** drop-down list and select one of the following:
    - **PEAP**
    - **TLS**
    - **TTLS**
    - **PWD**
    - **LEAP**
  - b) Fill in the appropriate information. Options vary depending on the **EAP method** chosen.
    - When selecting **CA certificate**, Certification Authority (CA) certificates are installed using the **Security** settings.
    - When using the EAP methods PEAP, TLS, or TTLS, specify a domain.
    - Touch **Advanced options** to display additional network options.
11. If the network security is **WPA3-Enterprise 192-bit**:
  - Touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the Security settings.
  - Touch **User certificate** and select a user certificate. Note: User certificates are installed using the Security settings.
  - In the **Identity** text box, enter the username credentials.



**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 104 for setting the connection to a proxy server and see [Configuring the Device to Use a Static IP Address](#) on page 104 for setting the device to use a static IP address.

12. Touch **Connect**.

## 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. Go to **Settings**.
2. Touch **Network & Internet**.
3. On Android 11, touch **Wi-Fi**.
4. On Android 13, touch **Internet**.
5. Slide the Wi-Fi switch to the **On** position.
6. Scroll to the bottom of the list and select **Add network**.

7. In the **Network name** text box, enter the name of the Wi-Fi network.
8. In the **Security** drop-down list, set the type of security to:
  - **None**
  - **Enhanced Open**
  - **WEP**
  - **WPA/WPA2-Personal**
  - **WPA3-Personal**
  - **WPA/WPA2/WPA3-Enterprise** (Android 11 only)
  - **WPA/WPA2-Enterprise** (Android 13 only)
  - **WPA3-Enterprise** (Android 13 only)
  - **WPA3-Enterprise 192-bit**
9. If the network security is **None** or **Enhanced Open**, touch **Save**.
10. If the network security is **WEP**, **WPA3-Personal**, or **WPA/WPA2-Personal**, enter the required password and then touch **Save**.
11. If network security is **WPA/WPA2/WPA3 Enterprise**:
  - a) Touch the **EAP method** drop-down list and select one of the following:
    - **PEAP**
    - **TLS**
    - **TTLS**
    - **PWD**
    - **SIM**
    - **AKA**
    - **AKA'**
    - **LEAP**
  - b) Fill in the appropriate information. Options vary depending on the **EAP method** chosen.
    - When selecting **CA certificate**, Certification Authority (CA) certificates are installed using the **Security** settings.
    - When using the EAP methods PEAP, TLS, or TTLS, specify a domain.
    - Touch **Advanced options** to display additional network options.
12. If the network security is **WPA3-Enterprise 192-bit**:
  - You must specify a domain and user certificate
  - Certification Authority (CA) and User certificates are installed using the **Security** settings.
  - Touch **Advanced options** to display additional network options.




**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 104 for setting the connection to a proxy server and see [Configuring the Device to Use a Static IP Address](#) on page 104 for setting the device to use a static IP address.

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

## 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.

1. Go to **Settings**.
2. Touch **Network & Internet**.
3. On Android 11, touch **Wi-Fi**.
4. On Android 13, touch **Internet**.
5. Slide the Wi-Fi switch to the **On** position.
6. In the network dialog box, select and touch a network.
7. If configuring the connected network, touch  to edit the network details and then touch the down arrow to hide the keyboard.
8. Touch **Advanced options**.
9. Touch **Proxy** and select **Manual**.
10. In the **Proxy hostname** text box, enter the address of the proxy server.
11. In the **Proxy port** text box, enter the port number for the proxy server.
12. 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.
13. If configuring the connected network, touch **Save** otherwise, touch **Connect**.
14. Touch **Connect**.

## 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.

1. Go to **Settings**.
2. Touch **Network & Internet**.
3. On Android 11, touch **Wi-Fi**.
4. On Android 13, touch **Internet**.
5. Slide the Wi-Fi switch to the **On** position.

6. In the network dialog box, select and touch a network.
7. If configuring the connected network, touch  to edit the network details and then touch the down arrow to hide the keyboard.
8. Touch **Advanced options**.
9. Touch **IP settings** and select **Static**.
10. In the **IP address** text box, enter an IP address for the device.
11. If required, in the **Gateway** text box, enter a gateway address for the device.
12. If required, in the **Network prefix length** text box, enter the prefix length.
13. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
14. If required, in the **DNS 2** text box, enter a DNS address.
15. If configuring the connected network, touch **Save** otherwise, touch **Connect**.

## 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 on Android 11 or Network preference on Android 13.

- **Turn on Wi-Fi automatically** - When enabled, Wi-Fi automatically turns back on when near high-quality saved networks.
- **Open network notification** (Android 11 only) or **Notify for public networks** (Android 13 only) - When enabled, notifies the user when an open network is available.
- **Advanced** - Touch to expand options. (Android 11 only)
  - **Additional settings** - Touch to view additional Wi-Fi 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. (Android 11 only)
  - **Wi-Fi Direct** - Displays a list of devices available for a direct Wi-Fi connection.

## Additional Wi-Fi Settings

Use the Additional Settings to configure additional Wi-Fi settings.



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

- **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**
  - **Logging** – Touch to enable advanced logging or change the log directory. (Android 11 only)
  - **Advanced Logging** - Touch to enable logging, enable **Wi-Fi Verbose Logging**, or change the log directory (Android 13 only).
  - **Wireless logs**
    - **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 version information. Touch the version to display addition version details.

## Wi-Fi Direct

1. Go to **Settings**.
  2. Touch **Network & Internet**.
  3. On Android 11, touch **Wi-Fi**.
  4. On Android 13, touch **Internet**.
  5. Slide the **Wi-Fi** switch to the **On** position.
  6. In the network dialog box, select and touch a network.
  7. On Android 11, scroll down to the bottom of the screen and touch **Wi-Fi preferences > Advanced > Wi-Fi Direct**. The device begins searching for another Wi-Fi Direct device.
  8. On Android 13, scroll down to the bottom of the screen and touch **Network preferences > Wi-Fi Direct**. The device begins searching for another Wi-Fi Direct device.
  9. Under **Peer devices**, touch the other device name.
  10. On the other device, select **Accept**.
- Connected** appears on the device. On both devices, in their respective Wi-Fi Direct screens, the other device name appears in the list.

## Bluetooth

Bluetooth devices can communicate without wires, using frequency-hopping spread spectrum (FHSS) radio frequency (RF) to transmit and receive data in the 2.4 GHz Industry Scientific and Medical (ISM)

band (802.15.1). Bluetooth wireless technology is specifically designed for short-range (10 m (32.8 ft)) communication and low power consumption.

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

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

## Adaptive Frequency Hopping

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

AFH for Bluetooth consists of four main sections:

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

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

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



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

## Security

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

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

Recommendations are:

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

## Bluetooth Profiles

The device supports the Bluetooth services listed.

**Table 20** Bluetooth Profiles

Profile	Description
Service Discovery Protocol (SDP)	Handles the search for known and specific services as well as general services.
Serial Port Profile (SPP)	Allows use of RFCOMM protocol to emulate serial cable connection between two Bluetooth peer devices. For example, connecting the device to a printer.
Object Push Profile (OPP)	Allows the device to push and pull objects to and from a push server.
Advanced Audio Distribution Profile (A2DP)	Allows the device to stream stereo-quality audio to a wireless headset or wireless stereo speakers.
Audio/Video Remote Control Profile (AVRCP)	Allows the device to control A/V equipment to which a user has access. It may be used in concert with A2DP.
Personal Area Network (PAN)	Allows the use of Bluetooth Network Encapsulation Protocol to provide L3 networking capabilities over a Bluetooth link. Only PANU role is supported.
Human Interface Device Profile (HID)	Allows Bluetooth keyboards, pointing devices, gaming devices and remote monitoring devices to connect to the device.
Headset Profile (HSP)	Allows a hands-free device, such as a Bluetooth headset, to place and receive calls on the device.
Hands-Free Profile (HFP)	Allows car hands-free kits to communicate with the device in the car.
Phone Book Access Profile (PBAP)	Allows exchange of Phone Book Objects between a car kit and a mobile device to allow the car kit to display the name of the incoming caller; allow the car kit to download the phone book so you can initiate a call from the car display.
Out of Band (OOB)	Allows exchange of information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. Using OOB with NFC enables pairing when devices simply get close, rather than requiring a lengthy discovery process.
Symbol Serial Interface (SSI)	Allows for communication with Bluetooth Imager.

**Table 20** Bluetooth Profiles (Continued)

Profile	Description
File Transfer Profile (FTP)	Provides the capability to browse, manipulate and transfer files in file system of another system. Uses GOEP as a basis.
Generic Attribute Profile (GATT)	Provides profile discovery and description services for Bluetooth Low Energy protocol. It defines how attributes are grouped together into sets to form services.
HID Over GATT Profile (HOGP)	Defines the procedures and features used by Bluetooth low energy HID Devices using GATT and Bluetooth HID Hosts using GATT.
Scan Parameters Profile (ScPP)	Provides devices with information to assist them in managing their connection idle timeout and advertising parameters to optimize for power consumption and/or reconnection latency.
Dial Up Networking (DUN)	Provides a standard to access the Internet and other dial-up services over Bluetooth.
Generic Access Profile (GAP)	Use for device discovery and authentication.
OBject EXchange (OBEX)	Facilitates the exchange of binary objects between devices.

## Bluetooth Power States

The Bluetooth radio is off by default.


- **Suspend** - When the device goes into Sleep mode, the Bluetooth radio stays on.
- **Airplane Mode** -
  - Android A10 OS version and previous versions - When the device is placed in Airplane Mode, the Bluetooth radio turns off. When Airplane mode is disabled, the Bluetooth radio returns to the prior state. When in Airplane Mode, the Bluetooth radio can be turned back on if desired.
  - Android A11 OS version and versions onward - When the device is placed in Airplane Mode, the Bluetooth radio is not turned off when the device is connected to a Bluetooth headset or hearing device.
- **Airplane Mode** - When the device is placed in Airplane Mode, the Bluetooth radio is not turned off when the device is connected to a Bluetooth headset or hearing device.

## Bluetooth Radio Power


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

### Enabling Bluetooth

1. Swipe down from the Status bar to open the Notification panel.

2. Touch  to turn Bluetooth on.

### Disabling Bluetooth

1. Swipe down from the Status bar to open the Notification panel.
2. Touch  to turn Bluetooth off.

### Discovering Bluetooth Device(s)

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

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

### Changing the Bluetooth Name

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

1. Go to **Settings**.
2. Touch **Connected devices** > **Connection preferences** > **Bluetooth**.
3. If Bluetooth is not on, move the switch to turn Bluetooth on.
4. Touch **Device name**.
5. Enter a name and touch **RENAME**.

### Connecting to a Bluetooth Device

Once paired, connect to a Bluetooth device.

1. Go to **Settings**.
2. Touch **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the list, touch the unconnected Bluetooth device.

When connected, **Connected** appears below the device name.

## Selecting Profiles on the Bluetooth Device

Some Bluetooth devices have multiple profiles.

1. Go to **Settings**.
2. Touch **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the **Paired Devices** list, touch  next to the device name.
4. Turn on or off a profile to allow the device to use that profile.


## Unpairing a Bluetooth Device

Unpairing a Bluetooth device erases all pairing information.

1. Go to **Settings**.
2. Touch **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the **Paired Devices** list, touch  next to the device name.
4. Touch **FORGET**.

## Cast

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

1. Go to **Settings**.
2. Touch **Connected devices** > **Connection preferences** > **Cast**.
3. Touch  > **Enable wireless display**.

The device searches for nearby Miracast devices and lists them.

4. Touch a device to begin casting.

## Near Field Communications

NFC/HF RFID is a short-range wireless connectivity technology standard that enables a secure transaction between a reader and a contactless smart card.



**NOTE:** Applicable to CC6000 only.

The technology is based on ISO/IEC 14443 type A and B (proximity), ISO/IEC 15693 (vicinity), and FeliCa standards, using the HF 13.56 MHz unlicensed band.

The device supports the following operating modes:

- Reader mode
- Card Emulation mode.

Using NFC, the device can:

- Read contactless cards, such as contactless tickets, ID cards, and ePassport.
- Read and write information to contactless cards, such as SmartPosters and tickets, as well as devices with an NFC interface, such as vending machines.

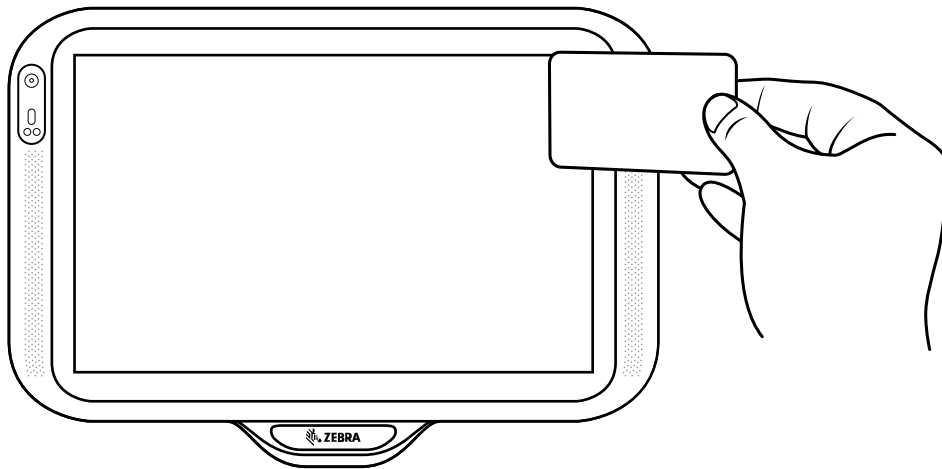
- Read information from supported medical sensors.
- Pair with supported Bluetooth devices such as printers, ring scanners (for example, RS6000), and headsets (for example, HS3100).
- Exchange data with another NFC device.
- Emulate contactless cards such as a payment, ticket, or SmartPoster.

The device's NFC antenna is positioned to read NFC cards from the top of the device while the device is being held.

## Reading NFC Cards

Read contactless cards using NFC.

**Figure 50** Reading Cards



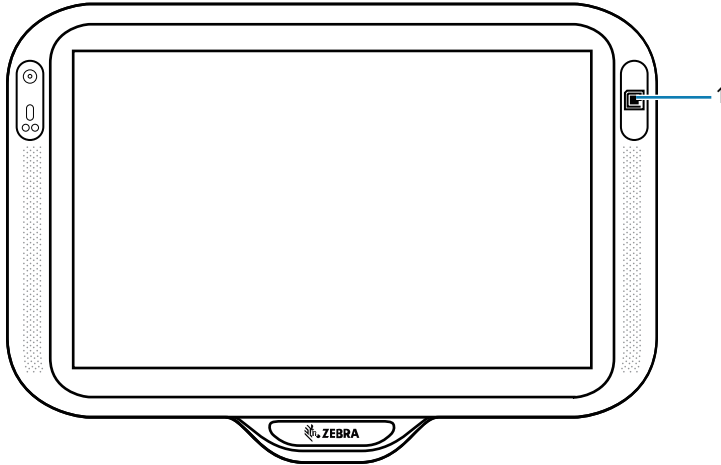
1. Launch an NFC-enabled application.
2. Move the device close to the NFC card until it detects the card.
3. Hold the card steadily until the transaction is complete (usually indicated by the application).

## Sharing Information Using NFC

You can beam content like a web page, contact cards, pictures, YouTube links, or location information from your screen to another device by bringing the devices together back to back.

Make sure both devices are unlocked, support NFC, and have both NFC and Android Beam turned on.

1. Open a screen that contains a web page, video, photo, or contact.
2. Align the NFC logo on the device with the NFC antenna on the other device.



1	NFC antenna
---	-------------

3. Touch anywhere on the screen.

The transfer begins.

## Sharing Information Using NFC

You can beam content like a web page, contact cards, pictures, YouTube links, or location information from your screen to another device by bringing the devices together back to back.

Make sure both devices are unlocked, support NFC, and have both NFC and Android Beam turned on.

1. Open a screen that contains a web page, video, photo, or contact.
2. Move the back of the device toward the back of the other device.
3. Align the NFC logo on the device with the NFC antenna on the other device.
4. Move the front of the device toward the front of the other device.

When the devices connect, a sound emits, the image on the screen reduces in size, and the message **Touch to beam** displays.

5. Touch anywhere on the screen.

The transfer begins.

## Enterprise NFC Settings

Improve NFC performance or increase battery life by selecting which NFC features to use on the device.

- **Card Detection Mode** - Select a card detection mode.
  - **Low** - Increases battery life by lowering the NFC detection speed.
  - **Hybrid** - Provides a balance between NFC detection speed and battery life (default).
  - **Standard** - Provides the optimal NFC detection speed, but reduces battery life.

- **Supported Card Technology** - Select an option to detect only one NFC tag type, increasing battery life, but reducing detection speed.
  - **All (Default)** - Detects all NFC tag types.
  - **All (Default)** - Detects all NFC tag types. This provides the best detection speed, but reduces battery life.
  - **ISO 14443 Type A**
  - **ISO 14443 Type B**
  - **FeliCa**
  - **ISO 15693**
- **NFC Debug Logging** - Use to enable or disable debug logging for NFC.
- **Other NFC settings available with Zebra administrator tools (CSP)** - Allows configuration of additional Enterprise NFC Settings through staging tools and Mobile Device Management (MDM) solutions with an MX version that supports the Enterprise NFC Settings Configuration Service Provider (CSP). For more information on using the Enterprise NFC Settings CSP, refer to: [techdocs.zebra.com](https://techdocs.zebra.com).

# Accessories

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

## Device Accessories

This table lists the accessories available for the device.

**Table 21** Accessories

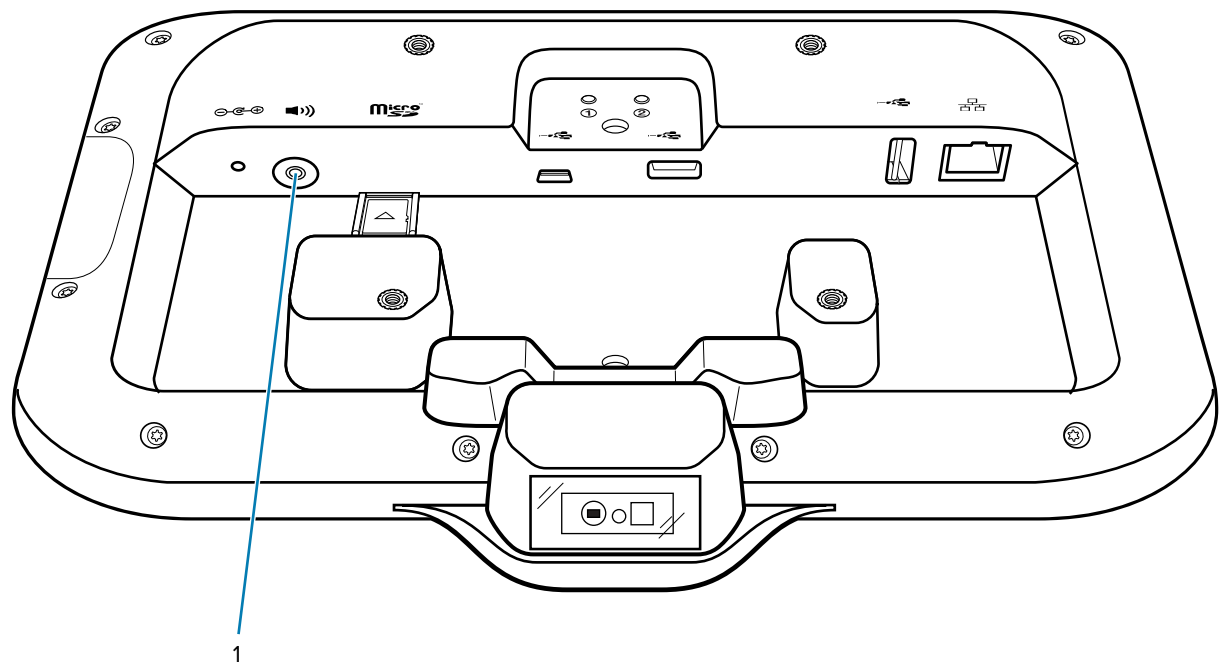
Accessory	Part Number	Description
<b>Mounting Plates</b>		
CC600 Wall Mount	21-118517-01R	CC600 Wall Mounting Kit
CC600 Pole Mount	21-118517-02R	CC600 Pole Mounting Kit
CC6000 Wall Mounting Kit	KT-152097-03	CC6000 Wall Mounting Kit with Power Supply Storage
CC6000 Wall Mounting Kit	KT-152097-01	100 mm VESA
CC6000 Wall Mounting Kit	KT-152098-03	Slimmer, CC6000 specific mount
CC6000 Pole Mounting Kit	KT-152096-0	100 mm 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	100 mm VESA
<b>Communication Cables</b>		
USB-C Cable	CBL-TC2X-USBC-01	Used to communicate with the device via the USB OTG port.
USB-C Cable	CBL-TC5X-USBC2A-01	Used to communicate with the device via the USB OTG port.
<b>Power Supplies</b>		
DC Line Cord	CBL-DC-383A1-01	Used with Power Supply (PWR-BUA5V16W0WW) The cable length is 6 ft.

**Table 21** Accessories (Continued)

Accessory	Part Number	Description
Power Supply	PWR-BUA5V16W0WW	100-240 VAC, 5.4 V, 3 A, 16 W 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

## Headset (CC6000 Only)

Connect the 3.5 mm connector plug of the headset to the 3.5 mm audio port.

**Figure 51** CC6000 Audio Port

1	Audio port
---	------------

## USB cable

The USB cable plugs into the port at the back of the device. When attached to the device the cable allows transferring data to a host computer and connecting USB peripherals.

1. Connect the USB cable to the device.
2. Connect the USB connector of the cable to a host computer.

# Application Deployment

This section provides steps on device security, app development, and app management. It also provides instructions for installing apps and updating the device software.



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

## Android 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

If required by the VPN or Wi-Fi network, install a secure certificate on the device.

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory.
2. Go to **Settings**.
3. Touch **Security > Encryption & credentials**.

4. Touch **Install a certificate** and select one of the following:
  - **CA certificate**
  - **VPN & app user certification**
  - **Wi-Fi certificate.**
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**.

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

Configure credential storage from the device settings.

1. Go to **Settings**.
2. Touch **Security > Encryption & credentials**.
3. Select an option.
  - Touch **Trusted credentials** to display the trusted system and user credentials.
  - Touch **User credentials** to display user credentials.
  - Touch **Install a certificate** to install a secure certificate from the internal storage.
  - Touch **Clear credentials** to delete all secure certificates and related credentials.

## Android Development Tools

Development tools for Android include Android Studio, EMDK for Android, and StageNow.

### Android Development Workstation

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

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

Applications are written in Java or Kotlin, but compiled and executed in the Dalvik virtual machine. Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

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

### Enabling Developer Options

The **Developer options** screen sets development-related settings. By default, the Developer Options are hidden.

1. Go to **Settings**.
2. Touch **About phone**.
3. Scroll down to **Build number**.
4. Tap **Build number** seven times.  
The message **You are now a developer!** appears.
5. Touch **Back**.
6. On Android 11, touch **System > Advanced > Developer options**.
7. On Android 13, touch **System > Developer options**.
8. Slide the **USB debugging** switch to the **ON** position.

### EMDK for Android

EMDK for Android provides developers with tools to create business applications for enterprise mobile devices. It is designed for use with Google's Android Studio and includes Android class libraries such as Barcode, sample applications with source code, and the associated documentation.

EMDK for Android allows applications to take full advantage of the capabilities that Zebra devices have to offer. It embeds Profile Manager technology within Android Studio IDE, providing a GUI-based development tool designed specifically for Zebra devices. This allows fewer lines of code, resulting in reduced development time, effort, and errors.

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

### StageNow for Android

StageNow is Zebra's next-generation Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a 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](https://techdocs.zebra.com).

## GMS Restricted

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

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

For more information on StageNow, go to [techdocs.zebra.com](https://techdocs.zebra.com).

## ADB USB Setup

To use the ADB, install the development SDK on the host computer then install the ADB and USB drivers.

Before installing the USB driver, make sure that the development SDK is installed on the host computer. Go to [developer.android.com/sdk/index.html](https://developer.android.com/sdk/index.html) for details on setting up the development SDK.

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

## Enabling USB Debugging

By default, USB debugging is disabled.

1. Go to **Settings**.
2. Touch **About phone**.
3. Scroll down to **Build number**.
4. Tap **Build number** seven times.  
The message **You are now a developer!** appears.
5. Touch **Back**.
6. On Android 11, touch **System > Advanced > Developer options**.
7. On Android 13, touch **System > Developer options**.
8. Slide the **USB debugging** switch to the **ON** position.
9. Touch **OK**.
10. Connect the device to the host computer using the USB Cable.

The **Allow USB debugging?** dialog box appears on the device.

If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.

11. Touch **OK** or **Allow**.
12. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.

13. Type `adb devices`.

The following displays:

```
List of devices attached      XXXXXXXXXXXXXXXXXX device
```

Where XXXXXXXXXXXXXXXXXX is the device number.



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

14. Return to the Home screen.

## Entering Android Recovery Manually

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

1. Press and hold the Reset button until the Restart option appears. Release the Reset button when the option appears. The device restarts if the button is held down for longer than 3 seconds.
2. Touch **Restart**.
3. Press and hold the Number 1 button.

The System Recovery screen appears.

## Application Installation Methods


After an application is developed, install the application onto the device using one of the supported methods.

- USB connection
- Android Debug Bridge
- Wireless Android Debug Bridge
- microSD Card
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

## Installing Applications Using the USB Connection

Use the USB connection to install applications onto the device.

1. Connect the device to a host computer using the USB cable.
2. On the device, pull down the Notification panel and touch **Connect this device via USB**.  
By default, **No data transfer** is selected.
3. Touch **File Transfer**.
4. On the host computer, open a file explorer application.
5. On the host computer, copy the application APK file from the host computer to the device.
6. Disconnect the device from the host computer.

7. Swipe the screen up and select  to view files on the microSD card or Internal Storage.
8. Locate the application APK file.
9. Touch the application file.
10. Touch **Continue** to install the app or **Cancel** to stop the installation.
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 applications onto the device.

1. Ensure that the ADB drivers are installed on the host computer.
2. Connect the device to a host computer using a USB cable.
3. Go to **Settings**.
4. On Android 11, touch **System > Advanced > Developer options**.
5. On Android 13, touch **System > Developer options**.
6. Slide the **USB debugging** switch to the **ON** position.
7. Touch **OK**.
8. If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.
9. Touch **OK** or **Allow**.
10. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
11. Type `adb install <application>`.  
where: <application> = the path and filename of the apk file.
12. Disconnect the device from the host computer.

### Installing Applications Using Wireless ADB

Use ADB commands to install an application onto the device.

Go to the Zebra Support & Downloads web site at [zebra.com/support](https://zebra.com/support) and download the appropriate file to a host computer.



**IMPORTANT:** Note the following:

- Ensure that the latest adb files are installed on the host computer.
  - The device and the host computer must be on the same wireless network.
1. Go to **Settings**.
  2. On Android 11, touch **System > Advanced > Developer options**.

3. On Android 13, touch **System > Developer options**.



**IMPORTANT:** If **Developer options** does not appear in the advanced system settings on your device, perform the steps in [Enabling Developer Options](#) on page 119.

4. Slide the **USB debugging** switch to the **ON** position.
5. At the prompt, tap **OK**.
6. Slide the **Wireless debugging** switch to the **ON** position.
  - a) If the device and host computer are connected for the first time, the **Allow wireless debugging on this network?** dialog box with the **Always allow on this network** check box displays. Select the check box, if required.
  - b) Touch **ALLOW**.
7. Touch **Wireless debugging**.  
The **Wireless debugging** screen displays.
8. Note the IP address and Port on the **Wireless debugging** screen.
9. Touch **Pair device with pairing code**.  
The **Pair with device** dialog box displays.
10. Note the Port on the **Pair with device** dialog box. It will be different than the one on the **Wireless debugging** screen. The IP address will be the same.
11. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
12. Type `adb pair XX.XX.XX.XX:XXXXXX`  
where `XX.XX.XX.XX:XXXXXX` is the IP address and port number from the **Pair with device** dialog box.
13. Press **Enter**.
14. Type the pairing code from the **Pair with device** dialog box.
15. Press **Enter**.
16. Type `adb connect XX.XX.XX.XX:XXXXXX`  
where `XX.XX.XX.XX:XXXXXX` is the IP address and port number from the **Wireless debugging** screen.
17. Press **Enter**.  
The device is now connected to the host computer.
18. Type `adb devices`.  
The following displays:

```
List of devices attached      XXXXXXXXXXXXXXXXXX device
```

Where XXXXXXXXXXXXXXXXXX is the device number.



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

19. Press **Enter**.
20. Type `adb install <file>`.  
where `<file>` = the path and filename of the apk file.

21. Press **Enter**.
22. On the host computer, type:  



```
adb disconnect.
```
23. Press **Enter**.

## Installing Applications Using a microSD Card

Use a microSD card to install applications on your device.



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

1. Copy the APK file to the root of the microSD card.
  - Copy the APK file to a microSD card using a host computer (see [USB Communication](#) for more information), and then install the microSD card into the device (see [Installing a microSD Card \(Optional\)](#) on page 26 for more information).
  - Connect the device with a microSD card already installed to the host computer, and copy the .apk file to the microSD card. See [USB Communication](#) for more information. Disconnect the device from the host computer.
2. Swipe the screen up and select  to view files on the microSD card.
3. Touch  **SD card**.
4. Locate the application APK file.
5. Touch the application file.
6. Touch **Continue** to install the app or **Cancel** to stop the installation.
7. To confirm installation and accept what the application affects, touch **Install**. Otherwise, touch **Cancel**.
8. Touch **Open** to open the application or **Done** to exit the installation process.

The application appears in the App list.

## Uninstalling an Application

Free up device memory by removing unused apps.

1. Go to **Settings**.
2. On Android 11, touch **Apps & notifications**.
3. On Android 13, touch **Apps**.
4. Touch **See all apps** to view all apps in the list.
5. Scroll through the list to the app.
6. Touch the app.  
 The **App info** screen displays.
7. Touch **Uninstall**.
8. Touch **OK** to confirm.

## Android 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 website. Perform a system update using either a microSD card or using ADB.

### Performing a System Update Using microSD Card

It is strongly recommended that, prior to use, you format the microSD card on the device.

Go to the Zebra Support & Downloads website at [zebra.com/support](https://zebra.com/support) and download the appropriate System Update package to a host computer.

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 install the microSD card into the device. See Getting Started for information on installing the microSD card.
  - Connect the device (with a microSD card already installed) to the host computer, copy the ZIP file to the microSD card, and then 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 restarts if the button is held down for longer than 3 seconds.

3. Touch **Restart**.

4. Press and hold the Number 1 button.

The System Recovery screen appears.

5. Press the Number 2 button to navigate to **Apply upgrade from SD card**.

6. Press the Number 1 button to select.

7. Press 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.

### Performing a System Update Using ADB

Use ADB to perform a system update.

Go to the Zebra Support & Downloads web site at [zebra.com/support](https://zebra.com/support) and download the appropriate System Update package to a host computer.

1. Connect the device to a host computer using a USB cable.
2. Go to **Settings**.
3. On Android 11, touch **System > Advanced > Developer options**.
4. On Android 13, touch **System > Developer options**.
5. If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.
6. Touch **OK** or **Allow**.

7. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
8. Type `adb devices`.



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

9. Type `adb reboot recovery`.
10. Press **Enter**.  
The System Recovery screen appears on the device.
11. Press the Number 2 button to navigate to **Apply upgrade from ADB**.
12. Press the Number 1 button to select.
13. On the host computer command prompt window type `adb sideload <file>`.  
where: <file> = the path and filename of the zip file.
14. Press **Enter**.  
The System Update installs (progress appears as a percentage in the Command Prompt window) and then the System Recovery screen appears on the device.
15. Press the Number 1 button to reboot the device.
16. Disconnect the USB cable from the device.

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

## Verifying System Update Installation

Verify that the system update was successful.

1. Go to **Settings**.
2. Touch **About phone**.
3. Scroll down to **Build number**.
4. Ensure that the build number matches the new system update package file number.

## Android Enterprise Reset

An Enterprise Reset erases all user data in the /data partition, including data in the primary storage locations (/sdcard and emulated storage), while preserving the contents of the /enterprise folder and its subfolders. The contents of the /enterprise folder and its subfolders are preserved. Zebra distributes the Enterprise Reset packages on the Zebra Support & Downloads website.

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

## Performing an Enterprise Reset From Device Settings

Perform an Enterprise Reset from the device settings.

1. Go to **Settings**.
2. On Android 11, touch **System > Advanced > Reset options > Erase all data (enterprise reset)**.

3. On Android 13, touch **System > Reset options > Erase all data (enterprise reset)**.
4. Touch **Erase all data** twice to confirm the Enterprise Reset.

### Performing an Enterprise Reset Using microSD Card

It is strongly recommended that, prior to use, you format the microSD card on the device.

Go to the Zebra Support & Downloads web site at [zebra.com/support](https://zebra.com/support) and download the appropriate Enterprise Reset file to a host computer.

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 install the microSD card into the device. See Getting Started for more information.
  - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See USB Communication for more information. 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 restarts if the button is held down for longer than 3 seconds.

3. Touch **Restart**.
4. Press and hold the Number 1 button.

The System Recovery screen appears.
5. Press the Number 2 button to navigate to **Apply upgrade from SD card**.
6. Press the Number 1 button to select.
7. Press the Number 2 button to navigate to the Enterprise Reset file.
8. Press the Number 1 button.

The Enterprise Reset occurs and then the device returns to the Recovery screen.

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

### Performing an Enterprise Reset Using ADB

Perform an Enterprise Reset using ADB.

Go to the Zebra Support & Downloads web site at [zebra.com/support](https://zebra.com/support) and download the appropriate Enterprise Reset file to a host computer.

1. Connect the device to a host computer using a USB cable.
2. Go to **Settings**.
3. On Android 11, touch **System > Advanced > Developer options**.
4. On Android 13, touch **System > Developer options**.
5. Slide the **USB debugging** switch to the **ON** position.
6. Touch **OK**.
7. If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.

8. Touch **OK** or **Allow**.
9. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
10. Type `adb devices`.

The following displays:

```
List of devices attached
XXXXXXXXXXXXXXXXX device
```

Where XXXXXXXXXXXXXXXX is the device number.



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

11. Type `adb reboot recovery`.
12. Press **Enter**.  
The System Recovery screen appears on the device.
13. Press the Number 2 button to navigate to **Apply upgrade from ADB**.
14. Press the Number 1 button to select.
15. On the host computer command prompt window type `adb sideload <file>`  
where: <file> = the path and filename of the zip file.
16. Press **Enter**.

The Enterprise Reset package installs, and then the System Recovery screen appears on the device.

17. Press the Number 1 button to reboot the device.
18. Disconnect the USB cable from the device.

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

## Android 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. Zebra distributes the Factory Reset packages on the Zebra Support & Downloads website.

### Performing a Factory Reset Using microSD Card

Perform a Factory Reset using a microSD card.

Go to the Zebra Support & Downloads website at [zebra.com/support](https://zebra.com/support) and download the appropriate Factory Reset file to a host computer.

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 [Getting Started](#) for more information.
  - Connect the device with a microSD card already installed to the host computer, copy zip file to the microSD card, and then 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 restarts if the button is held down for longer than 3 seconds.
3. Touch **Restart**.
4. Press and hold the Number 1 button.

The System Recovery screen appears.
5. Press the Number 2 button to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
6. Press the Number 1 button to select.
7. Press the Number 2 button to navigate to the Factory Reset file.
8. Press the Number 1 button.

After the Factory Reset the device returns to the Recovery screen.
9. Press the Number 1 button to reboot the device.

## Performing a Factory Reset Using ADB

Perform a Factory Reset using ADB.

Go to the Zebra Support & Downloads website at [zebra.com/support](https://zebra.com/support) and download the appropriate Factory Reset file to a host computer.

1. Connect the device to a host computer using a USB cable.
2. Go to **Settings**.
3. On Android 11, touch **System > Advanced > Developer options**.
4. On Android 13, touch **System > Developer options**.
5. Slide the **USB debugging** switch to the **ON** position.
6. Touch **OK**.
7. If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.
8. Touch **OK** or **ALLOW**.
9. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
10. Type `adb devices`.

The following displays:

```
List of devices attached
```

```
XXXXXXXXXXXXXXXXXXXX device
```

Where XXXXXXXXXXXXXXXXXXXX is the device number.



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

11. Type:

```
adb reboot recovery
```

12. Press **Enter**.

The System Recovery screen appears on the device.

13. Press the Number 2 button to navigate to **Apply upgrade from ADB** or **Apply downgrade from ADB**.

14. Press the Number 1 button to select.

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 System Recovery screen appears on the device.

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

18. Disconnect the USB cable from the device.

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

## Android Storage

The device contains multiple types of file storage.

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

### Random Access Memory

Executing programs use RAM to store data. Data stored in RAM is lost upon a reset.

The operating system manages how applications use RAM. It only allows applications and component processes and services to use RAM when required. It may cache recently used processes in RAM, so they restart more quickly when opened again, but it will erase the cache if it needs the RAM for new activities.

The screen displays the amount of used and free RAM.

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

- **Memory used by apps** - Touch to view RAM usage by individual apps.

### Viewing Memory

View the amount of memory used and free RAM.

1. Go to **Settings**.
2. On Android 11, touch **System** > **Advanced** > **Developer options**.
3. On Android 13, touch **System** > **Developer options**.
4. Touch **Memory**.

### 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.

#### Viewing Internal Storage

View available and used internal storage on the device.

1. Go to **Settings**.
2. Touch **Storage**.



If the device has removable storage installed, touch **Internal shared storage** to display the amount of internal storage used by apps, photos, videos, audio, and other files.

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


#### Viewing External Storage

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

1. Go to **Settings**.
2. Touch **Storage**.  
Touch **General USB Drive** to view the contents of the card.  
Touch **SD card** to view the contents of the card.
3. To unmount the microSD card, touch .
4. To unmount the USB drive, touch .


### Formatting a microSD Card as Portable Storage

Format a microSD card as portable storage for the device.

1. Touch **SD card**.
2. Touch  > **Storage settings**.
3. Touch **Format**.
4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.


### Formatting a USB Drive as Portable Storage

Format a USB drive as portable storage on the device.

1. Touch **USB drive**.
2. Touch  > **Storage settings**.
3. Touch **Format**.
4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.

### Formatting a microSD Card 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.

1. Touch **SD card**.
2. Touch  > **Storage settings**.
3. Touch **Format as internal**.
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.

## Managing Apps

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. Go to **Settings**.

2. On Android 11, touch **Apps & notifications**.
3. On Android 13, touch **Apps**.
4. Touch **See all XX apps** to view all apps on the device.
5. Touch  > **Show system** to include system processes in the list.
6. 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.




## App Details

Apps have different kinds of information and controls.

- **Force stop** - Stop an app.
- **Disable** - Disable an app.
- **Uninstall** - Remove the app and all of its data and settings from the device.
- **Notifications** - Set the app notification settings.
- **Permissions** - Lists the areas on the device that the app has access to.
- **Storage & cache** - Lists how much information is stored and includes buttons for clearing it.
- **Mobile data & Wi-Fi** - Provides information about data consumed by an app.
- **Mobile data & Wi-Fi** - Provides information about data consumed by an app. Mobile data not supported.
- **Advanced**
  - **Screen time** - Displays the amount of time the app has displayed on the screen.
  - **Battery** - Lists the amount of computing power used by the app.
  - **Open by default** - If you have configured an app to launch certain file types by default, you can clear that setting here.
  - **Display over other apps** - Allows an app to display on top of other apps.
  - **App details** - Provides a link to additional app details on the Play store.
  - **Additional settings in the app** - Opens settings in the app.
  - **Modify system settings** - Allows an app to modify the system settings.

## Managing Downloads

Files and apps downloaded using the Browser or Email are stored on the USB drive, 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**.
  3. Touch and hold an item to delete, and then touch .
- The item is deleted from the device.

# Maintenance and Troubleshooting

This section explains how to maintain and troubleshoot the device.

## Maintaining the Device

Follow these guidelines to maintain the device properly.

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

- To avoid scratching the screen, use a Zebra-approved, capacitive-compatible stylus intended for use with a touch-sensitive screen. Never use an actual pen, pencil, or other sharp object on the surface of the device screen.
- The device's touch-sensitive screen is made of 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 dusty, damp, or wet location.
- Use a soft lens cloth to clean the device. If the surface of the device screen becomes soiled, clean it with a soft cloth moistened with an approved cleanser. For a list of approved cleansers, see [Approved Cleanser Active Ingredients](#) on page 135.

## Cleaning Instructions

Use caution and avoid damaging the device when using cleaning materials.



**CAUTION:** Always wear eye protection. Read the warning label on alcohol product before using. If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.



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

### Approved Cleanser Active Ingredients

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



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

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

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

### Harmful Ingredients

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

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

### Device Cleaning Instructions

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

Do not handle the device while wearing vinyl gloves containing phthalates. Remove vinyl gloves and wash hands to eliminate any residue left from the gloves.

If products containing any of the harmful ingredients listed above are used prior to handling the device, such as a hand sanitizer that contains 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 the build-up of particles, which makes 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**

This section describes how to clean the housing, display, and camera for 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 lens tissue or other material suitable for cleaning optical material such as eyeglasses.

## Troubleshooting the Device

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

**Table 22** 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). Go to <b>Settings &gt; Storage &gt; MANAGE STORAGE</b> . Select the unused program(s) and tap <b>FREE UP</b> .
	Too many applications installed on the device.	Remove user-installed applications on the device to recover memory. Go to <b>Settings &gt; Apps &amp; notifications</b> . Select the unused programs and touch <b>Uninstall</b> .
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.

**Table 22** Troubleshooting the Device (Continued)

Problem	Cause	Solution
	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.	<p>If the user enters an incorrect password eight times, the user is requested to enter a code before trying again.</p> <p>If the user forgot the password, contact system administrator.</p>

# Technical Specifications

For device technical specifications, go to [zebra.com](http://zebra.com). This chapter also provides decode distances for the CC6000 and CC6000.

## Data Capture Supported Symbolologies

**Table 23** Data Capture Supported Symbolologies

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)

## CC6000 - SE4710 Scan Engine

This table 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 24** 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
5 mil PDF417	3.1 in. 7.9 cm	7.5 in. 19.0 cm

**Table 24** CC6000 - SE4710 Decode Ranges (Continued)

Barcode Type	Near Distance	Far Distance
	Typical	Typical
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
20.0 mil Data Matrix	2.0 in. 5.08 cm*	26 in. 66.0 cm
*Limited by the 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

This table 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 25** CC600 - SE2100 Decode Ranges

Barcode Type	Near Distance	Far Distance
	Typical	Typical
5 mil Code 128	2.0 in. 51 mm	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 the width of barcode in field of view. Note: Photographic quality barcode at 15° tilt pitch angle under 30 fcd ambient illumination.		

