INTERACTIVE KIOSK

KC401

Product Reference Guide

MN-005803-01EN Rev A

Zebra Technologies | 3 Overlook Point | Lincolnshire, IL 60069 USA
zebra.com

Copyright

2026/08/27

The Zebra wordmark and logo are trademarks of Zebra Technologies Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2026 Zebra Technologies Corp. and/or its affiliates.

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.
COPYRIGHTS: zebra.com/copyright.
PATENTS: ip.zebra.com.
WARRANTY: zebra.com/warranty.
END USER LICENSE AGREEMENT: 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.

About this Guide

This guide provides information about using the KC401 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) 15 and above. Android 15 is the baseline, and updated OS releases are indicated in the content where applicable.

Notational Conventions

The following 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 you to know and that is not required to complete a task.



IMPORTANT: The text here indicates information that is important for you to know.

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

WARNING: If danger is not avoided, you CAN be seriously injured or killed.

DANGER: If danger is not avoided, you 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. When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software/firmware 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:
   - Status
   - SW components
   - Legal information
   - Model & hardware
   - Model
   - Android version
     - Android security patch level
     - Android security patch version
     - Google Play system update
     - Kernel version
     - Build Fingerprint

- Build number
- Android Security Update

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**.
3. Touch **Model & hardware**.

Viewing Regulatory Information

View the device e-label to access regulatory information.

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

   The regulatory e-label content displays.

Getting Started

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

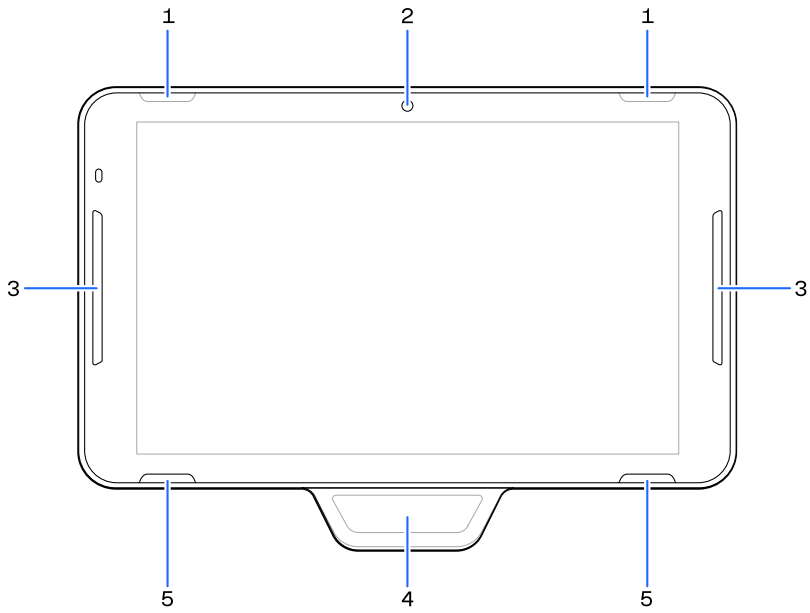
Unpacking the Device

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:
   - KC401 Interactive Kiosk
   - 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.

KC401 Features

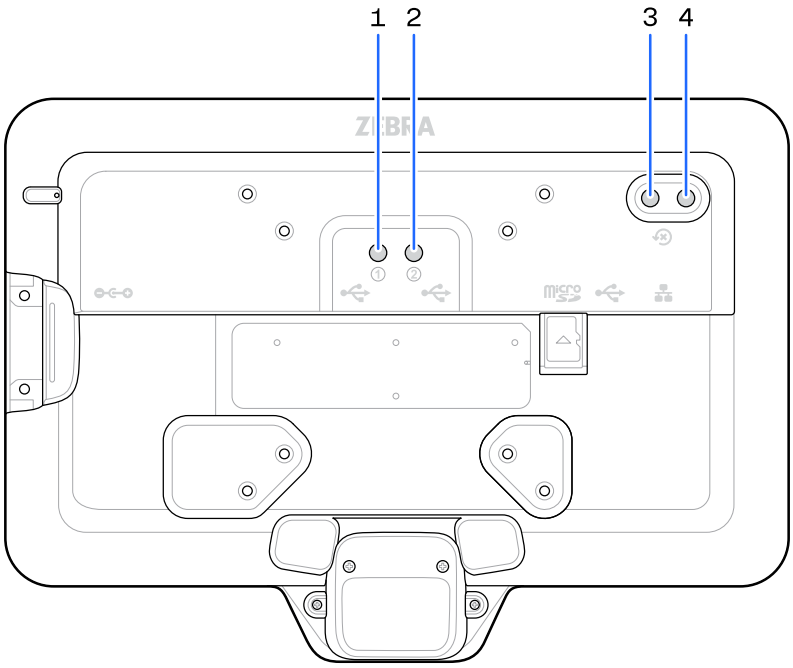
The KC401 Kiosk Computer has a 10.1 in. display and an optional scanner.

Figure 1 KC401 Front View



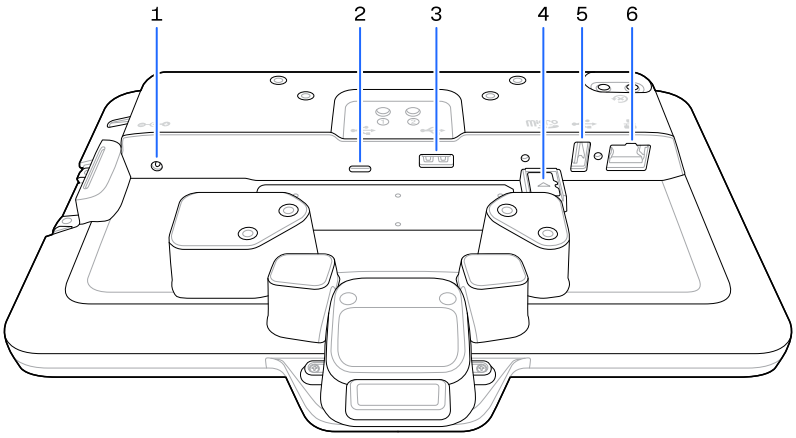
Number	Item	Function
1	False Speakers	Non-functioning speaker grills. Audio is provided by the bottom speakers only.
2	5 MP Camera	Front-facing fixed-focus camera for data capture and communication.
3	LED Light Bars	Two programmable RGB light bars. **NOTE:** If the LED Light Bars flash red, an incorrect Power over Ethernet (PoE) power supply is connected or the power supply class cannot be determined.
4	Scanner Edge Accessory (Optional)	Provides data capture using the imager and reads a barcode. **NOTE:** To read a barcode, a scan-enabled app is required on the device.
5	Speakers	Provides audio output for video and music playback. Provides audio in speakerphone mode.

Figure 2 KC401 Back View



Number	Item	Function
1	Volume Down	Decreases device volume.
2	Volume Up	Increases device volume.
3	Reset Key 1	Press and hold both Reset buttons to reset the device. Go to Resetting the Device for more information.
4	Reset Key 2	Press and hold both Reset buttons to reset the device.

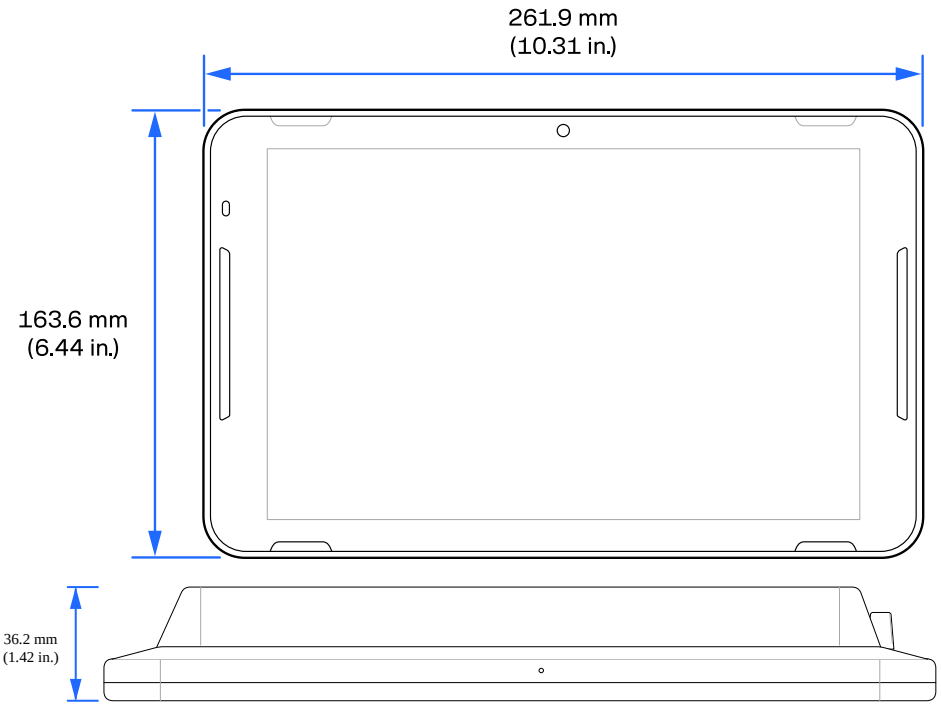
Figure 3 KC401 Power and Cable Ports

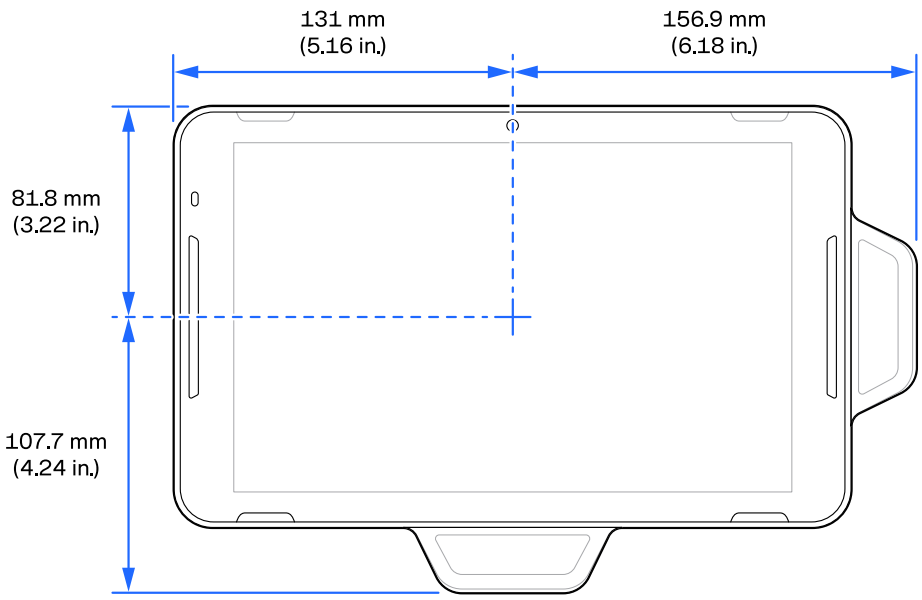


Number	Item	Function
1	DC Power Port	Connects the power supply.
2	USB C Port	USB-C port.
3	USB-A	USB-A port.
4	Micro SD Card Slot	Installs a Micro Secure Digital (SD) card.
5	USB-A	USB-A port.
6	Ethernet With PoE	RJ45 Ethernet port with Power over Ethernet (PoE). The two port LEDs indicate the link speed (left) and link activity (right).

Dimensions

The dimensions of the KC401 Interactive Kiosk are shown with and without the Scanner Edge accessory.





Setting Up the Device

Before using the device for the first time, install and configure your device.

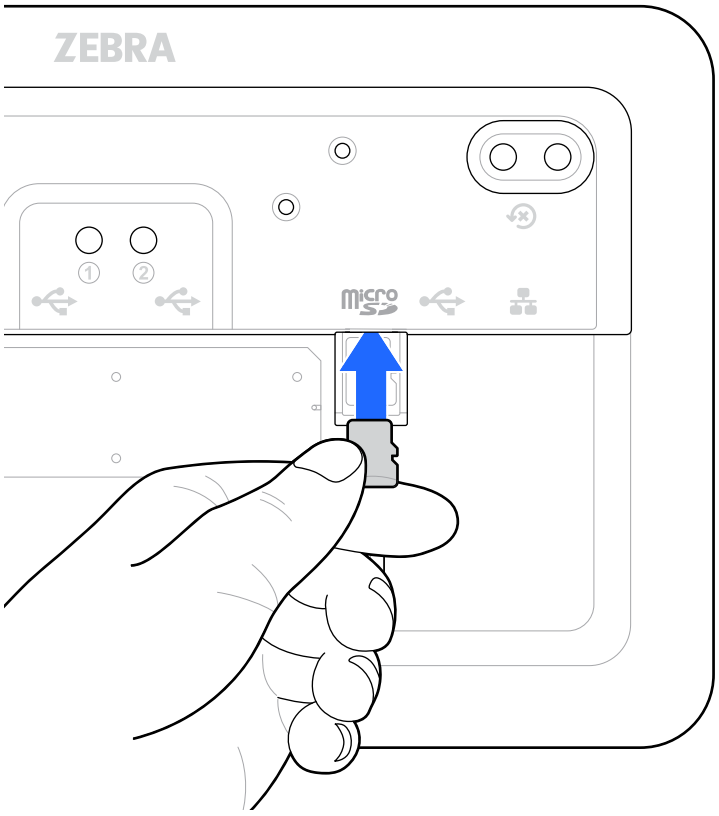
1. (Optional) Install a microSD card.
2. (Optional) Install the Scanner Edge Accessory.
3. Mount the device with the mounting bracket.
4. Connect the device to a power supply.

Installing a microSD Card (Optional)

The microSD card slot provides secondary non-volatile storage. The slot is located on the back of the device. 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. (If installed) Remove the device from the mounting bracket.
2. Slide the microSD card, connectors down, into the device.

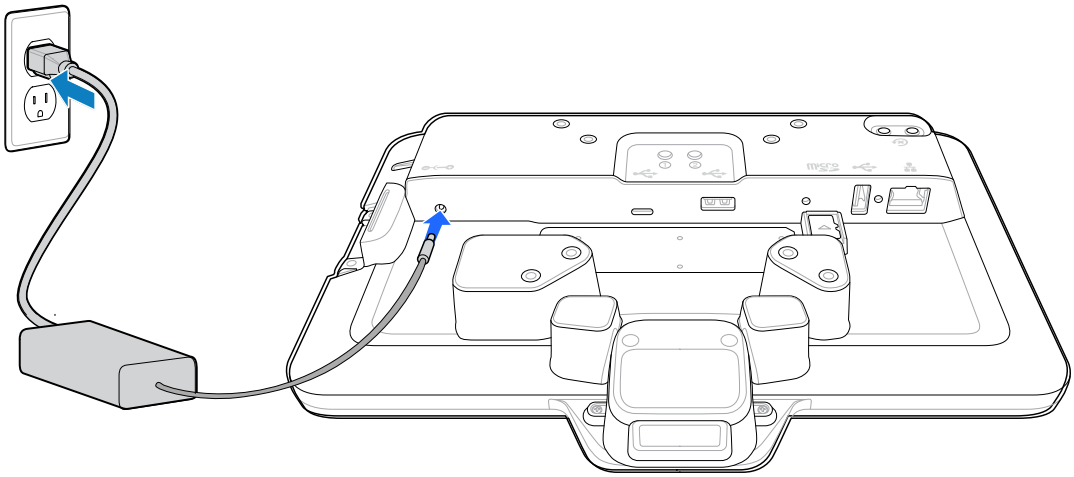


Connecting a DC Power Supply

Power the kiosk using a DC power supply (sold separately) for deployments that do not use Power over Ethernet (PoE).

NOTE: To power the KC401 Interactive Kiosk with a PoE connection, go to Connecting an Ethernet Cable.

1. Mount the KC401 Interactive Kiosk with your mounting solution (see Mounting the Device for mounting instructions).
2. Unpack your power supply from the packing container.
3. On the back of the KC401 Interactive Kiosk, connect the DC line to the DC port.



4. Connect the AC power cord to the power adapter.
5. Connect the KC401 Interactive Kiosk power adapter to an electrical outlet.

The KC401 Interactive Kiosk turns on when connected to power.

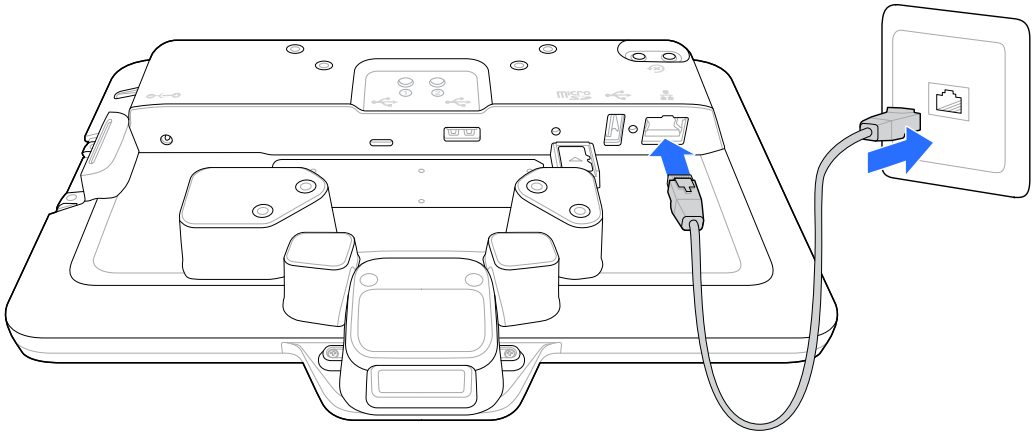
Connecting an Ethernet Cable

Establish a wired network connection for data communication and to optionally supply power via Power over Ethernet (PoE).

NOTE: Power the KC401 Interactive Kiosk with your Ethernet connection by connecting the cable to a powered PoE+ connection that complies with 802.3at or 802.3bt. This connection requires a minimum Class 4 PSE (30 W).

1. On the back of the KC401 Interactive Kiosk, connect a shielded Cat 6e RJ45 ethernet cable.

Figure 4 Ethernet Connection

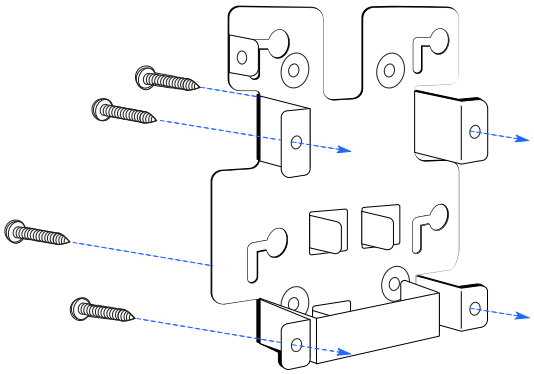


2. Connect the other end of the ethernet cable to an active network port.

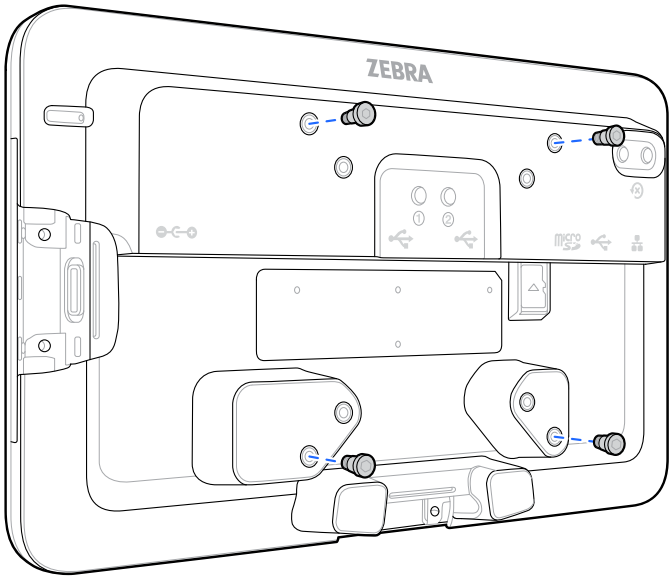
Mounting the Device

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.). The device features both 75 x 75 mm (2.95x2.95 in.) and 100 x 100 mm (3.94x3.94 in.) VESA mounting options.

1. Determine the device mounting location.
2. Secure the mounting plate to the accessory using the screws provided.



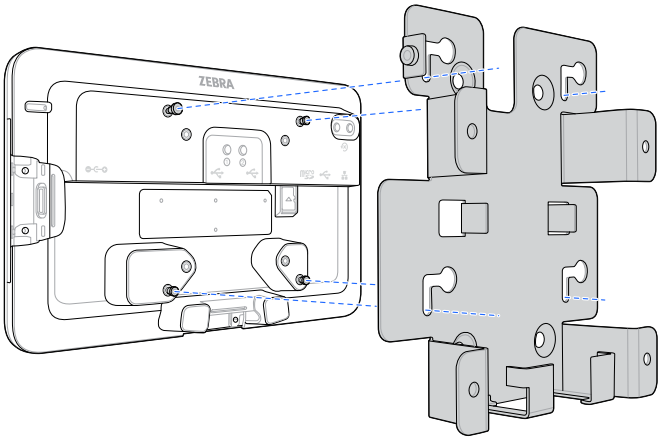
3. With a hex wrench, insert the four M4x8 shoulder screws, also provided, into the mounting holes in the back of the device. Do not overtighten.



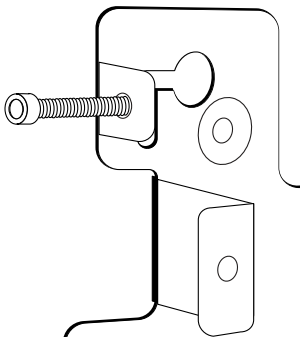
4. Connect the power supply to the device. Power may be supplied by a power supply unit or Power over Ethernet (PoE).

NOTE: If both PoE and a power supply unit are connected, the device uses the highest available power.

5. Connect any additional peripherals into the appropriate ports shown in KC401 Power and Cable Ports.
6. Mount the device by placing the shoulder screws through the four keyholes on the mounting plate, and then slide the device down to secure it in place.



7. Insert the locking screw through the hole in the tab at the top of the mounting plate and then hand-tighten the screw to secure the device.



Turning On the Device

The device turns on automatically when it receives power. If the device remains off, turn it on using the two Reset buttons.

The KC401 Interactive Kiosk does not have a dedicated power button. Connect the device to a power source before turning it on.

On the back of the device, press and hold both Reset buttons simultaneously for at least half a second.

The device turns on and the boot screen displays.

Powering Off the Device

The KC401 Interactive Kiosk does not have a dedicated power button.

Power off the device from the Android menu before disconnecting the power.

1. On the device, swipe down from the top of the screen to access **Quick Settings**.
2. Touch **Power**.

3. Touch **Power off the device**.

Resetting the Device

If the device stops responding, perform a hardware reset using the two Reset buttons.

On the back of the device, press and hold both Reset buttons simultaneously for three seconds.

The device restarts.

Turning Off the Display

Turn off the display and put the device into Sleep mode using the two Reset buttons.

On the back of the device, press both **Reset** buttons.

The display turns off. Press both **Reset** buttons again to turn the display back on.

NOTE: If the device is unresponsive, press and hold both **Reset** buttons for three seconds to perform a hardware reset. See Resetting the Device for more information.

Using the Device

Learn how to operate the device and access its features.

Waking the Device

The display turns off and the device goes into Sleep mode when pressing both Reset buttons simultaneously.

NOTE: The display dims after a period of inactivity. The device does not enter Sleep mode unless the display is turned off using the **Reset** buttons.

1. To wake the device from Sleep mode, touch the screen, and then swipe.

   If a screen lock is enabled, the lock screen displays. Otherwise, the Home screen displays.

2. Swipe the screen to unlock.
   - If the screen option is set to Swipe, the Home screen displays.
   - If either the PIN or Password screen unlock feature is enabled, a prompt displays. Enter the PIN or password to unlock the device and move to the Home screen.
   - If the Pattern screen unlock feature is enabled, the Pattern screen displays. Swipe the correct pattern between the dots to unlock the device and move to the Home screen.

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

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 turns off. Touch the screen to wake the device. The Home screen provides four additional screens to place widgets and shortcuts. Touch and hold an icon, and then move it to place the icon on one of the other screens. Swipe the Home screen left or right to view the additional screens. By default, the device displays the Home screen in landscape orientation.

Figure 5 Home Screen



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

Setting the Home Screen Rotation

By default, the Home screen rotation is enabled.

1. Touch and hold anywhere on the Home screen until the options display.
2. Touch **Home settings**.
3. Touch the **Allow Home screen rotation** switch.
4. Touch **Home**.
5. Rotate the device.

Status Bar

The Status bar displays the time, notification icons on the left side, and status icons on the 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 icons.



1	Notification icons
2	Status icons

Status Icons

Status icons display system information for the device.

Table 1 Status Icons

Icon	Description
	Alarm is active.
	All sounds, except media and alarms, are muted. Vibrate mode 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.

Table 1 Status Icons (Continued)

Icon	Description
	Connected to an Ethernet network.
	Speakerphone enabled.
	Indicates that a Bluetooth headset is connected to the device.

Notification Icons

Notification icons indicate app events and messages.

Table 2 Notification Icons

Icon	Description
	More notifications are available for viewing.
	Data is synching.
	Indicates an upcoming event.
	An Open Wi-Fi network is available. The device is not connected to it.
	Audio is playing.
	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.

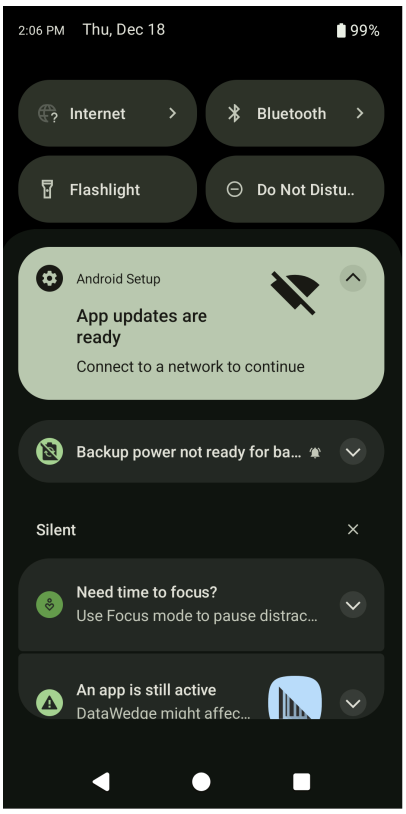
Table 2 Notification Icons (Continued)

Icon	Description
	A wired headset with a boom module is connected to the device.
	A wired headset without a boom module is connected to the device.
	The RxLogger app is running.
	A Bluetooth scanner is connected to the device.
	A ring scanner is connected to the device in HID mode.
	A device is connected via USB cable.

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 6 Android 15 Notification Panel



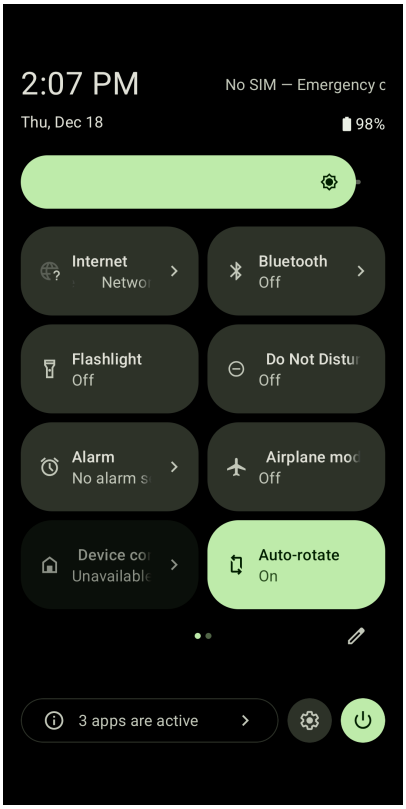
- To view a list of all notifications, open the Notification panel by dragging the Status bar down from the top of the screen.
- To respond to a notification, open the Notification panel and then touch a notification. The Notification panel closes and the corresponding app opens.
- To manage recent or 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, Internet settings).

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

Figure 7 Quick Access Panel



- If the device is locked, swipe down once from the top of the screen.
- If the device is unlocked, swipe down once.
- If the Notification panel is open, swipe down from the Quick Settings bar.

Quick Access Panel Icons

The Quick Access panel icons indicate frequently used settings (for example, Internet settings).

Table 3 Quick Access Panel Icons

Icon	Description
	Display brightness- Use the slider to decrease or increase the brightness of the screen.
	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.
	Color inversion- Invert the display colors.

Table 3 Quick Access Panel Icons (Continued)

Icon	Description
	**Do not disturb**- Control how and when to receive notifications.
	**Airplane mode**- Turn Airplane mode on or off. When Airplane mode is on the device does not connect to Wi-Fi or Bluetooth.
	**Auto-rotate**- Lock the device's orientation in portrait or landscape mode or set to automatically rotate.
	**Data Saver**- Turn on to prevent some apps from sending or receiving data in the background.
	**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 the device screen on Chromecast or a television with Chromecast built-in. On the Cast screen, select 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.
	**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 distractions.
	**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.
	**Alarm**- Opens the Alarm app.
	**Scan QR code**- Opens the camera app for QR code reading.

Table 3 Quick Access Panel Icons (Continued)

Icon	Description
	**Color correction**- Enable to help your device compensate for color blindness.
	**Live caption**- Enables captions to appear for any media playing, regardless of the device's volume level.
	**Nearby Share**- Helps find and interact with services and devices close to the device.
	**RXLogger**- Report an issue.

Editing the Quick Access Tiles

You can change which Quick Access tiles appear at the top of the Quick Access panel.

- Open the Quick Access panel.
- Pull down on the notifications bar to minimize it.
- Touch ✎ to edit, add, or remove settings tiles.

USB Communication

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.

NOTE: If moisture is in the USB port, disconnect the USB-C cable immediately.

USB Host and Client Modes

The device provides one USB-C port that supports host and client modes, and two USB-A 2.0 host ports.

In host mode, the device supports USB keyboards, mice, storage, printers, scanners, and headsets through the USB-A ports or the USB-C port. Application debugging remains available while a USB host port communicates with an accessory.

When a powered USB-C cable (for example, from a host computer or a USB wall adapter) is inserted, the device switches to client mode. In client mode, the device enumerates as a portable device on the host computer, and the storage is explorable using the Media Transfer Protocol (MTP) or the Picture Transfer Protocol (PTP). Enable MTP, PTP, or both from the device software.

NOTE: In client mode, the USB-A ports are unavailable and Ethernet ceases data transmission. When the device switches between client and host modes, all USB ports momentarily disconnect and re-enumerate.

Transferring Files

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

1. Connect the device to a host device using a USB accessory.
2. On the device, open **Settings** > **Connected Devices** > **USB**.
   - To transfer files, touch **File Transfer**.
   - To transfer photos, touch **PTP**.
3. On the host device, open a file explorer application.
4. Locate the device in the file explorer.
5. Open the microSD card or internal storage folder.
6. Copy files between the devices as required.

Disconnecting from the Host Device

Safely disconnect the device from the host computer when the file transfer is complete.

1. Unmount the device on the host computer.
2. Remove the device from the USB accessory.

Power over Ethernet (PoE)

Aside from using a DC power cable, power the device with an 802.3at/802.3bt-compliant PoE injector or network switch.

PoE requires sufficient power from the network, the switch, and the injector. A network administrator ensures uninterrupted power to the device by evaluating the network and selecting the correct injector and connector. The network setup must be tested by a qualified cabling technician to confirm compliance with the ANSI/TIA 568.2-D standard. The testing prevents unbalanced resistances in the cabling which may cause data bit errors, or a breakdown in consistent power delivery to the device. Go to Power Profiles for information on how PoE affects device functionality.

NOTE: The device requires power sourcing equipment (PSE) that complies with 802.3at or 802.3bt Class 4 (30 W) or higher. If lower-class PSE is connected, the device indicates a power error on the LED light bars.

Setting up PoE

Follow these guidelines to correctly set up PoE for the device. For more information on configuring PoE, go to techdocs.zebra.com.

- Select a power class that powers your required ports, peripherals, and device brightness settings.

  Each power class profile defines default restrictions on USB ports, peripherals, and device brightness settings.
- Select an 8-wire cable with RJ45 connectors.
  - Ethernet-8 conductor cable compliant to Cat5e or higher is recommended.
  - The maximum distance from the Power Sourcing Equipment (PSE) to the device is 100 m.

- Do not use a Cat5 cable that mixes telephone/ethernet signal.
- Use a standalone power injector that complies with 802.3at or 802.3bt Class 4 (30 W) or higher.

  Compatible power sourcing equipment includes the Microchip PD-9001GR/SP 30 W PSE and the Wmo QPE088Gb1 30 W PSE.

  NOTE: Class 0, 1, 2, and 3 PSE do not provide sufficient power. If lower-class PSE is connected, the device indicates a power error on the LED light bars.
- If using an 802.3bt-compliant network switch, configure your network switch to ensure the Ethernet port(s) for the device have the highest priority to prevent power demotion and unexpected power loss.

Power Profiles

The Zebra Power Input Manager applies a power profile that matches the connected power source to keep the device within the available power budget.

Power profiles are available out of the box for each supported power source:

- 5.4 V, 16 W power supply
- 12 V, 36 W power supply
- 25.5 W PoE (Class 4) power supply

Each profile defines power-restriction settings for Wi-Fi, Bluetooth, Ethernet, the display backlight level, the speaker level, the USB-A ports, and the USB-C port. For example, when a 5.4 V supply is detected, the device applies a profile that limits certain features to keep power consumption within 16 W.

NOTE: By default, powering the device with PoE (Class 4) reduces the display brightness.

To customize the restrictions, an administrator can create a replacement profile file with the Power Profile Editor and download it to the power profile folder on the device's flash memory. The editor only allows selections that fit within the power available from each power source; to turn one option higher or on, other options may need to be turned lower or off.

LED Indicators

The device uses two RGB LED light bars and two Ethernet port LEDs to indicate power status, notifications, and network activity.

LED Light Bars

Two RGB LED notification light bars are integrated behind the cover glass on each front side edge of the device (in landscape orientation). The light bars mix red, green, and blue light to create other colors, and their color, brightness, and on/off state are controlled programmatically as one unit. All LED states are visible in direct sunlight.

Applications control the light patterns through software APIs. The brightness is adjustable from 0% to 100% in at least 16 levels. LED settings are not persisted after a reboot; a pattern continues until the next command is sent.

State	Indication
No light	The device is powered off.

State	Indication
Solid amber	The device is powered on.
Flashing red	The PoE power supply is incorrect, or the power supply class cannot be determined. Use power sourcing equipment that complies with 802.3at or 802.3bt Class 4 (30 W) or higher.
Blue	Android OS notifications.

Ethernet Port LEDs

The RJ45 Ethernet jack has two integrated activity LEDs:

- The left LED is bi-color. Orange indicates a 10/100 Mbps link, and green indicates a 1 Gbps link.
- The right LED is green. It illuminates when a data link is established and blinks to indicate network activity through the port.

Settings

Configure system, network, and display options on the device.

Accessing Settings

There are multiple ways to access settings on a device.

- Swipe down from the top of the Home screen to open the Quick Access panel, and then touch the Settings icon .
- 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, enable screen rotation, set screen timeout, enable dark theme, and change font size.

Setting the Screen Brightness Manually

Manually set the screen brightness using the touchscreen.

1. Swipe down from the Status bar to open the Quick Access panel.
2. Slide the brightness slider 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. Touch **Use Night Light** to enable.

   By default, **Night Light** is disabled.

7. Adjust the tint using the **Intensity** slider.

Setting Screen Rotation

By default, the screen rotation is enabled.

1. Go to **Settings**.
2. Touch **Accessibility** > **System controls**.
3. Touch **Auto-rotate screen**.
4. Touch **Home**.

Setting Screen Timeout

The screen dims after the selected period of inactivity.

NOTE: Press both **Reset** keys on the rear of the device to manually turn the display off and put the device into Sleep Mode.

1. Go to **Settings**.
2. Touch **Display** > **Screen timeout**.
3. Select one of the system sleep values:
   - **15 seconds**
   - **30 seconds**
   - **1 minute**
   - **2 minutes**
   - **5 minutes**
   - **10 minutes**
   - **30 minutes**
   - **Never** (default)

Setting Lock Screen Notifications

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

1. Go to **Settings**.
2. Touch **Display**.
3. Touch **Lock screen**.
4. Enable or disable an option using the toggle switch.

Setting Font and Display Size

Set the size of the font and display in system apps.

1. Go to **Settings**.
2. Touch **Display**.
3. Touch **Display size and text**.
4. Use the size **+** and **-** slider to vary the size of the font and the display accordingly.

Setting Touch Panel Mode

The display is able to detect touches using a finger, a stylus, or a gloved finger.

NOTE: Supported gloves are lightweight nylon gloves, latex and nitrile gloves up to 5 mils thick, and knit nylon gloves with a nitrile coating. Leather and cotton/polyester gloves are not supported. For optimal performance, use a Zebra-certified stylus.

NOTE: Switching between touch panel modes does not require a reboot.

1. Go to **Settings**.
2. Touch **Display**.
3. Touch **Touch panel mode**.
4. Select one of the following options:
   - **Finger Only** to use a finger (no gloves) on the screen.
   - **Stylus, Glove, and Finger** to use a stylus, a gloved finger, or a finger on the screen.
5. Touch **Home**.

Setting the Date and Time

Connecting to a cellular or wireless network automatically synchronizes the device's date and time via a Network Identity and Time Zone (NITZ) server. Manually set the date, time, or time zone only if the network lacks NTP support or the device is offline.

1. Go to **Settings**.
2. Touch **System** > **Date & time**.
3. Touch **Set time automatically** to disable automatic date and time synchronization.
4. Touch **Set automatically** to disable automatic time zone synchronization.
5. Touch **Date** to select the date in the calendar.
6. Touch **OK**.
7. 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**.
8. Touch **OK**.

9. Touch **Time zone** to select the current time zone from the list.
10. Touch **Update Interval** to select an interval to synchronize the system time from the network.
11. Under Time Format, select either **Use locale default** or **Use 24-hour format**.

Configuring General Sound Settings

Press the volume buttons on the device to display on-screen volume controls.

Use the Sound settings to configure media and alarm volumes.

1. Go to **Settings**.
2. Touch **Sound & vibration**.
3. Touch an option to set sounds.

Sound Options

The Sound Options menu allows users to customize and manage their device's audio and vibration settings to suit their preferences.

- **Zebra volume controls:**
  - **Media volume** - Controls the music, games, and media volume.
  - **Call volume** - Controls the volume during a call.
  - **Ring volume** - Controls the ringtone volume.
  - **Notification volume** - Controls the notification volume.
  - **Alarm volume** - Controls the alarm clock volume.
  - **Do Not Disturb** - Mutes some or all sounds and vibrations.
  - **Live Caption** - Automatically caption speech.
  - **Media** - Shows the media player in Quick Settings while sound is playing, allowing quick access.
  - **Vibration & haptics:**
    - **Ring vibration** - Vibrate the device when the phone rings.
    - **Notification vibration** - Vibrate the device when a notification comes in.
    - **Alarm vibration** - Vibrate the device when an alarm goes off.
    - **Touch feedback** - Vibrate the device when making screen selections.
    - **Media vibration** - Enable vibration when using a media player.
  - **Default notification sound** - Select a sound to play for all system notifications.
  - **Default alarm sound** - Select a sound to play for alarms.
  - **Screen locking sound** - Play a sound when locking and unlocking the screen (default - enabled).
  - **Charging sounds and vibration** - Play a sound and vibrate when power is applied to the device (default - enabled).
  - **Tap & click sounds** - Play a sound when interacting with the screen (default - enabled).
  - **Always show icon when in vibrate mode** - Enable the vibrate mode status bar icon.

Zebra Volume Controls

In addition to the default sound settings, Zebra Volume Controls display when the volume buttons are pressed.

Zebra Volume Controls are configured using Audio Volume UI Manager (AudioVolUIMgr). Administrators can use AudioVolUIMgr to add, delete, and replace Audio Profiles, select an Audio Profile to use the device, and modify the default Audio Profile. For information on how to configure Zebra Volume Controls using AudioVolUIMgr, go to techdocs.zebra.com.

Keyboards

The device provides multiple keyboard options.

NOTE: The Enterprise Keyboard is available for download from the Zebra Support Site.

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

Enabling Keyboards

Enable additional onscreen keyboards to make them available for text entry.

1. Go to **Settings**.
2. Touch **System** > **Keyboard** > **On-screen keyboard**.
3. Touch a keyboard to enable.

Switching Between Keyboards

When multiple keyboards are enabled, you can switch between them to access different settings and characters.

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

1. Touch a text box to display the current keyboard.
2. Touch the keyboard icon in the lower-left corner of the screen.
3. Select a keyboard from the **Choose input method** dialog.

Using the Keyboards

Using the 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

This section describes how to input numbers, symbols, and special characters using the keyboard.

1. Enter numbers and symbols.
   - Touch and hold one of the top-row keys until a menu displays 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.

NOTE: Only available with a Mobility DNA Enterprise License.

- 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

Select and order system languages to display device menus in your preferred language.

1. Go to **Settings**.
2. Touch **System** > **Languages**.
3. Touch **System 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 the ═ icon that is located to the right of the newly added language, then drag it to the top of the list.

   The operating system text changes to the selected language.

Adding Words to the Dictionary

This section describes how to add words to the device's dictionary.

1. Go to **Settings**.
2. Touch **System** > **Keyboard** > **Personal dictionary**.
3. If prompted, select the language where this word or phrase is stored.
4. Touch **+** to add a new word or phrase to the dictionary.
5. Enter the word or phrase.
6. In the **Shortcut** text box, enter a shortcut for the word or phrase.

Notifications

Device notification settings allow you to configure how notifications occur on the device, and app notification settings allow you to configure how notifications for a specific app occur.

To view device notification settings, touch **Settings** > **Notifications**.

To view app notifications, touch **Settings** > **Notifications** > **App notifications**, and then select an app.

Enabling Blink Light

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

1. Go to **Settings**.
2. Touch **Notifications**.
3. Touch **Blink light** to toggle the notification on or off.

Applications

The APPS screen displays icons for all installed apps. Go to Application Deployment for information on installing and uninstalling apps. For information on standard Android apps, refer to the Google Play Store (https://play.google.com/store/apps).

Installed Applications

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

Table 4 Apps

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

Table 4 Apps (Continued)

Icon	Description
	**RxLogger** - Use to diagnose device and app issues.
	**Settings** - Use to configure the device.
	**VoD** - The Video on Device basic app provides a how-to video for proper device cleaning. For Video on Device licensing information, contact learningservices@zebra.com.
	**Wireless Analyzer** - 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.
	**Zebra Bluetooth Settings** - Use to configure Bluetooth logging.
	**Zebra Data Services** - Use to enable or disable Zebra Data Services. Some options are set by the system administrator.
	**Zebra Showcase** - Provides a way to experience and learn about Zebra's new or existing capabilities.

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

On the device, you can switch between open applications.

1. Touch **Recent**.

   A window displays with a list of recently used applications.
2. Slide the apps left or right to view all the apps.
3. Swipe up to remove the app from the list and force close the apps.
4. Touch 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 front-facing camera.

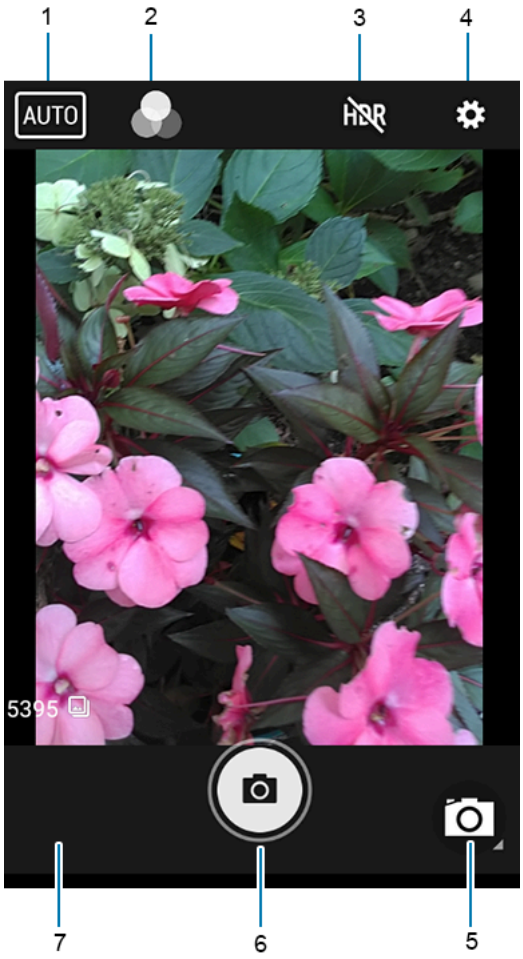
The device is equipped with a 5 MP fixed-focus front-facing camera and uses the Qualcomm Snapdragon camera application. Use the camera to take photos, record videos, and scan barcodes for staging (for example, StageNow barcodes).

To configure camera options, touch the settings icon in the Camera application.

Taking Photos

Use the front-facing camera to take photos.

1. Swipe up from the bottom of the Home screen, and then 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 then 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 displays. The two bars turn green when in focus.
6. Touch .

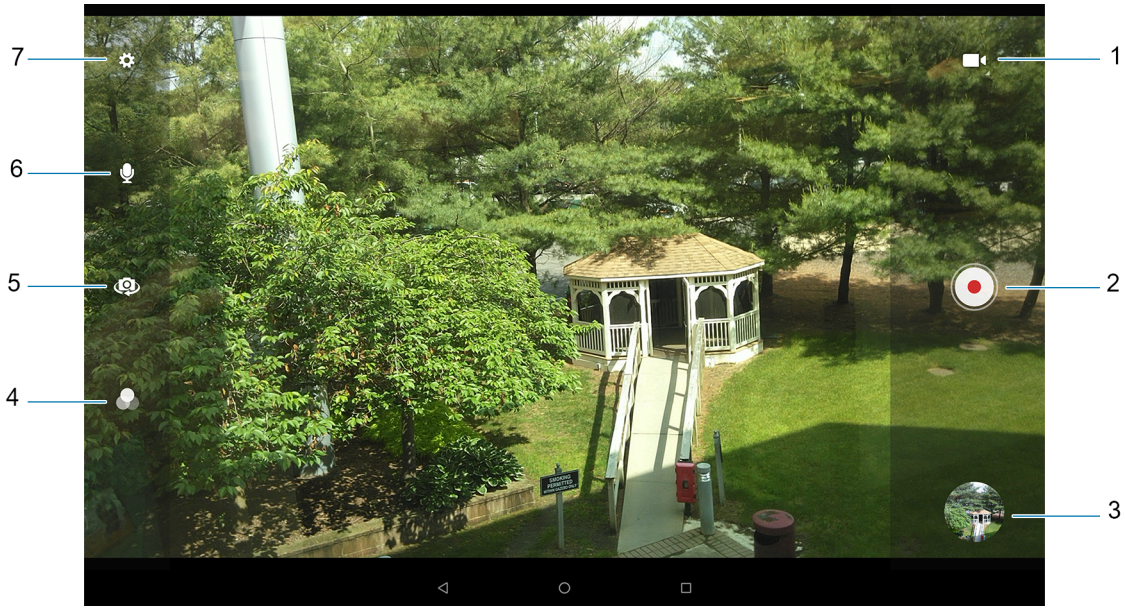
The camera takes a photo and a shutter sound plays.

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

Recording Videos

Use the front-facing camera to record videos.

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



1	Camera mode
2	Shutter button
3	Thumbnail
4	Color effect
5	Camera flip if your device has a front and rear facing camera

6	Audio
7	Settings

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 displays in the top left of the screen.
6. Touch to start recording.

   The video time remaining displays in the top left of the screen.
7. Touch to end the recording.

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

Camera Settings

In the Camera app, camera settings display on the screen. Touch to display the camera setting options.

- **General** - These settings apply to both the still camera and video camera.
  - **Camera Sounds** - Select to play a shutter sound when taking a photo. Options: Disable or Enable (default).
  - **Haptic Feedback** - Provides tactile responses when interacting with the camera.
  - **Location Tags** - Includes location information when pictures and videos are taken.
  - **Storage** - Set the location to store the photo to: Phone or SD Card.
  - **Dirty Lens Detection** - Notifies when the camera lens might be dirty. Options: Disable (default) or Enable.
  - **QR Code Mode** - Enable to scan QR Codes with the option to launch URL. Options: Disable (default) or Enable.
  - **Google Lens** - Select to enable Google-developed recognition technology that brings up relevant information related to identified objects within an image.
  - **Digital Level** - Display a level line to ensure the photo or video is level. Options: Disable (default) or Enable.
  - **Face Detection** - Select to turn the face detection On (default) or Off.
  - **Gestures** - View gestures and power user controls. Gestures include: Swipe Down, Swipe Up, Side Swipe, Tap, Tap + Hold, Double Tap, and Hold Zoom.
- **Still Camera** - These settings apply only to the still camera.
  - **Photo Grid** - Displays a 3 x 3 grid guide on the camera viewport. Options: Disabled (default), or Enable.
  - **Countdown timer** - Select Off (default), 3 seconds, or 10 seconds.
  - **Picture size** - The size (in pixels) of the photo: 12.5M (default), 8M, 5M, 720p, WVGA, VGA, QVGA, 50M.

- **Picture quality** - Set the picture quality setting to: Low, Standard (default), or High.
- **Image Quality Analyzer** - Analyze the image quality for it's degree of sharpness.
- **Privacy Blur - Face Blur** - Identify faces in a captured photo and automatically blur them.
- **Picture Format** - For most resolutions, still images are saved in RAW + JPEG format.
- **MFNR** - Sets multi-frame noise reduction to improve quality in low light conditions. Options: Enabled (default), or Disabled.
- **AutoFocus Animation** - Select to enable or disable the camera focus square in the camera preview. Options: Disable (default) or Enable.

- **Video Camera** - These settings apply only to the video camera.
  - **Video quality** - Set video quality to: 4k UHD (rear camera only), HD 1080p (default), HD 720p, SD 480p, VGA, CIF, or QVGA.
  - **Video duration** - Set to: 30 seconds (MMS), 10 minutes (default), 30 minutes, or no limit.
  - **Noise Reduction** - Off, Fast, or High Quality (default).
  - **HEVC Encoder** - Save video recordings using high-efficiency video codec (HEVC/h265) for smaller file size. Options: Disabled (default), or Enable.
  - **Audio Encoder** - Set the audio encoder to: AMRNB, or AAC (default).
  - **Video Rotation** - Set the rotation of the video to: 0 (default), 90, 180, or 270.
- **System**
  - **Restore defaults** - Select to restore all settings to the default values.
  - **About** - Displays the software version of the camera app.

DataWedge Demonstration

Use DataWedge Demonstration (DWDemo) to demonstrate data capture functionality on the device. To configure DataWedge, refer to techdocs.zebra.com.

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

DataWedge Demo Icons

This table lists the icons available on the device DWDemo app.

Table 5 dataWedge Demonstration 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		Indicates a USB scanner is connected to the device.

Table 5 dataWedge Demonstration Icons (Continued)

Category	Icon	Description
Data capture		Indicates a USB scanner is not connected to the device.
Data Capture		The data capture function is through the internal imager or USB scanner.
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

Select one of the scanning options available on the device.

See Data Capture 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 displays in the text field below the yellow Scan button.

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, Bugreport, logcat, TCP dump, ANR, Tombstone dumps, pre-configured instant logging, and so on. 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, go to 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 , permitting remote configuration and mass deployment of setting files using an enterprise mobile management (EMM) system.

The config.json configuration file is located in the RxLogger\config folder. Copy the file from the device to a host computer using a USB connection. Edit the configuration file and then replace the JSON file on the device. There is no need to stop and restart the RxLogger service because the file change is automatically detected.

IMPORTANT: The RxLogger configuration file is human-readable; however, it should not be edited by hand as doing so can lead to unpredictable behavior. Zebra recommends modifying RxLogger settings only through the RxLogger UI.

- File name: `config.json`
- Location: `/<internal_storage>/RxLogger`

When a new settings file is pushed to the device, RxLogger restarts all affected modules and applies the new settings immediately.

Copy the file from the device to a host computer using a USB connection. Edit the configuration file through the RxLogger UI 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

Enable logging to track system activity and troubleshoot issues.

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

Disabling Logging

Disable logging to conserve system resources and battery life.

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

Extracting Log Files

Extract log files to a computer or memory card for further analysis.

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

Initiate the main chat head to access RxLogger features directly from the active screen.

1. Open **RxLogger**.
2. Touch ⋮ > **Toggle Chat Head**.

   The Main Chat Head icon displays on the screen.
3. Touch and drag the Main Chat Head icon to move it around the screen.

Removing the Main Chat Head

Remove the Main Chat Head to hide the floating RxLogger icon.

1. Touch and drag the icon.

   A circle with an X displays.
2. Move the icon over the circle and then release.

Viewing Logs

1. Touch the Main Chat Head icon.

   The RxLogger Utility screen displays.
2. Touch a log to open it.

   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

Remove a Sub Chat Head icon when it is no longer needed.

- 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 displays.

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:

- Scanner Edge Accessory
- 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

NOTE: The device supports using the Scanner Edge Accessory and a connected scanner at the same time, and supports multiple connected scanners (wired and Bluetooth) simultaneously, including more than one scanner of the same model.

2D Imaging

Devices with an integrated 2D imager have the following features:

- Omnidirectional reading of a variety of barcode symbologies, including common 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 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 the latest software decoding algorithms to extract the barcode data from the image.

Linear Imager

Devices with an 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 barcode 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 you hold 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 learn proper techniques.

However, consider the following to optimize scanning performance:

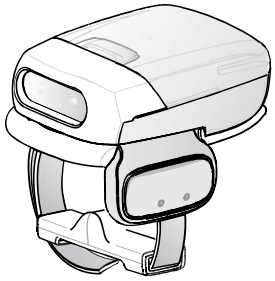
- Range — Scanners decode optimally over a particular working range — minimum and maximum distances from the barcode. This range varies depending on barcode density and the scanning device's optics. Scan within range for quick, consistent decodes; scanning too close or too far away prevents decodes. 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 the beam does not bounce back directly. Do not scan at too sharp an angle; the scanner needs to collect scattered reflections 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 than those listed.

Scanning with the RS507/RS507X Hands-Free Imager

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

Figure 8 RS507/RS507X Hands-Free Imager

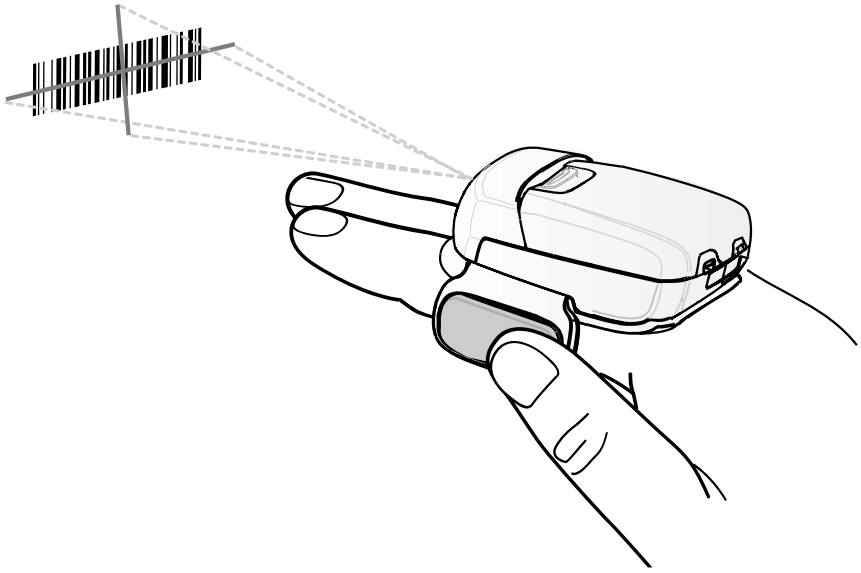


Refer to the RS507/RS507X Hands-free Imager Product Reference Guide for more information.

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

To scan with the RS507/RS507x:

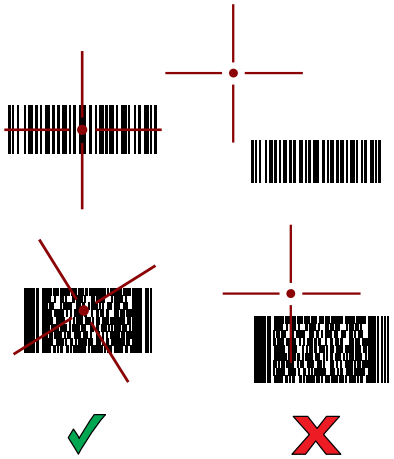
1. Pair the RS507/RS507X with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS507/RS507X at a barcode.



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 9 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 10 RS507/RS507X Pick List Mode with Multiple Barcodes in Aiming Pattern



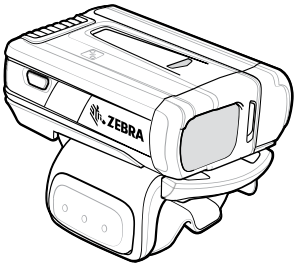
The RS507/RS507X LEDs light green and a beep sounds to indicate the barcode was decoded successfully.

The captured data displays in the text field.

Scanning with the RS6000 Bluetooth Ring Scanner

Use the RS6000 Bluetooth Ring Scanner to capture barcode data.

Figure 11 RS6000 Bluetooth Ring Scanner

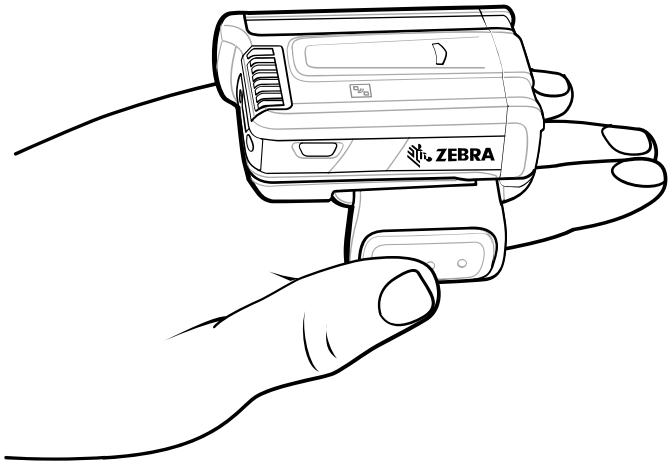


Refer to the RS6000 Bluetooth Ring Scanner Product Reference Guide for more information.

NOTE: To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that enables you to use the scanner to decode barcode data and display the barcode content.

To scan with the RS6000:

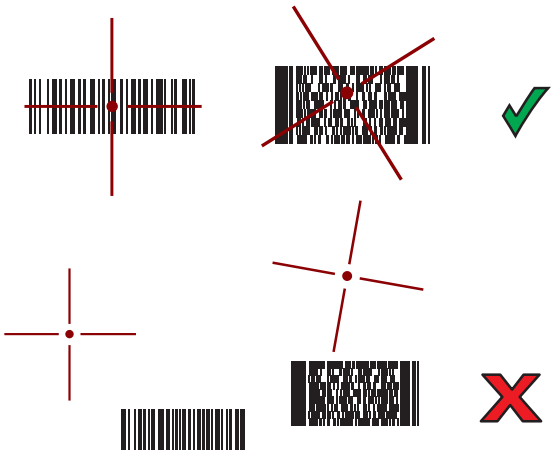
1. Pair the RS6000 with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS6000 at a barcode.



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 12 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 13 RS6000 Pick List Mode with Multiple Barcodes in Aiming Pattern



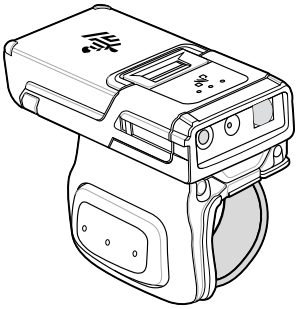
The RS6000 LEDs light green and a beep sounds to indicate the barcode was decoded successfully.

The captured data displays in the text field.

Scanning with the RS5100 Ring Scanner

Use the RS5100 Ring Scanner to capture barcode data.

Figure 14 RS5100 Ring Scanner

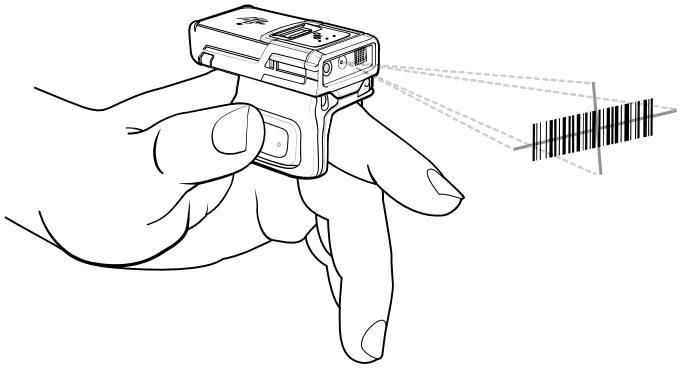


Refer to the RS5100 Ring Scanner Product Reference Guide for more information.

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

To scan with the RS5100:

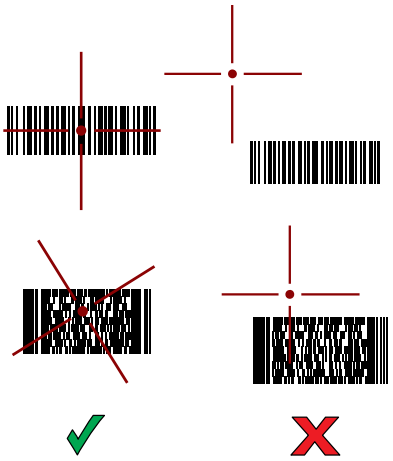
1. Pair the RS5100 with the device.
2. Ensure that an app is open on the device and a text field is in focus (text cursor in text field).
3. Point the RS5100 at a barcode.



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 15 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 16 RS5100 Pick List Mode with Multiple Barcodes in Aiming Pattern



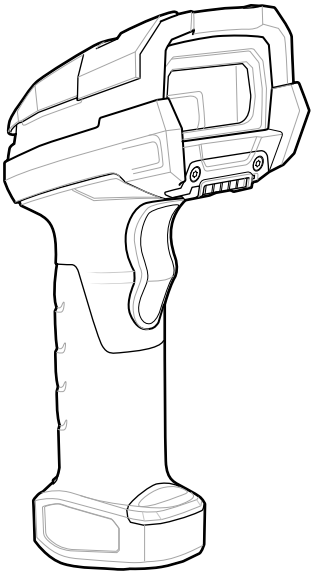
The RS5100 LEDs light green and a beep sounds to indicate the barcode was decoded successfully.

The captured data displays in the text field.

Scanning with the DS3678 Bluetooth Scanner

Use the DS3678 Bluetooth Scanner to capture barcode data.

Figure 17 DS3678 Digital Scanner

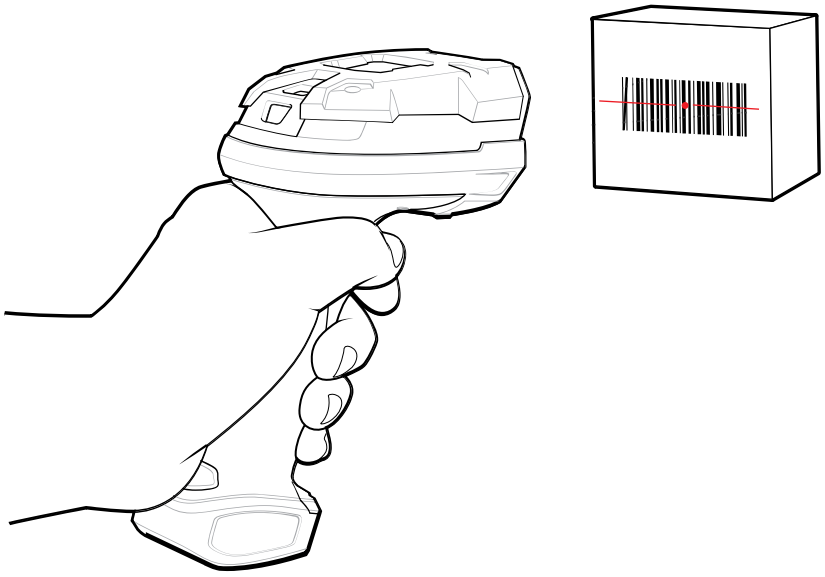


Refer to the DS3678 Product Reference Guide for more information.

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

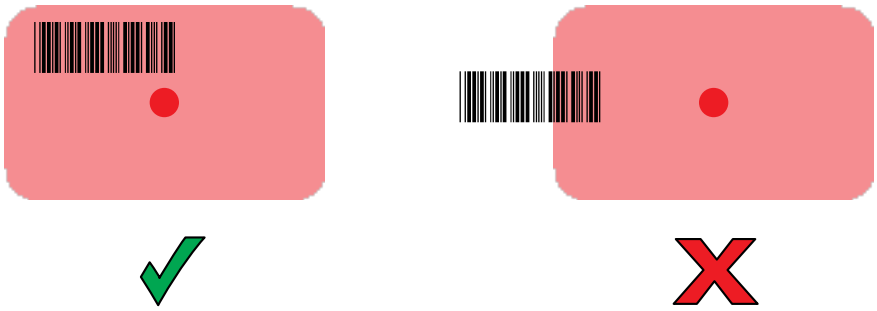
To scan with the DS3678 scanner:

1. Pair the scanner with the device. See Pairing 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.

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

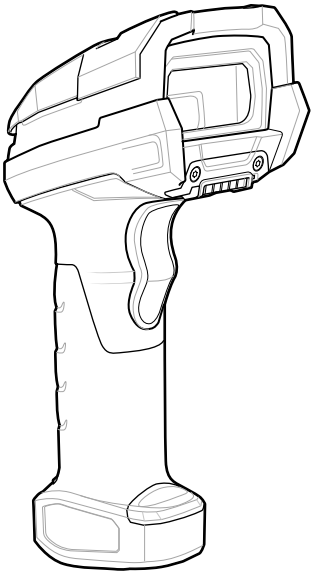


   The captured data displays in the text field.

Scanning with the LI3678 Linear Imager

Use the LI3678 linear imager to capture barcode data.

Figure 18 LI3678 Bluetooth Scanner

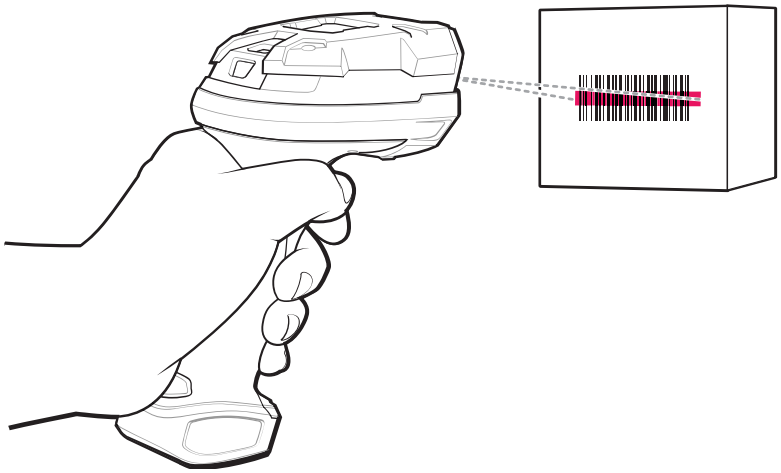


Refer to the LI3678 Product Reference Guide for more information.

NOTE: To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows you 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 displays in the text field.

Scanning with the DS2278 Digital Scanner

Use the DS2278 Digital Scanner to capture barcode data.

Figure 19 DS2278 Digital Scanner

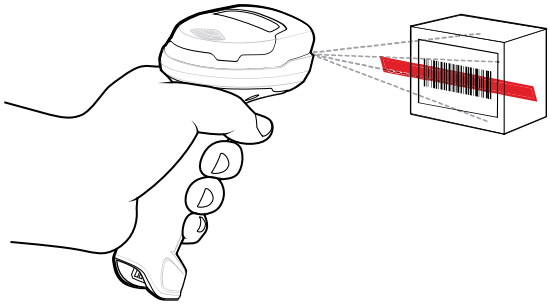


Refer to the DS2278 Digital Scanner Product Reference Guide for more information.

NOTE: To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows you 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.

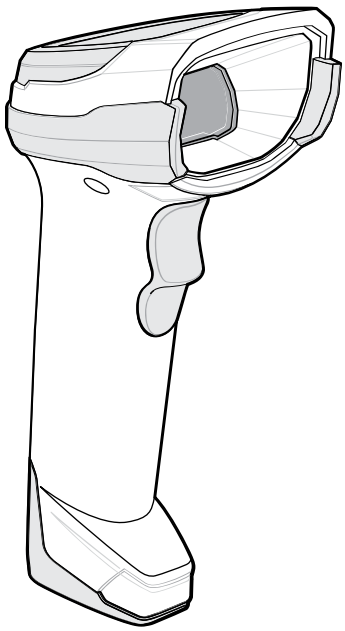


6. Upon successful decode, the scanner beeps and the LED flashes, and the scan line turns off. The captured data displays in the text field.

Scanning with the DS8178 Digital Scanner

Use the DS8178 Bluetooth Scanner to capture barcode data.

Figure 20 DS8178 Digital Scanner

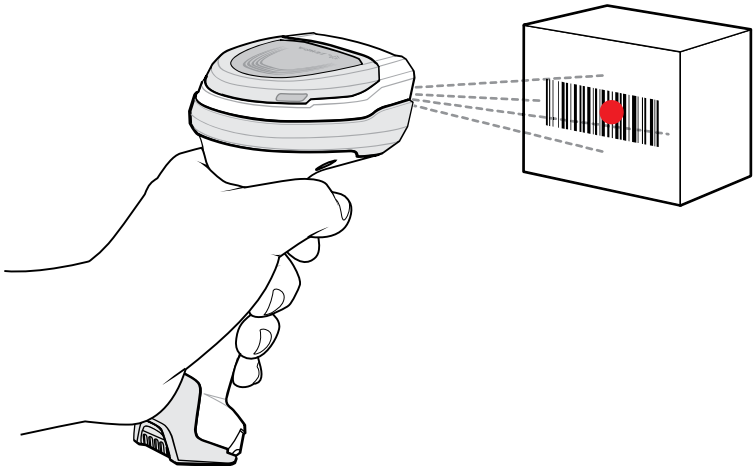


Refer to the DS8178 Digital Scanner Product Reference Guide for more information.

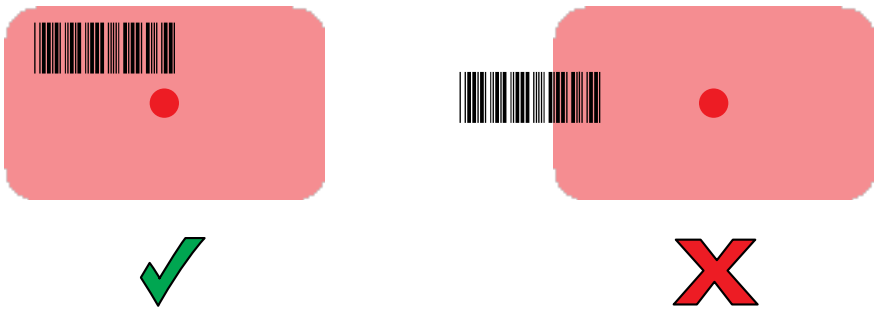
NOTE: To read a barcode, a scan-enabled app is required. The device contains the DataWedge app that allows you to enable the scanner to decode barcode data and display the barcode content.

To scan with the DS8178 scanner:

1. Pair the scanner with the device. See Pairing 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 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 displays 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)
- Simple Serial Interface (SSI)

- Bluetooth Human Interface Device (HID) Mode

NOTE: The device forgets the Bluetooth scanner pairing when the device is powered off or when the scanner disconnects. Pair the scanner again to reconnect.

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 KC401 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.

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 displays in the Status bar.

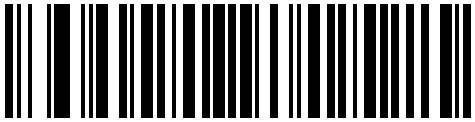
Pairing in HID Mode Using Near Field Communication

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

NOTE: Applicable to KC401 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 21 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.

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 displays on the device screen.

The icon displays 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 22 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 displays on the Notification panel and the icon displays in the Status bar.

Pairing the Ring Scanner 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 23 RS507 Bluetooth HID Barcode

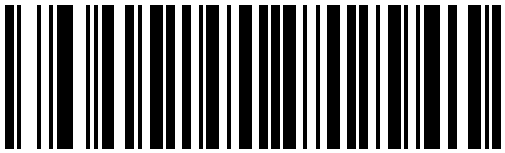
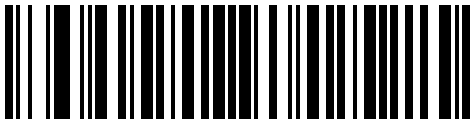


Figure 24 RS6000 Bluetooth HID Barcode



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** displays below the device name. The Bluetooth device is added to the **Paired devices** list and a trusted ("paired") connection is established.

    A notification displays on the Notification panel and the A icon displays 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 25 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 displays on the Notification panel and the icon displays 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** displays 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. DataWedge converts the captured barcode data to keystrokes and sends it to the target application as if it were typed on the keypad.

DataWedge allows any app on the device to get data from input sources such as a barcode scanner or voice 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, go to 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 displays 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 ⋮ > **Settings**.

3. Uncheck the **DataWedge enabled** checkbox.

Supported Decoders

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

RS507/RS507x Supported Decoders

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

Table 6 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	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	-	Trioptic 39	O
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	O	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 7 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
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 8 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

Table 8 RS5100-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
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 9 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	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

Table 9 DS2278 Digital Scanner-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
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	Codablock	O
EAN13	X	MicroQR	O	Finnish Postal 4S	O
GS1 Digital Link	O	MICR E13B	O	OCR A	O
OCR B	O	US Currency	O		

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

DS3678 Supported Decoders

This section lists the supported decoders for the DS3678 scanner.

Table 10 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	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

Table 10 DS3678-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
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	Codablock	O
EAN13	X	MicroQR	O	Finnish Postal 4S	O
GS1 Digital Link	O	MICR E13B	O	OCR A	O
OCR B	O	US Currency	O		

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

LI3678 Supported Decoders

This section lists the supported decoders for the LI3678 scanner.

Table 11 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	O	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
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	O	US4state FICS	—
Datamatrix	—	Matrix 2 of 5	O	US Planet	—

Table 11 LI3678-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Dutch Postal	—	Maxicode	—	US Postnet	—
DotCode	O	MicroPDF	—	Codablock	O
EAN13	X	MicroQR	—	Finnish Postal 4S	O
GS1 Digital Link	O	MICR E13B	O	OCR A	O
OCR B	O	US Currency	O		

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

DS8178 Supported Decoders

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

Table 12 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	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	Codablock	O
EAN13	X	MicroQR	O	Finnish Postal 4S	O

Table 12 DS8178 Digital Scanner-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
GS1 Digital Link	O	MICR E13B	O	OCR A	O
OCR B	O	US Currency	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, and so on.) for instructions on how to set up the infrastructure.

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **Network & internet** 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-Enterprise
  - Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA).
  - Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA').
  - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP) with MSCHAP and MSCHAPv2 authentication, and GTC authentication.
  - 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.
- WPA3-Enterprise
    - Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA).
    - Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (AKA').
    - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP) with MSCHAP and MSCHAPv2 authentication, and GTC authentication.
    - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
    - Transport Layer Security (TLS)

The device supports the following WLAN security options:

Connecting to a Wi-Fi Network

Connect to your local Wi-Fi network through the **Settings** menu

1. Go to **Settings**.
2. Touch **Network & internet**.
3. Touch **Internet** to open the **Internet** screen.

   The device searches for WLANs in the area and lists them.
4. Select the desired WLAN network.

   For secure networks, enter the required password or other credentials, and touch **Connect**.

In the Wi-Fi setting field, **Connected** displays, 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 13 Wi-Fi Version Icons

Icon	Description
	Connected to Wi-Fi 7, the 802.11be standard.
	Connected to Wi-Fi 6, the 802.11ax standard.
	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.

1. Go to **Settings**.
2. Touch **Network & Internet**.
3. Touch **Internet**.
4. Scroll down to the bottom of the list and touch **Saved networks**.
5. Touch the name of the network.
6. Touch **FORGET**.

WLAN Configuration

This section provides information on configuring Wi-Fi settings.

Configuring a Secure Wi-Fi Network

The device supports several authentication protocols for a secure connection.

1. Go to **Settings**.
2. Touch **Network & Internet**.
3. Slide the switch to the **ON** position.

   The device searches for WLANs in the area and lists them on the screen.
4. Scroll through the list and select the desired WLAN network.
5. 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.
6. If network security is **WPA/WPA2-Personal**, **WPA3-Personal**, or **WEP**, enter the required password and then touch **Connect**.
7. 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.

8. 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.
9. 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. Touch **Internet**.
4. Slide the Wi-Fi switch to the **On** position.
5. Scroll to the bottom of the list and select **Add network**.
6. In the **Network name** text box, enter the name of the Wi-Fi network.
7. In the **Security** drop-down list, set the type of security to:
   - **None**
   - **Enhanced Open**
   - **WEP**
   - **WPA/WPA2-Personal**
   - **WPA3-Personal**
   - **WPA/WPA2-Enterprise**
   - **WPA3-Enterprise**
   - **WPA3-Enterprise 192-bit**
8. If the network security is **None** or **Enhanced Open**, touch **Save**.
9. If the network security is **WEP**, **WPA3-Personal**, or **WPA/WPA2-Personal**, enter the required password and then touch **Save**.
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**
       - **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.

11. 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 for setting the connection to a proxy server and see Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

12. 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. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. If configuring the connected network, touch to edit the network details and then touch the down arrow to hide the keyboard.
6. Touch **Advanced options**.
7. Touch **Proxy** and select **Manual**.
8. In the **Proxy hostname** text box, enter the address of the proxy server.
9. In the **Proxy port** text box, enter the port number for the proxy server.

10. 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.
11. If configuring the connected network, touch **Save**; otherwise, touch **Connect**.
12. 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. Touch **Internet**.
4. Slide the Wi-Fi switch to the **On** position.
5. In the network dialog box, select and touch a network.
6. If configuring the connected network, touch ✎ to edit the network details and then touch the down arrow to hide the keyboard.
7. Touch **Advanced options**.
8. Touch **IP settings** and select **Static**.
9. In the **IP address** text box, enter an IP address for the device.
10. If required, in the **Gateway** text box, enter a gateway address for the device.
11. If required, in the **Network prefix length** text box, enter the prefix length.

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 Network preferences.

- **Turn on Wi-Fi automatically** - When enabled, Wi-Fi automatically turns back on when near high-quality saved networks.

  Notify for public networks - When enabled, notifies the user when an open network is available.
- **Additional settings** - Touch to expand options.
  - **Install Certificates** - Touch to install certificates.
  - **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)**6 GHz only**, **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**.
  - **Available channels (6 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
- **Logging**
  - **Advanced Logging** - Touch to enable logging, enable **Wi-Fi Verbose Logging**, or change the log directory.
  - **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

Use Wi-Fi Direct to correct directly to a device without a router or network access.

1. Go to **Settings**.
2. Touch **Network & Internet**.
3. Slide the **Wi-Fi** switch to the **On** position.
4. 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.

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). The device uses a Class 1 Bluetooth radio with a free-space range of up to 50 m (164 ft).

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 1 device power class. The maximum output power is 2.5 mW and the expected range is 50 m (164 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 you 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 14 Bluetooth Profiles

Profile	Description
Service Discovery Protocol (SDP)	Handles the search for known and specific services and 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.

Table 14 Bluetooth Profiles (Continued)

Profile	Description
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.
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

This section describes the method for enabling Bluetooth.

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

Disabling Bluetooth

This section describes the method for 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 displays.
8. Touch **Pair** on both devices.

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** displays 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.

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.

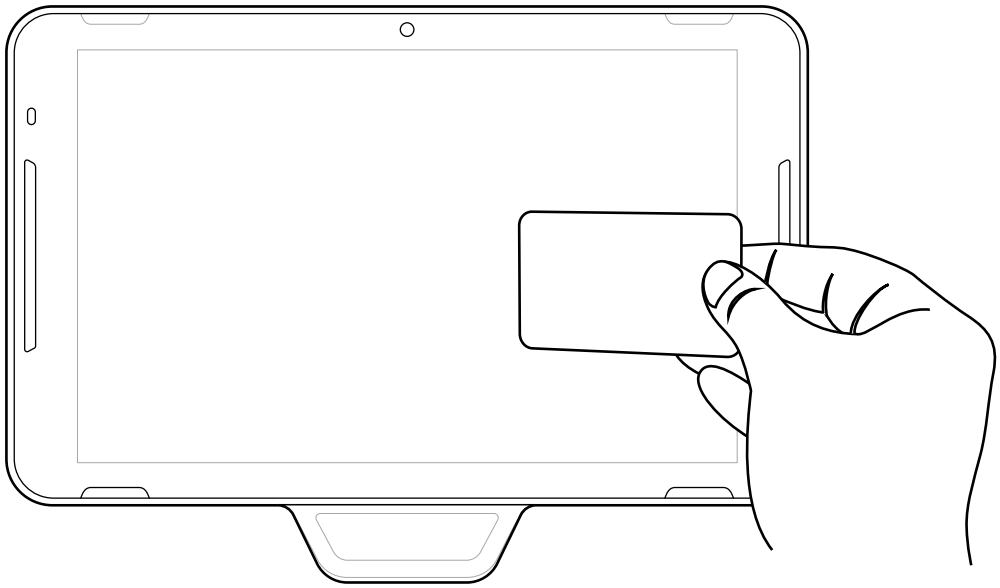
Using NFC, the device can:

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

Reading Contactless Cards

Read contactless cards using Near Field Communication (NFC).

1. Launch an NFC-enabled application.
2. Move the NFC card close to the device until the device detects the card.



3. Hold the card steadily until the application completes the transaction (usually indicated by the application).

Enterprise NFC Settings

Improve NFC performance by selecting which NFC features to use on the device.

- **Card Detection Mode** - Select a card detection mode
  - **Low** - Lower the NFC detection speed

  - **Standard** - Provides the optimal NFC detection speed
- **Supported Card Technology** - Select an option to detect only one NFC tag type, but reducing detection speed.
  - **All (Default)**
  - **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, go to: techdocs.zebra.com/nfcmgr/.

Accessories

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

Accessories List

For a complete list of the accessories available for the device, go to zebra.com/kc401 and select the **Accessories** tab.

Table 15 Accessories

Accessory	Part Number/Device	Description
Data Capture		
Scanner Edge Accessory	• KC401-SCNR-SR0 • KC401-SCNR-SR1 • KC401-SCNR-SR2	Adds hands-free barcode scanning using the SR500 Scan Engine. The accessory is available as three separately orderable SKUs with a 0°, +25°, or -25° scan angle. The accessory maintains the device IP65 sealing and is installed once during initial assembly. The device supports one Scanner Edge accessory at a time.
Bluetooth Ring Scanners	• RS507 • RS507x • RS5100 • RS6000	RS507 and RS507x (Bluetooth), RS5100 (Bluetooth for data, with optional USB-C connection for power), and RS6000 (Bluetooth for data).
Wireless Bluetooth Scanners	• DS8178 • DS2278 • DS3678	These wireless scanners are connected through bluetooth.
Wired USB Scanners	• DS3608 • LI3608	These USB scanners are connected through a USB host port.
Power		

Table 15 Accessories (Continued)

Accessory	Part Number/Device	Description
DC power supply	PWR-BGA12V36W0WW	Powers the device from a 5.4 V or 12 V source (up to 3 A) through the 5.5 mm x 2.1 mm DC input jack, including the 12 V 3 A power supply unit.
DC cable adapter (CBL-DC-383A1-01)	MISC-KC401-PLUGCONV	Connects legacy CC6000 power adapters (PWR-BUA5V16W0WW) to the device. When a 5.4 V supply is detected, the device applies a power profile that limits certain features to keep power consumption within 16 W.
Power over Ethernet (PoE)	N/A	Powers the device through the RJ45 Ethernet port from power sourcing equipment that complies with 802.3at or 802.3bt Class 4 (30 W minimum).
Printers		
Wireless printers	• ZQ510 • ZQ520 • EZ320	ZQ510 and ZQ520 mobile printers support Bluetooth pairing using NFC. The EZ320 printer uses a generic Android printer application. Supported printer applications: Zebra Printer Setup Utility, Zebra Utilities, and Print Connect.
Audio		
Bluetooth headsets	• C300-XT • C400-XT • B350-XT • B550-XT • (Zebra) HS3100	The devices has been tested to work with these bluetooth enabled headsets.
Wired USB-C headsets	• EHLG1WRFD-USBC-WA • HDST-USBC-PTT1-01	Standard Google-compliant USB-C headsets and the Workforce Audio full-duplex earpiece.
Payment		
Mobile Payment Module (standalone)		Bluetooth-based mobile payment modules in standalone mode: Verifone e285 and Ingenico Link2500i.
Mounting		
Pole Mount Kit	KT-152096-03	Pole mount bracket allows kiosk to be mounted directly to a pole with dedicated power supply storage shelf. • Compatible with KC401 and CC6000 • 100mm (3.94 in.) x 100mm (3.94 in.) VESA Mount • Includes mounting hardware to attach kiosk to bracket as well as a security screw to lock the device safely onto the mount

Table 15 Accessories (Continued)

Accessory	Part Number/Device	Description
Wall Mount Kit with Shelf	KT-152097-03	Wall mount bracket with dedicated shelf to store CC6 or KC401 device power supply. • Compatible with KC401 and CC6000 • 100mm (3.94 in.) x 100mm (3.94 in.) VESA Mount • Includes mounting hardware to attach kiosk to bracket as well as a security screw to lock the device safely onto the mount
Wall Mount Kit	KT-152097-04	Wall mount bracket without dedicated shelf for device power supply. • Compatible with KC401 and CC6000 • 100mm (3.94 in.) x 100mm (3.94 in.) VESA Mount • Includes mounting hardware to attach kiosk to bracket as well as a security screw to lock the device safely onto the mount
Thin Wall Mount Kit	KT-152098-03	Low-profile wall mount bracket with dedicated shelf to store CC6 or KC401 device power supply. • Compatible with KC401 and CC6000 • 100mm (3.94 in.) x 100mm (3.94 in.) VESA Mount • Includes mounting hardware to attach kiosk to bracket as well as a security screw to lock the device safely onto the mount
Kiosk and Printer	BRKT-DPA-SK1-01	Unified mounting solution that securely holds both a kiosk tablet and desktop thermal printer. • Compatible with KC401 and CC6000 • Dual-standard 75mm (2.95 in.) x 75mm(2.95 in.) or 100mm (3.94 in.) x 100mm (3.94 in.) VESA Mount • Includes mounting hardware to attach kiosk to bracket as well as a security screw to lock the device safely onto the mount

Scanner Edge Accessory

The Scanner Edge Accessory adds hands-free barcode scanning to the device using the SR500 imager.

The accessory is available as three separately orderable SKUs with a +25°, 0°, or -25° scan angle, so the scan field can be matched to the mounting position. It attaches to either the landscape or portrait edge interface location; the device supports one Scanner Edge Accessory at a time.

The accessory is installed once during initial assembly, uses captive mounting screws, and maintains the device IP65 sealing when installed. The device detects automatically whether the accessory is installed.

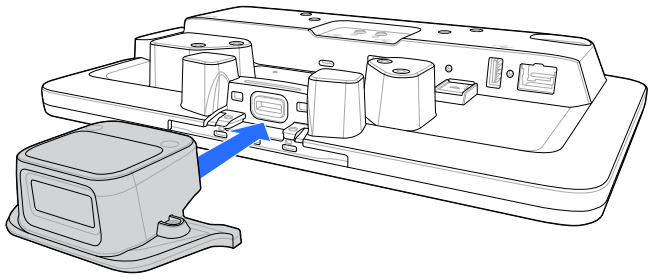
Installing the Scanner Edge Accessory

Install the optional Scanner Edge Accessory to enable barcode scanning capabilities.

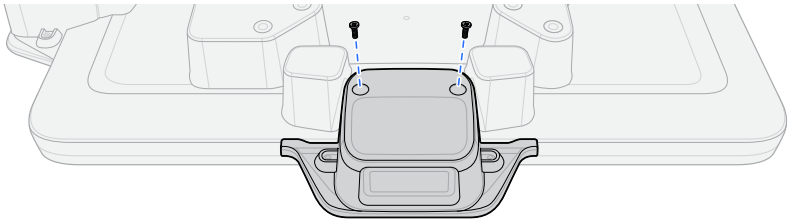
For a list of supported barcode formats, see Data Capture Supported Symbologies.

NOTE: There are two available slots to support either portrait or landscape orientations.

1. Remove the Scanner Edge Accessory from the packaging.
2. Slide the Scanner Edge Accessory into the KC401 Interactive Kiosk scanner slot.



3. Ensure the scanner is fully seated in the slot.
4. Tighten the screws in the scanner module.



NOTE: The screws for the edge scanner are shown for demonstration. The screws are captive and part of the scanner assembly.

The Scanner Edge Accessory is installed and ready for use.

Using the Scanner Edge Accessory

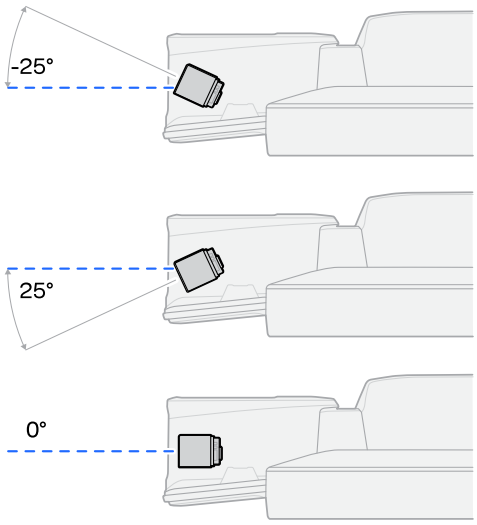
After installation, present barcodes to the Scanner Edge accessory to capture data with a scan-enabled application.

NOTE: Reading a barcode requires a scan-enabled app. Use the DataWedge app to enable the scanner to decode barcode data and display the barcode content.

1. Configure your KC401 Interactive Kiosk for barcode scanning.
2. Position the barcode in front of the Scanner Edge Accessory.

NOTE: Your scanner's decode angle varies based on the model. The view is either:

- Backward-tilted (-25°)
- Forward-tilted (25°)
- Centered



The KC401 Interactive Kiosk beeps and the LED flashes, indicating a successful barcode read.

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 websites.

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 website, 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.

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. After 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!** displays.
5. Touch **Back**.
6. Touch **System** > **Developer options**.
7. 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/emdk-for-android/about/.

StageNow for Android

StageNow is Zebra's Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles and can deploy to devices by scanning a barcode or reading a tag.

The StageNow Staging Solution includes the following components:

- The StageNow Workstation tool installs on the staging workstation (host computer) and lets the administrator 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 or read an NFC tag) to deliver staging material to the device.

For more information, go to techdocs.zebra.com/stagenow/.

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, go to techdocs.zebra.com/gmsmgr/.

ADB USB Setup

To use the Android Debug Bridge (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 for details on setting up the development SDK.

The ADB and USB drivers for Windows and Linux are available on the Zebra Support Central website at 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!** displays.
5. Touch **Back**.
6. Touch **System** > **Developer options**.
7. Slide the **USB debugging** switch to the **ON** position.
8. Touch **OK**.
9. Connect the device to the host computer using the USB Cable.

   The **Allow USB debugging?** dialog box displays 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.
10. Touch **OK** or **Allow**.
11. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
12. Type `adb devices`.

    The following displays:

    ```
    List of devices attached          XXXXXXXXXXXXXXX device
    ```

    Where XXXXXXXXXXXXXXX is the device number.

    NOTE: If device number does not display, ensure that ADB drivers are installed properly.
13. 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 both **Reset** buttons until the **Restart** option displays, and then release both buttons.

   The device restarts if the buttons are held for longer than three seconds.
2. Touch **Restart**.
3. Press and hold the **Volume Up** button.

   The System Recovery screen displays.

Entering Fastboot Mode

Enter Android Fastboot mode using the Reset and Volume buttons.

1. Press and hold both **Reset** buttons until the **Restart** option displays, and then release both buttons.

   The device restarts if the buttons are held for longer than three seconds.
2. Touch **Restart**.
3. Press and hold the **Volume Down** button.

   The Fastboot screen displays.

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 displays 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. Touch **System** > **Developer options**.
5. Enable **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.

Installing Applications Using Wireless ADB

Use ADB commands to install an application onto the device.

Go to the Zebra Support & Downloads website at 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. 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.
3. Slide the **USB debugging** switch to the **ON** position.
4. At the prompt, touch **OK**.
5. 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**.

6. Touch **Wireless debugging**.

   The **Wireless debugging** screen displays.

7. Note the IP address and Port on the **Wireless debugging** screen.

8. Touch **Pair device with pairing code**.

   The **Pair with device** dialog box displays.

9. 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.

10. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.

11. Type `adb pair XX.XX.XX.XX:XXXXX`

    where XX.XX.XX.XX:XXXXX is the IP address and port number from the **Pair with device** dialog box.

12. Press **Enter**.

13. Type the pairing code from the **Pair with device** dialog box.

14. Press **Enter**.

15. Type `adb connect XX.XX.XX.XX:XXXXX`

    where XX.XX.XX.XX:XXXXX is the IP address and port number from the **Wireless debugging** screen.

16. Press **Enter**.

    The device is now connected to the host computer.

17. Type `adb devices`.

    The following displays:

```
List of devices attached          XXXXXXXXXXXXXXX device
```

    Where XXXXXXXXXXXXXXX is the device number.

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

18. Press **Enter**.

19. Type `adb install <file>`.

    where <file> = the path and filename of the apk file.

20. Press **Enter**.

21. On the host computer, type:

    `adb disconnect`.

22. 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) 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 displays in the App list.

Uninstalling an Application

Free up device memory by removing unused apps.

1. Go to **Settings**.
2. Touch **Apps**.
3. Touch **See all apps** to view all apps in the list.
4. Scroll through the list to the app.
5. Touch the app.

   The **App info** screen displays.
6. Touch **Uninstall**.
7. 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, before use, you format the microSD card on the device.

Go to the Zebra Support & Downloads website at 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 both **Reset** buttons until the **Restart** option displays, and then release both buttons.

   The device restarts if the buttons are held for longer than three seconds.
3. Touch **Restart**.
4. Press and hold the **Volume Up** button.

   The System Recovery screen displays.
5. Press the **Volume Down** button to navigate to **Apply upgrade from SD card**.
6. Press the **Volume Up** button to select.
7. Press the **Volume Down** button to navigate to the System Update file.
8. Press both **Reset** buttons.

   The System Update installs and then the device returns to the Recovery screen.
9. Press the **Volume Up** button to reboot the device.

Performing a System Update Using ADB

Use ADB to perform a system update.

Go to the Zebra Support & Downloads website at 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. Touch **System** > **Developer options**.
4. Slide the switch to the **ON** position.
5. Slide the **USB debugging** switch to the **ON** position.
6. 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.

7. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
8. Touch **OK** or **Allow**.
9. On the device, press the **Volume Down** button to navigate to **Apply upgrade from ADB**.
10. On the device, press the **Volume Up** button to select.
11. Press **Enter**.
12. Press **Enter** or **Power** to select.
13. On the device, press both **Reset** buttons to reboot the device.
14. Press **Enter**.

    The System Update installs (progress displays as a percentage in the Command Prompt window) and then the System Recovery screen displays on the device.

If you are not able to enter Android Recovery mode through the adb command, see Entering Android Recovery Manually.

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. Touch **System** > **Reset options** > **Erase all data (enterprise reset)**.
3. Touch **Erase all data** twice to confirm the Enterprise Reset.

Performing an Enterprise Reset Using microSD Card

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

Go to the Zebra Support & Downloads web site at 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 both **Reset** buttons until the **Restart** option displays, and then release both buttons.

   The device restarts if the buttons are held for longer than three seconds.
3. Touch **Restart**.
4. Press and hold the **Volume Up** button.

   The System Recovery screen displays.
5. Press the **Volume Down** button to navigate to **Apply upgrade from SD card**.
6. Press the **Volume Up** button to select.
7. Press the **Volume Down** button to navigate to the Enterprise Reset file.
8. Press both **Reset** buttons to commit the selection.

   The Enterprise Reset occurs and then the device returns to the Recovery screen.
9. Press the **Volume Up** 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 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. Touch **System** > **Developer options**.
4. Slide the switch to the **ON** position.
5. Slide the **USB debugging** switch to the **ON** position.
6. 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.
7. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
8. Touch **OK** or **Allow**.
9. On the device, press the **Volume Down** button to navigate to **Apply upgrade from ADB**.
10. On the device, press the **Volume Up** button to select.
11. Use **Volume Up** and **Volume Down** to navigate to **Full OTA Package**.
12. On the device, press both **Reset** buttons to reboot the device.

If you are not able to enter Android Recovery mode through the adb command, see Entering Android Recovery Manually.

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 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 both **Reset** buttons until the **Restart** option displays, and then release both buttons.

   The device restarts if the buttons are held for longer than three seconds.
3. Touch **Restart**.
4. Press and hold the **Volume Up** button.

   The System Recovery screen displays.
5. Press the **Volume Down** button to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
6. Press the **Volume Up** button to select.
7. Press the **Volume Down** button to navigate to the Factory Reset file.
8. Press both **Reset** buttons to commit the selection.

   After the Factory Reset the device returns to the Recovery screen.
9. Press the **Volume Up** 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 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. Touch **System** > **Developer options**.
4. Slide the **USB debugging** switch to the **ON** position.
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`.

   The following displays:

   ```
   List of devices attached
   XXXXXXXXXXXXXXX device
   ```

   Where XXXXXXXXXXXXXXX is the device number.

   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. On the device, press the **Volume Down** button to navigate to **Apply upgrade from ADB**.
12. On the device, press the **Volume Up** 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 Factory Reset package installs, and then the System Recovery screen appears on the device.
15. On the device, press the **Volume Down** button to navigate to **Reboot system now**, and then press both **Reset** buttons to select.

    The device reboots.

If you are not able to enter Android Recovery mode through the adb command, see Entering Android Recovery Manually.

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 - three 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. Touch **System** > **Advanced** > **Developer options**.

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. 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. Touch **Apps**.
3. Touch **See all XX apps** to view all apps on the device.
4. Touch ⋮ > **Show system** to include system processes in the list.
5. Touch an app, process, or service in the list to open a screen with details about it and, depending on the item, to change its settings, permissions, notifications and to force stop or uninstall it.

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.

Cleaning Instructions

This section provides instructions for cleaning the device.

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

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

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 types of disinfectants come in contact with metal on the device, prompt removal with an alcohol-dampened cloth or cotton swab after the cleaning step is critical.

Approved cleaners include:

- Purell Ethanol Wipes
- 409 Glass Cleaner
- Windex Blue

Harmful Ingredients

The following chemicals are known to damage the plastics on the device and should not come in contact with the device: acetone; ketones; ethers; aromatic and chlorinated hydrocarbons; 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.

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

This section lists the necessary cleaning materials.

- Alcohol wipes with 70% isopropyl alcohol
- Lens tissue
- Cotton-tipped applicators
- 70% Isopropyl alcohol
- Can of compressed air for electronics with a dispenser tube

Cleaning Frequency

This section explains how often you must clean the device.

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 and display of the device.

For more information on cleaning the device connector, refer to Cleaning the Connectors.

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 the 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 16 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 displays 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 **Settings** > **Storage** > **MANAGE STORAGE**. Select the unused program(s) and tap **FREE UP**.
	Too many applications installed on the device.	Remove user-installed applications on the device to recover memory. Go to **Settings** > **Apps & notifications**. Select the unused programs and touch **Uninstall**.
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 16 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.	If the user enters an incorrect password eight times, the user is requested to enter a code before trying again. If the user forgot the password, contact system administrator.

Technical Specifications

For device technical specifications, go to zebra.com. This section also provides decode distances for the device.

Edge Scanner Decode Distances

Typical decode distances for the SR500 scan engine used by the Scanner Edge Accessory.

Measurements are taken straight from the face of the scan engine exit window to the surface of the barcode, using a photographic-quality barcode at an 18° tilt pitch angle.

Table 17 Decode Distances - Ambient Light (30 fcd)

Barcode Type	Near Distance (typical)	Far Distance (typical)
3 mil Code 39	7.6 cm/3.0 in	14.7 cm/5.8 in
5 mil Code 128	5.8 cm/2.3 in	24.9 cm/9.8 in
5 mil PDF417	7.6 cm/3.0 in	20.1 cm/7.9 in
6.67 mil PDF417	6.4 cm/2.5 in	25.7 cm/10.1 in
10 mil Data Matrix	5.3 cm/2.1 in	27.9 cm/11.0 in
100% UPCA	4.1 cm/1.6 in*	63.2 cm/24.9 in
15 mil Code 128	7.1 cm/2.8 in*	70.6 cm/27.8 in
20.0 mil Code 39	6.6 cm/2.6 in*	91.7 cm/36.1 in

Table 18 Decode Distances - Dark Room (0.1 fcd)

Barcode Type	Near Distance (typical)	Far Distance (typical)
3 mil Code 39	7.6 cm/3.0 in	14.7 cm/5.8 in
5 mil Code 128	5.8 cm/2.3 in	24.9 cm/9.8 in
5 mil PDF417	7.6 cm/3.0 in	20.1 cm/7.9 in
6.67 mil PDF417	6.4 cm/2.5 in	25.7 cm/10.1 in
10 mil Data Matrix	5.3 cm/2.1 in	27.9 cm/11.0 in
100% UPCA	4.1 cm/1.6 in*	58.9 cm/23.2 in

Table 18 Decode Distances - Dark Room (0.1 fcd) (Continued)

Barcode Type	Near Distance (typical)	Far Distance (typical)
15 mil Code 128	7.1 cm/2.8 in*	63.8 cm/25.1 in
20.0 mil Code 39	6.6 cm/2.6 in*	71.6 cm/28.2 in

* Limited by the width of the barcode in the field of view. Refer to the SR500 Integration Guide for details.

Device Technical Specifications

Reference this table for KC401 Interactive Kiosk technical specifications.

Feature	Specification
Operating system	Android 15 (GMS)
Processor	Qualcomm QCS6690 FP1
Memory (RAM)	6 GB LPDDR5
Storage (Flash)	64 GB UFS 2.2
Display	10.1 in., 1280 x 800, 300 nits
Touch panel	Capacitive, multi-touch (4-point), finger/stylus/glove
Front camera	5 MP, fixed focus
WLAN	Wi-Fi 7 (802.11be); 2.4 GHz, 5 GHz, and 6 GHz bands
Bluetooth	Bluetooth 6.0, Class 1, Bluetooth Low Energy (BLE)
NFC	Supported (Google Smart Tap, Apple VAS)
Ethernet	RJ-45, 10/100/1000 Mbps
USB	1x USB-C (3.1), 2x USB-A (2.0)
Power	DC input (5.4 V or 12 V, up to 3 A), PoE (802.3at/802.3bt Class 4), or USB-C
Dimensions	278 x 183 x 36.2 mm (10.9 x 7.2 x 1.4 in.)
Weight	< 980 g (2.16 lb)
Sealing	IP65
Operating temp	0°C to 40°C (32°F to 104°F)
Expansion	microSD (up to 2 TB SDXC)
Scanner (optional)	SR500/SE4730 Scanner Edge Accessory
Physical buttons	Volume Up, Volume Down, Reset (x2)

Feature	Specification
Sensors	Proximity, accelerometer, gyroscope
Audio	2 speakers, 2 microphones