KC50

Kiosk Computer

Product Reference Guide

ZEBRA

MN-005073-02EN Rev. A

Copyright

2025/02/26

Terms of Use

Proprietary Statement

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

Product Improvements

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

Liability Disclaimer

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

Limitation of Liability

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

Contents

Contents

About this Guide

This guide provides information about setting up and using the KC50 Kiosk computer. Some screens shown in the guide may differ from the actual screens shown on the device.

This guide includes Android 13 operating system (OS) and above.

Configurations

This guide covers the following configurations of the KC50 kiosk computers.

Table 1 KC50 Configurations

Configuration	Display	Memory/Storage
KC50A22-G0B1C0-NA	55.88 cm (22 in.)	8 GB RAM, 128 GB Storage
KC50A22-G0B1C0-A6	55.88 cm (22 in.)	8 GB RAM, 128 GB Storage
KC50A22-G0B1C0-TR	55.88 cm (22 in.)	8 GB RAM, 128 GB Storage
KC50E22-G0A200-NA	55.88 cm (22 in.)	6 GB RAM, 64 GB Storage
KC50E22-G0A200-A6	55.88 cm (22 in.)	6 GB RAM, 64 GB Storage
KC50E22-G0A200-TR	55.88 cm (22 in.)	6 GB RAM, 64 GB Storage
KC50A15-G0B1C0-NA	38.1 cm (15 in.)	8 GB RAM, 128 GB Storage
KC50A15-G0B1C0-A6	38.1 cm (15 in.)	8 GB RAM, 128 GB Storage
KC50A15-G0B1C0-TR	38.1 cm (15 in.)	8 GB RAM, 128 GB Storage
KC50E15-G0A200-NA	38.1 cm (15 in.)	6 GB RAM, 64 GB Storage
KC50E15-G0A200-A6	38.1 cm (15 in.)	6 GB RAM, 64 GB Storage
KC50E15-G0A200-TR	38.1 cm (15 in.)	6 GB RAM, 64 GB Storage

Notational Conventions

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

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

Icon Conventions

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

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

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

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

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

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

Service Information

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

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 Version

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:
   - Device name
   - Legal information
   - Software components
   - Model
   - Android version
     - Android security patch level
     - Android security patch version
     - Google Play system update
     - Baseband version
     - Kernel version
     - Build Fingerprint
     - Build number
     - Android Security Update
   - IP address
   - Wi-Fi MAC address
   - Device Wi-Fi MAC address
   - Bluetooth address
   - Up time
   - Build Fingerprint
   - Build number

Determining the Serial Number

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

1. Swipe up on the screen to the app list and then touch .
2. Touch **About phone**.

3. Touch **Model**.

The Serial number displays on the Model screen.

Getting Started

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

Unpacking the Device

Unpack the device and examine the contents before setting up the device.

1. Carefully remove the computer from the box.
2. Verify the following items are in the box:
   - KC50
   - Bags containing two back covers
   - Bag containing four M4 screws and a size 3 hex key
   - Regulatory guide
3. Inspect the equipment for any damage. If any equipment is missing or damaged, contact the Global Customer Support Center immediately.

IMPORTANT: Leave the protective film that covers the screen on the device until it is mounted/installed.

Device Features

This section lists the features of the device.

Figure 1 Front View Features

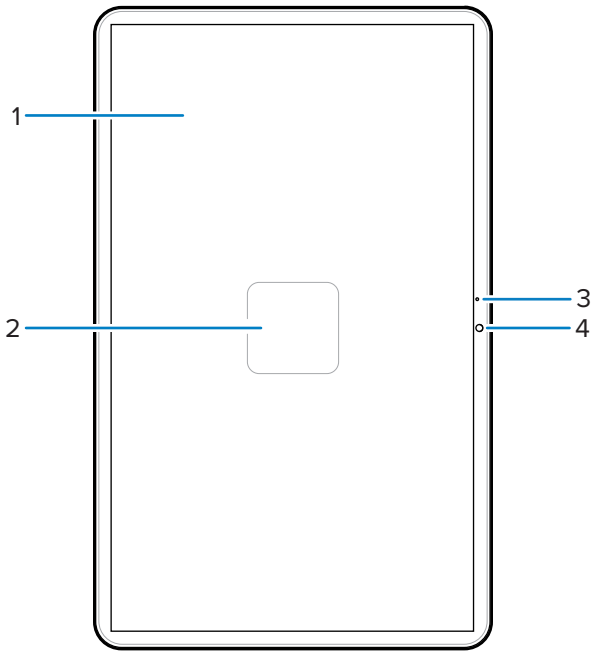


Table 2 Front View Features

Number	Item	Description
1	Touchscreen	Displays all information needed to operate the device.
2	NFC antenna	Provides communication with other NFC-enabled devices.
3	Main microphone	Use for communications in Handset mode.
4	Front camera	Captures photos, videos, and STAGENOW barcode data.

Figure 2 Rear View with Back Covers Removed Features

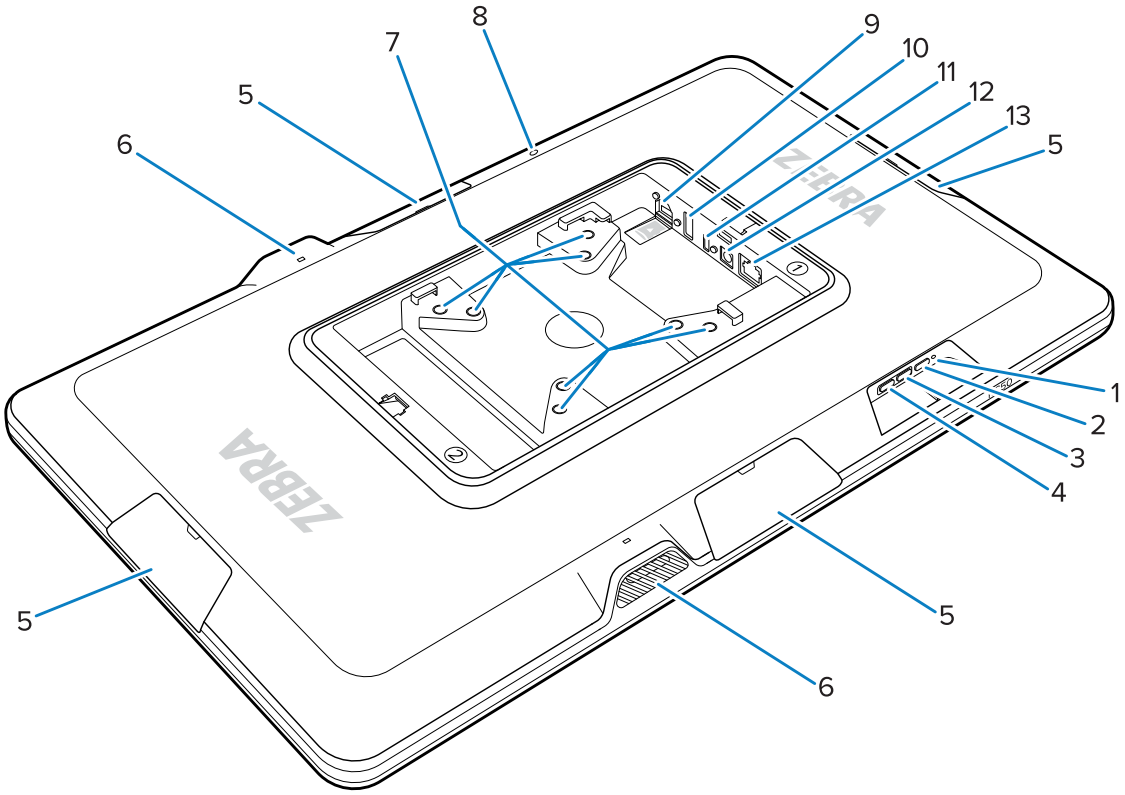


Table 3 Rear View Features

Number	Item	Description
1	Power LED	Indicates device power status.
2	Power button	Wakes the device.
3	Volume up button	Increases device volume (programmable).
4	Volume down button	Decreases device volume (programmable).
5	Accessory port cover	Protects the accessory port from dust/debris (removable).
6	Speaker	Provides audio output.
7	VESA-compliant mounting inserts	M4 threaded inserts - 100 mm (3.94 in.) and 75 mm (2.95 in.) squares.
8	Rear microphone	Used for noise cancellation.
9	microSD slot (bottom) and GPIO port (top)	The microSD slot holds a mircoSD card for additional storage capacity. **NOTE:** The GPIO port is reserved for future use.
10	USB-A port	USB-A input.

Table 3 Rear View Features (Continued)

Number	Item	Description
11	USB-C display port	Provides display information to a secondary screen such as the TD50.
12	DC power port	DC power supply.
13	Ethernet port	Accepts an RJ45 connector.

Setting up the Device

Set up the device by connecting a power supply, mounting the device, and installing optional accessories.

1. (Optional) Install a microSD card.
2. Connect the device to a power supply.
3. Mount the device.

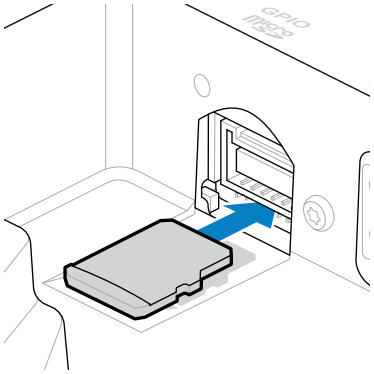
NOTE: If you are using an SC-2000 stand, refer to the SC-2000 Installation Guide for detailed instructions on mounting the device on the stand.

4. (Optional) Install the accessories.

Installing a microSD Card

Install a microSD card to increase the device's storage capacity.

1. Orient the microSD with the contacts facing down.
2. Push the microSD card into the slot until you engage the spring mechanism, and the card clicks into place.



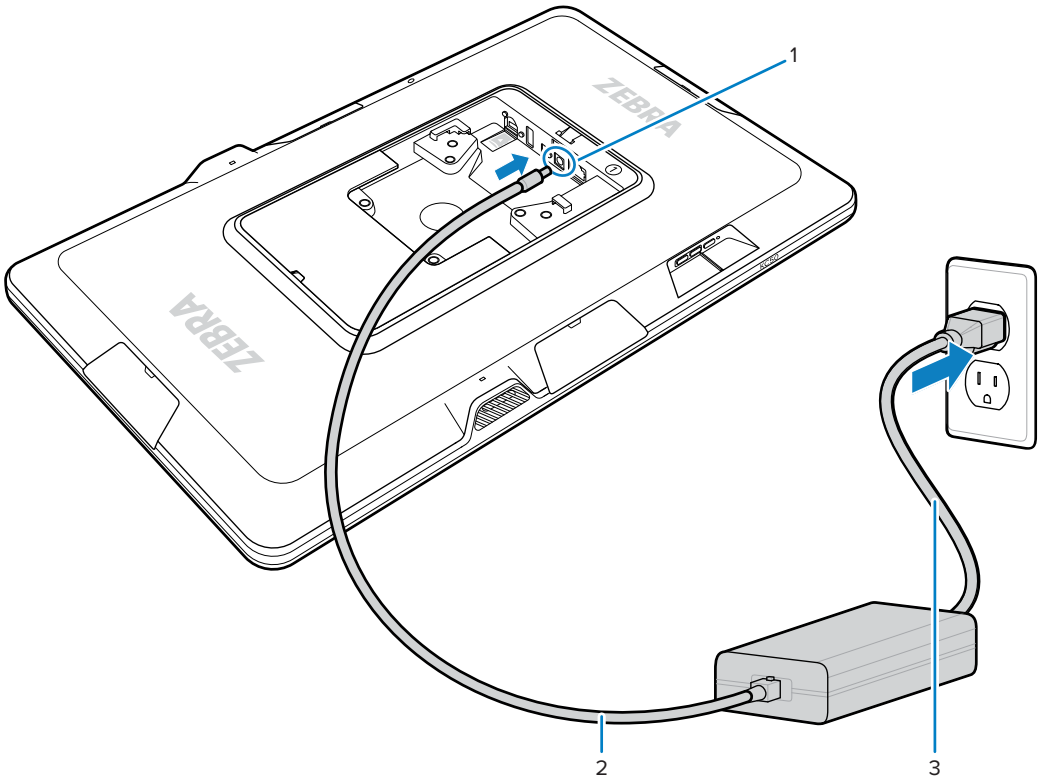
Connecting a DC Power Supply and Powering on the Device

The KC50 Kiosk computer requires an external power supply with either a DC line or Ethernet cable.

IMPORTANT: If you are using an SC-2000 stand, refer to the SC-2000 Installation Guide to connect the power supply.

1. Connect the DC line to the power port of the device (1).

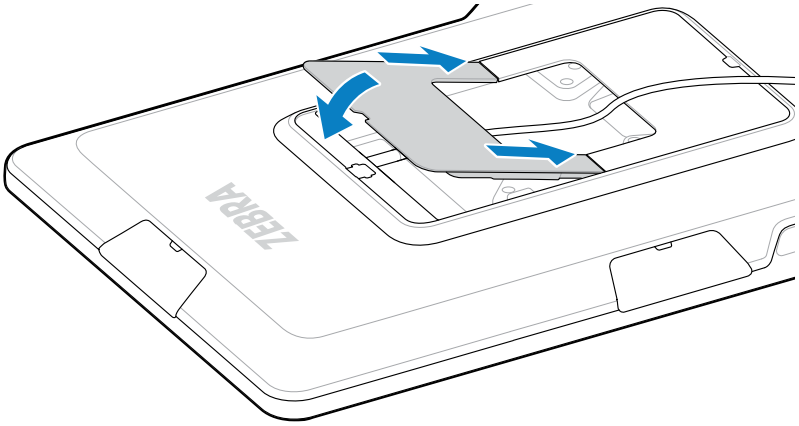
2. Connect the DC line cord to the power adapter (2).
3. Connect the AC line cord to a power supply (3).



The device turns on when connected to a power supply.

4. Place the cover backs onto the device and press firmly until they click into place.

NOTE: Insert the cover marked 1 on the side of the device marked 1. Insert the cover marked 2 on the side of the device marked 2.



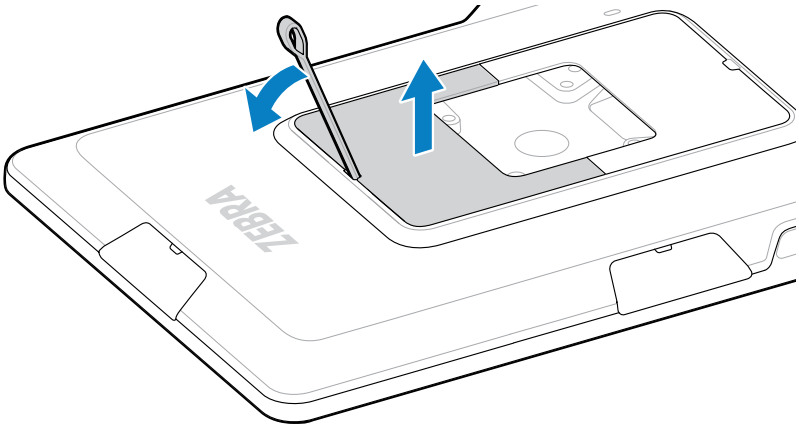
Connecting an Ethernet Power Supply and Powering on the Device

The KC50 Kiosk Computer requires an external power supply. Connect an Ethernet cable to power the device.

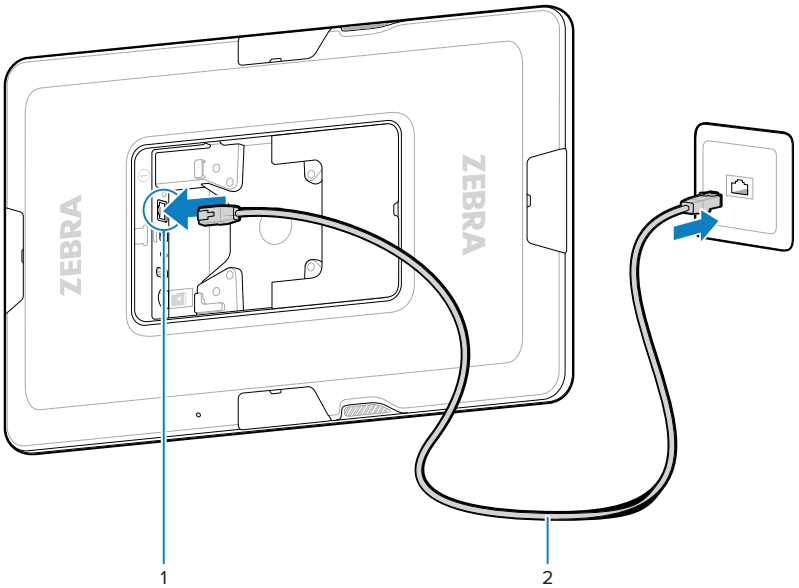
Ensure your network provides enough energy to power the device. Refer to the PoE-capable network switch or power injector configuration guide and the Power over Ethernet section for more information.

IMPORTANT: If you are using a Zebra stand, refer to the KC50 Stand Installation Guide to connect the power supply.

1. Insert the MC18 removal tool (sold separately) into the slot in the back cover to remove the cover from the device.



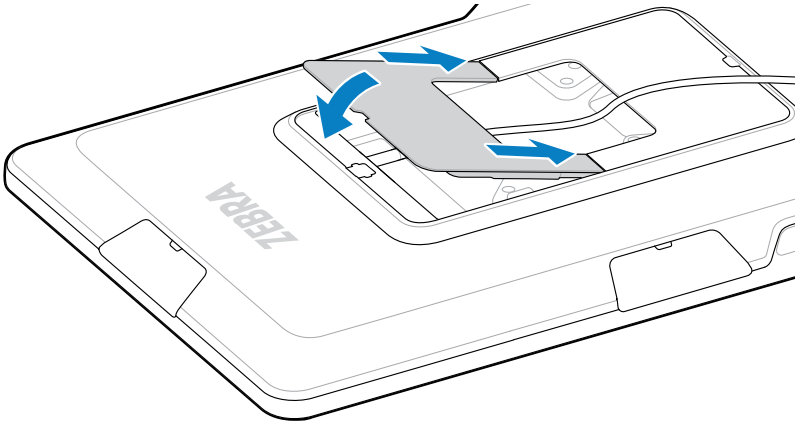
2. Connect the Ethernet cable to the Ethernet port of the device (1).
3. Connect the Ethernet cable to the PoE accessory (2).



The PoE accessory must be Class 4 or higher 802.3at/bt compliant Power Sourcing Equipment (PSE). The device turns on when it successfully negotiates with the PSE.

NOTE: Avoid excessive disconnecting/reconnecting the RJ45 on a PoE system to minimize electrical arcing on the RJ45 connector.

4. Place the cover back onto the device and press firmly until it clicks into place.



The device is ready for use.

Mounting the KC50

The VESA-compliant mounting inserts on the back of the device allow you to mount the device in different ways based on your floor plan and system configuration.

The device includes M4 threaded inserts spaced in 75 mm (2.95 in.) and 100 mm (3.94 in.) squares. You can mount the device onto a VESA mounting plate or create mounting holes in a wall, cabinet, or desk to secure the device in place.

- Use the correct hardware to mount the device.

Kiosk Computer Stand	Refer to the SC-2000 Installation Guide. Use the included M4 screws to secure the device to the stand.
VESA mounting plate	Use the included M4 screws to secure the device to the VESA plate.
Other	Use M4 screws long enough to secure the device to your mounting solution. **CAUTION:** The device should only be mounted by a trained professional to avoid the risk of fall injury.

- If you are not using the SC-2000 stand as a mounting solution, use good cable management practices to keep the cables inserted in the device. Use cable ties or hook and loop ties to secure the cables and prevent them from disengaging from the device.
- If you are attaching the Z-Flex scanner to the device, mount the device so that barcodes are comfortably placed 8 to 20 cm (3 to 8 in.) below the scanner.

Turning off the Device

This section describes how to turn off the device.

1. Press and hold the Power button until the menu appears.

2. Touch **Power off**.

Turning off the Display

Press and release the **Power** button to turn off the display.

Using the Device

This section explains how to use the device.

Waking the Device

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

1. To wake the device from Sleep mode, press Power.

   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 the 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.

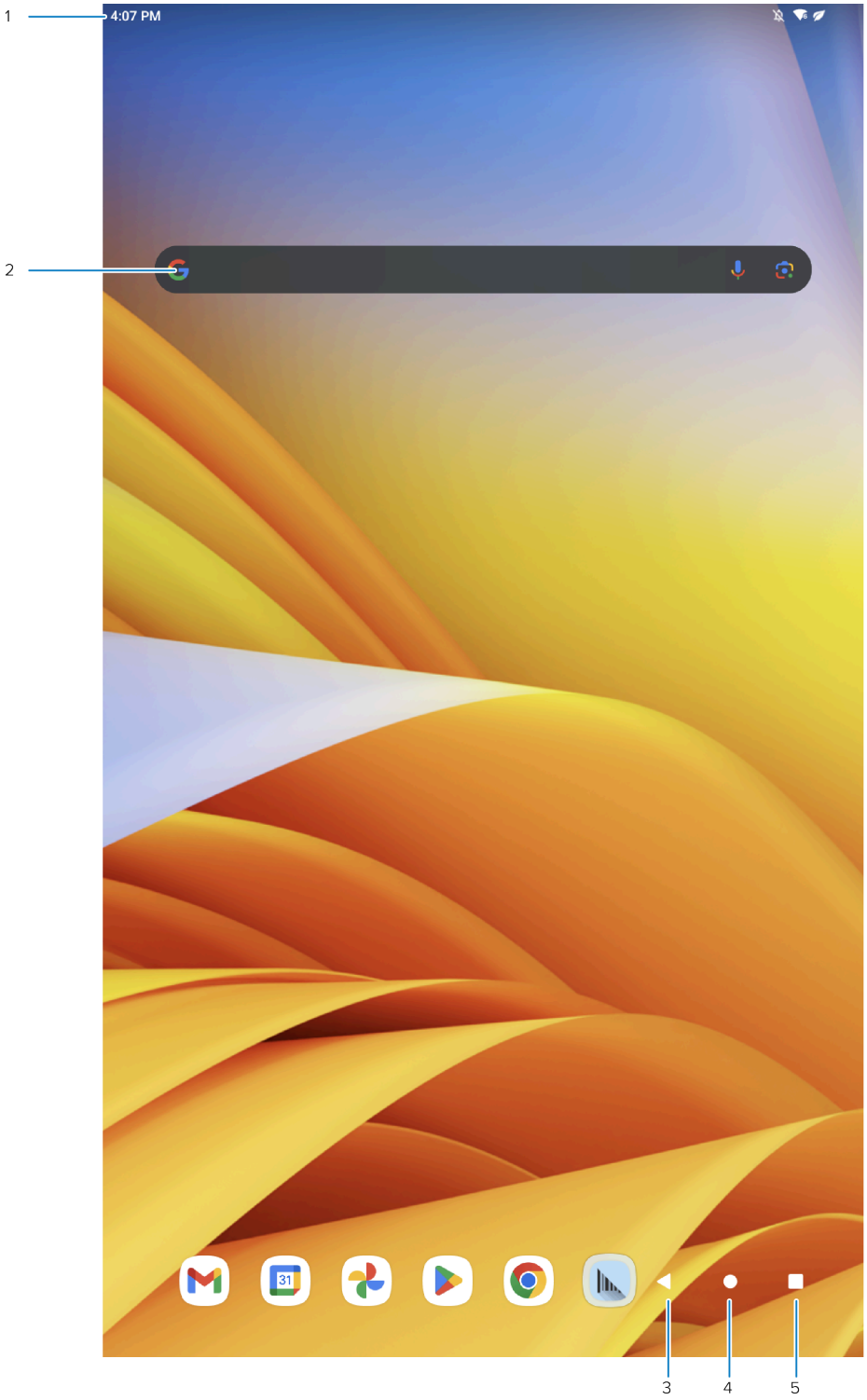
NOTE: If you enter the PIN, password, or pattern incorrectly five times, you must wait 30 seconds before trying again. If you forget the PIN, password or pattern, contact your system administrator.

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 and swipe to wake up the device. The Home screen provides four additional screens to place widgets and shortcuts. Touch and hold an icon, and move it for the option to place icon to place the icon on one of the other screens. Swipe the Home screen left or right to view the additional screens.

Figure 3 Home Screen



1	Status bar	Displays the time, status icons (right side), and notification icons (left side).
2	Search bar	Search with Google.

3	Back	Displays the previous screen.
4	Home	Displays the home screen.
5	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 appear.
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 (left side), and status icons (right side).

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

Figure 4 Notifications and Status Icons

1	Notification icons
2	Status icons

Notification Icons

Notification icons indicate app events and messages.

Table 4 Notification Icons

Icon	Description
•	More notifications are available for viewing.
	Data is synching.
31	Indicates an upcoming event.

Table 4 Notification Icons (Continued)

Icon	Description
	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.
	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.

Status Icons

Status icons display system information for the device.

Table 5 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.
	Connected to an Ethernet network.
	Speakerphone enabled.
	Indicates that a BT headset is connected to the device.

Managing Notifications

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

- 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.

- If the device is locked, press the power button and swipe down once.
- 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 6 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.
	**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.

Table 6 Quick Access Panel Icons (Continued)

Icon	Description
	**Night Light**- Tint the screen amber to make it easier to look at the screen in dim light. Set Night Light to turn on automatically from sunset to sunrise, or at other times.
	**Screen Cast**- Share phone content on Chromecast or a television with Chromecast built-in. On the Cast screen, check the "enable wireless display" option, and then touch "cast screen" to display a list of devices. Touch a device in the list to begin casting.
	**Dark Theme**- Toggles dark theme on and off. Dark themes reduce the luminance emitted by the screen while meeting minimum color contrast ratios. It helps improve visual ergonomics by reducing eye strain, adjusting brightness to current lighting conditions, and facilitating screen use in dark environments while conserving battery power.
	**Focus mode**- Turn on to pause distracting apps. To open Focus mode settings, touch and hold.
	**Bedtime mode**- Turn grayscale on and off. Grayscale turns the screen black and white, reducing phone distractions and improving battery life.
	**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.
	**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.

Waking the Device

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

1. To wake the device from Sleep mode, press Power.

   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 the 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.

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.

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, you can power the device with an 802.3at/bt-compliant PoE injector or network switch.

PoE requires sufficient power from the network, the switch, and the injector. A Network Administrator will ensure 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 ANSI/TIA 568.2-D standard. The testing prevents unbalanced resistances in the cabling usage which may cause data bit errors, or a breakdown in consistent power delivery to the device.

Setting up PoE

This section provides guidelines to correctly set up your device's PoE. For more information on configuring your PoE, go to zebra.com/techdocs-kc50_kiosk.

- Select a power class that will power your required ports, peripherals, and device brightness settings.
- Each power class profile defines default restrictions on USB ports, peripherals, and device brightness settings. Go to zebra.com/techdocs-kc50_kiosk for the power class profile definitions.
- 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 recommended standalone 802.3bt-compliant power injector. Class 8 (90 W or greater) injectors are recommended to allow the most flexibility for power budgeting.

Compatible with KC50	Incompatible with KC50
Microchip PD-9601GC 90 W PSE	PLUSPOE 60 W PSE
Microchip PD-9501GC/SP 60 W PSE	PLUSPOE 30 W PSE
Microchip PD-9001GR/SP 30 W PSE	YuanLey HG60A 60 W PSE
Wmo QPE088Gb1 30 W PSE	YuanLey HG30A 30 W PSE
	TP-link POE170S 60W PSE

- Select a Power Sourcing Equipment class that will provide sufficient power for your device. For the highest device functionality, the recommended class is Class 8, and the minimum functional requirement is Class 4.
- 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.

Settings

This section describes the settings on the device.

Accessing Settings

There are multiple ways to access settings on a device.

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

Display Settings

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

Setting the Screen Brightness Manually

Manually set the screen brightness using the touchscreen.

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

Setting Night Light

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

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

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

Setting Screen Rotation

By default, screen rotation is enabled.

To change the Home Screen rotation, go to Setting Home Screen Rotation.

1. Go to **Settings**.
2. Touch **Display**.
3. Touch **Auto-rotate screen**.

Setting Screen Timeout

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

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

Setting Font Size

Set the size of the font in systems apps.

1. Go to **Settings**.
2. Touch **Display** > **Display size and text**.
3. Touch a point on the **Font size** slider to set the font size.

Setting Display Size

The screen's display size can be adjusted larger or smaller.

1. Go to **Settings**.
2. Touch **Display** > **Display size and text**.
3. Touch a point on the **Display size** slider to set the screen display size.

Setting the Date and Time

The date and time are automatically synchronized using a NITZ server when the device is connected to a wireless network. You are only required to set the time zone or set the date and time if the wireless LAN does not support Network Time Protocol (NTP) or when not connected to a wireless network.

1. Go to **Settings**.
2. Touch **System** > **Date & time**.
3. Toggle **Set time automatically** off to manually set the date and time.
4. Touch **Date** to select the date in the calendar.
5. Touch **OK**.
6. 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**.
7. Touch **OK**.
8. Touch **Time zone** to select the current time zone from the list.
9. Touch **Update Interval** to select an interval to synchronize the system time from the network.
10. In **TIME FORMAT**, choose either **Use locale default** or **Use 24-hour format**.

Setting Sound Options

Set sound and vibration options for the the device.

1. Go to **Settings**.
2. Touch **Sound & vibration**.
3. Use the sliders to control the media, call, notification, and alarm volume on the device.

Sound Options

- **Media volume** - Controls the music, games, and media volume.
- **Call volume** - Controls the volume during a call.
- **Notification volume** - Controls the notification volume.
- **Alarm volume** - Controls the alarm clock volume.
- **Media volume** - Controls the music, games, and media volume.

- **Shortcut to prevent ringing** - Turn on the switch to make the device vibrate when a call is received (default – disabled).
- **Do Not Disturb** - Mutes some or all sounds and vibrations.
- **Media** - Shows the media player in Quick Settings while sound is playing, allowing quick access.
- **Shortcut to prevent ringing** - Select how the shortcut method prevents ringing.
- **Default notification sound** - Select a sound to play for all system notifications.
- **Default alarm sound** - Select a sound to play for alarms.
- **Other sounds and vibrations:**
  - **Screen locking sounds** - Play a sound when locking and unlocking the screen (default – enabled).
  - **Touch sounds** - Play a sound when making screen selections (default – disabled).
  - **Touch vibration** - Vibrate the device when making screen selections (default – enabled).
  - **Touch sounds** - Play a sound when making screen selections (default – enabled).
  - **Touch vibration** - Vibrate the device when making screen selections (default – enabled).
- **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.
- **Live Caption** - Automatically caption speech.
- **Always show icon when in vibrate mode** - Enable the vibrate mode status bar icon.

Setting Wake-Up Sources

By default, the device wakes from Sleep mode when the user presses **Volume Down** or **Volume Up**.

By default, the device wakes from suspend mode with the following:

- Volume down button.
- Volume up button.

1. Go to **Settings**.
2. Touch **Wake-Up Sources**.
   - **VOLUME_DOWN** - Programmable button on the side of the device.
   - **VOLUME_UP** - Programmable button on the side of the device.
3. Touch a checkbox.

   A check appears in the checkbox. The button is a wake-up source.

Remapping a Button

Buttons on the device can be programmed to perform different functions or as shortcuts to installed apps. For a list of key names and descriptions, go to techdocs.zebra.com.

1. Go to **Settings**.
2. Touch **Key Programmer**. A list of programmable buttons displays.
3. Select the button to remap.
4. Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.
5. Touch a function or application shortcut to map to the button.

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

6. If remapping the Back, Home, Search, or Menu button, perform a Soft Reset.

Keyboards

The device provides multiple keyboard options.

- On-screen keyboard
  - Gboard
  - Google Voice Typing
- Enterprise Keyboard

Keyboard Configuration

This section describes configuring the device's keyboard.

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.

Enabling Keyboards

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

Using the Android and Gboard Keyboards

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

Change the keyboard settings by touching and holding the comma icon on the keyboard. The keyboard settings screen opens.

Edit Text

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

Entering Numbers, Symbols, and Special Characters

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

Enterprise Keyboard

The Enterprise Keyboard contains multiple keyboard types.

NOTE: Only available with 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

1. Go to **Settings**.
2. Touch **System** > **Languages & input**.
3. Touch **Languages**.

   A list of available languages displays.
4. If the desired language is not listed, touch **Add a language** and select a language from the list.
5. Touch and hold to the right of the desired language, then drag it to the top of the list.

   The operating system text changes to the selected language.

Adding Words to the Dictionary

Words you use can be added to the system's dictionary to prevent them from being identified as misspelled.

1. Go to **Settings**.
2. Touch **System** > **Languages & input** > **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** > **Apps & notifications** > **Notifications**.

To view app notifications, touch **Settings** > **Apps & notifications** > **App info**, and then select an app.

Setting App Notifications

Configure the notifications settings for a specific app.

1. Go to **Settings**.
2. Touch **Notifications** > **App settings**.

   By default, the Most recent apps display on the **App notifications** screen.
3. Touch the drop-down menu and select one of the following:
   - Most recent
   - Most frequent
   - All apps
   - Turned off
4. Toggle app notification settings on and off.
5. Touch the app name to access further notification options.

   Options vary depending on the app.

Viewing Notifications

1. Go to **Settings**.
2. Touch **Apps & Notifications**.
3. Scroll down to **Notifications** to view how many apps have notifications turned off.

Controlling Lock Screen Notifiations

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

1. Go to **Settings**.
2. **Notifications** > **Notifications on lock screen** and select one of the following:
   - **Show alerting and silent notifications (default)**
   - **Show alerting notifications only**
   - **Don’t show notifications**.

Applications

Apart from the standard pre-installed Android apps, the device comes with Zebra apps installed. This section lists and explains the Zebra apps on the device.

Installed Applications

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

Table 7 Apps

Item	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.
	**License Manager** - Use to manage software licenses on the device.
	**RxLogger** - Use to diagnose device and app issues.
	**Camera** - Take photos or record videos.
	**StageNow** - Allows the device to stage a device for initial use by initiating the deployment of settings, firmware, and software.

Table 7 Apps (Continued)

Item	Description
	**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.

Viewing Recent Apps

Use the shortcut to view and access recently used apps.

1. Touch ■.

   Recently used apps display, with the most recent apps on the right.
2. Swipe your finger right to view all recently-used apps.
3. Swipe up on an app to force close the app and remove it from the list.
4. Touch an icon to open an app, or touch ● to return to the current screen.

DataWedge Demonstration

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

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

DataWedge Demonstration Icons

These icons display DataWedge information.

Table 8 DataWedge Demonstration Icons

Item	Icon	Description
Illumination		Imager illumination is on. Touch to turn illumination off.
Illumination		Imager illumination is off. Touch to turn illumination on.
Data Capture		The data capture function is through the internal imager.
Data Capture		An RS6000 Bluetooth imager is connected.
Data Capture		An RS6000 Bluetooth imager 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.

RxLogger Utility

RxLogger Utility is a data monitoring application for viewing logs in the device while RxLogger is running. Logs and RxLogger Utility features are accessed using Main Chat Head.

Initiating the Main Chat Head

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

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

Removing the Main Chat Head

1. Touch and drag the icon.

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

Viewing Logs

1. Touch the Main Chat Head icon.

   The RxLogger Utility screen 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

- To remove a Sub Chat Head icon, press and hold the icon until it disappears.

Backing Up In Overlay View

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

The Backup icon is always available in Overlay View.

1. Touch  .

   The Backup dialog box appears.

2. Touch **Yes** to create the backup.

Data Capture

This section provides information for capturing barcode data from using various devices.

The following scanners are supported on the device:

- Camera
- DS3678
- DS8178
- LI3678
- RS2100
- RS507
- RS507x
- RS5100
- RS6000
- RS6100
- SE4720 ZFLX scanner

NOTE: One one wired scanner can connect to the device at a time. The Z-Flex scanner is a wired scanner.

Scanning Considerations

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

However, consider the following to optimize scanning performance:

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

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

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

Scanning with the Camera

Use the internal camera to capture barcode data.

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

NOTE: The integrated camera is intended for light-duty barcode scanning. For heavy-duty scanning, 100 or more scans per day, use a compatible Zebra scanner such as the Z-Flex.

To scan with the internal camera:

1. Launch a scanning application.
2. Bring the barcode in front of the camera.
3. Move the barcode until it is visible on the screen. The scanning distance is 20-30 cm (7.87-11.81 in.) from the screen.
4. The captured data appears in the text field.

DataWedge

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

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

Configure DataWedge to:

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

To configure DataWedge, refer to techdocs.zebra.com/datawedge/.

Enabling DataWedge

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

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

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

Disabling DataWedge

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

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

Supported Decoders

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

DS3678 Supported Decoders

This section lists the supported decoders for the DS3678 scanner.

Table 9 DS3678-Supported Decoders

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

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

DS8178 Supported Decoders

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

Table 10 DS8178 Digital Scanner-Supported Decoders

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

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

LI3678 Supported Decoders

This section lists the supported decoders for the LI3678 scanner.

Table 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	—	GS1 DataBar	X	QR Code	—

Table 11 LI3678-Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Chinese 2 of 5	O	GS1 DataBar Expanded	X	Decoder Signature	—
Codabar	X	GS1 DataBar Limited	O	TLC 39	O
Code 11	O	GS1 Datamatrix	—	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	—	US4state FICS	—
Datamatrix	—	Matrix 2 of 5	O	US Planet	—
Dutch Postal	—	Maxicode	—	US Postnet	—
DotCode	O	MicroPDF	—		
EAN13	X	MicroQR	—		

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

RS2100/RS5000X Supported Decoders

This section lists the supported decoders for the RS2100 and RS5000X Wearable Scanner.

Table 12 RS2100 and RS5000X 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	X	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

Table 12 RS2100 and RS5000X Supported Decoders (Continued)

Decoder	Default State	Decoder	Default State	Decoder	Default State
Code 93	X	Interleaved 2 of 5	X	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	O	US Postnet	O
DotCode	O	MicroPDF	O		
EAN13	X	MicroQR	X		

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

RS507/RS507x Supported Decoders

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

Table 13 RS507/RS507x Supported Decoders

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

Table 13 RS507/RS507x Supported Decoders (Continued)

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

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

SE4720 Internal Imager Supported Decoders

This section lists the supported decoders for the SE4720 internal imager.

Table 14 SE4720 Internal Imager-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 15 RS5100-Supported Decoders

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

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

RS6000 Supported Decoders

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

Table 16 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

Table 16 RS6000-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

RS6100 Supported Decoders

Lists the supported decoders for the RS6100 Ring Scanner.

Table 17 RS6100 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

Table 17 RS6100 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		
EAN13	X	MicroQR	O		

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

Wireless

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

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

WLAN

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

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

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

The device supports the following WLAN security options:

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

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

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

Connecting to a Wi-Fi Network

Most of the device's functionality requires an internet connection. Connect to an available Wi-Fi network to use the device features.

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

   The device obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP). To configure the device with a fixed internet protocol (IP) address, see Configuring the Device to Use a Static IP Address.
6. In the Wi-Fi setting field, **Connected** appears, indicating that the device is connected to the WLAN.

Wi-Fi Version

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

Table 18 Wi-Fi Version Icons

Icon	Description
	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. Touch the name of the network.
5. Touch **FORGET**.

WLAN Configuration

This section provides information on configuring Wi-Fi settings.

Configuring a Secure Wi-Fi Network

Add a Wi-Fi network on the device to connect to the internet.

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

   The device searches for WLANs in the area and lists them on the screen.
5. Scroll through the list and select the desired WLAN network.
6. Touch the desired network. If network security is **Open**, the device automatically connects to the network. For all other network security, a dialog box appears.
7. If network security is **WPA/WPA2-Personal**, or **WEP**, enter the required password and then touch **Connect**.
8. If network security is **WPA/WPA2-Personal**, **WPA3-Personal**, or **WEP**, enter the required password and then touch **Connect**.

9. 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.

10. If the network security is **WPA3-Enterprise 192-bit**:

    - Touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the Security settings.
    - Touch **User certificate** and select a user certificate. Note: User certificates are installed using the Security settings.
    - In the **Identity** text box, enter the username credentials.

NOTE: By default, the network Proxy is set to **None** and the IP settings are set to **DHCP**. See Configuring for a Proxy Server for setting the connection to a proxy server and Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

11. 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** > **Internet**.
3. Slide the Wi-Fi switch to the **On** position.
4. Scroll to the bottom of the list and select **Add network**.
5. In the **Network name** text box, enter the name of the Wi-Fi network.

6. In the **Security** drop-down list, set the type of security to:
   - **None**
   - **Enhanced Open**
   - **WEP**
   - **WPA/WPA2-Personal**
   - **WPA3-Personal**
   - **WPA/WPA2/WPA3-Enterprise**
   - **WPA3-Enterprise 192-bit**
7. If the network security is **None** or **Enhanced Open**, touch **Save**.
8. If the network security is **None**, 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 the network security is **WEP** or **WPA/WPA2-Personal**, enter the required password and then touch **Save**.

NOTE: By default, the network Proxy server is set to **None** and the IP setting is set to DHCP. See Configuring for a Proxy Server for setting the connection to a proxy server, and Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

11. If network security is **WPA/WPA2/WPA3 Enterprise**:
    a) Touch the **EAP method** drop-down list and select one of the following:
       - **PEAP**
       - **TLS**
       - **TTLS**
       - **PWD**
       - **SIM**
       - **AKA**
       - **AKA'**
       - **LEAP**
    b) Fill in the appropriate information. Options vary depending on the **EAP method** chosen.
       - When selecting **CA certificate**, Certification Authority (CA) certificates are installed using the **Security** settings.
       - When using the EAP methods PEAP, TLS, or TTLS, specify a domain.
       - Touch **Advanced options** to display additional network options.
12. If the network security is WPA3-Enterprise 192-bit:
    - 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.

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

Configuring for a Proxy Server

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server and requests some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

It is important for enterprise customers to be able to set up secure computing environments within their companies, making proxy configuration essential. Proxy configuration acts as a security barrier ensuring that the proxy server monitors all traffic between the Internet and the intranet. This is normally an integral part of security enforcement in corporate firewalls within intranets.

1. Go to **Settings**.
2. Touch **Network & internet** > **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** > **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 **IP settings** and select **Static**.

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

Wi-Fi Preferences

Use the Wi-Fi preferences to configure advanced Wi-Fi settings. From the **Wi-Fi screen**, scroll down to the bottom of the screen, and touch **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, notify the user when an open network is available.
- **Additional settings** - Touch to view additional Wi-Fi settings.
- **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 **Additional Settings** to configure additional Wi-Fi settings. To view the additional Wi-Fi settings, scroll to the bottom of the **Wi-Fi screen** and touch **Network preferences** > **Additional Settings**.

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

- **Regulatory**
  - **Country Selection** - Displays the acquired country code if 802.11d is enabled, else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Set the frequency band to: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
  - **Available channels (2.4 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
  - **Available channels (5 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.
  - **Available channels (6 GHz)** - Touch to display the **Available channels** menu. Select specific channels and touch **OK**.

- **Logging**
  - **Advanced Logging** - Touch to enable advanced logging or change the log directory.
  - **Wireless Logs** - Use to capture Wi-Fi log files.
    - **Fusion Logger** - Touch to open the **Fusion Logger** application. This application maintains a history of high level WLAN events which helps to understand the status of connectivity.
    - **Fusion Status** - Touch to display live status of WLAN state. Also provides information about the device and connected profile.
- **Zebra RTT Location**
  - **Fusion Location Setting** - Logs more detailed location data. Touch to enable.
- **About**
  - **Version** - Displays the current version information. Touch the version to display addition version details.

Configuring Wi-Fi Direct

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

1. Go to **Settings**.
2. Touch **Network & internet**.
3. Touch **Internet**.
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). Bluetooth wireless technology is specifically designed for short-range (10 m (32.8 ft)) communication and low power consumption.

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

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

Adaptive Frequency Hopping

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

AFH for Bluetooth consists of four main sections:

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

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

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

The Bluetooth radio in this device operates as a Class 1 device power class. The maximum output power is 7.5 mW and the expected range is 30 m (98.4 ft). A definition of ranges based on power class is difficult to obtain due to power and device differences, and whether in open space or closed office space.

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

Security

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

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

Recommendations are:

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

Bluetooth Profiles

The device supports the Bluetooth services listed.

Table 19 Bluetooth Profiles

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

Table 19 Bluetooth Profiles (Continued)

Profile	Description
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** - 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.

NOTE: To achieve optimal battery life, turn off radios when not in use.

Enabling Bluetooth

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

Disabling Bluetooth

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

Using a Bluetooth Headset

Use a Bluetooth headset for audio communication when using an audio-enabled app. See Bluetooth for more information on connecting a Bluetooth headset to the device. Set the volume appropriately before putting on the headset. When a Bluetooth headset is connected, the speakerphone is muted.

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**.

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.

Connecting to a Bluetooth Device

Once paired, connect to a Bluetooth device.

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

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

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**.

Discovering Bluetooth Device(s)

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

1. Ensure that Bluetooth is enabled on both devices.
2. Ensure that the Bluetooth device to discover is in discoverable mode.
3. Ensure that the two devices are within 10 m (32.8 ft) of one another.
4. Swipe down from the Status bar to open the Quick Access panel.

5. Touch and hold **Bluetooth**.
6. Touch **Pair new device**. The device begins searching for discoverable Bluetooth devices in the area and displays them under **Available devices**.
7. Scroll through the list and select a device. The Bluetooth pairing request dialog box appears.
8. Touch **Pair** on both devices.
9. The Bluetooth device is added to the **Paired devices** list and a trusted ("paired") connection is established.

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 devices when they are within proximity of one another.

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.

NOTE: A Mobility DNA Enterprise License is required to pair and connect Zebra ring scanners.

The device supports the following operating modes:

- Reader mode
- Card Emulation mode.

Using NFC, the device can:

- Read contactless cards, such as contactless tickets, ID cards, and ePassport.
- Read and write information to contactless cards, such as SmartPosters and tickets, as well as devices with an NFC interface, such as vending machines.
- Read information from supported medical sensors.
- Pair with supported Bluetooth devices such as printers (for example, ZQ5x, ZD5x), ring scanners (for example, RS6000), and headsets (for example, HS3100).
- Exchange data with another NFC device.
- Emulate contactless cards such as a payment or ticket.
- Emulate contactless cards such as a payment, ticket, or SmartPoster.

The device's NFC antenna is positioned to read NFC cards placed in the center of the screen.

Advanced NFC Settings

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

- **Card Detection Mode** - Select a card detection mode.
  - **Low** - Increases battery life by lowering the NFC detection speed.
  - **Hybrid** - Provides a balance between NFC detection speed and battery life (default).
  - **Standard** - Provides the optimal NFC detection speed, but reduces battery life.
- **Supported Card Technology** - Select an option to detect only one NFC tag type, increasing battery life, but reducing detection speed.
  - **All (Default)** - Detects all NFC tag types.
  - **ISO 14443 Type A**
  - **ISO 14443 Type B**
  - **FeliCa**
  - **ISO 15693**
- **NFC Debug Logging** - Use to enable or disable debug logging for NFC.
- **Other NFC settings available with Zebra administrator tools (CSP)** - Allows configuration of additional Enterprise NFC Settings through staging tools and Mobile Device Management (MDM) solutions with an MX version that supports the Enterprise NFC Settings Configuration Service Provider (CSP). For more information on using the Enterprise NFC Settings CSP, refer to: techdocs.zebra.com.

Accessories

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

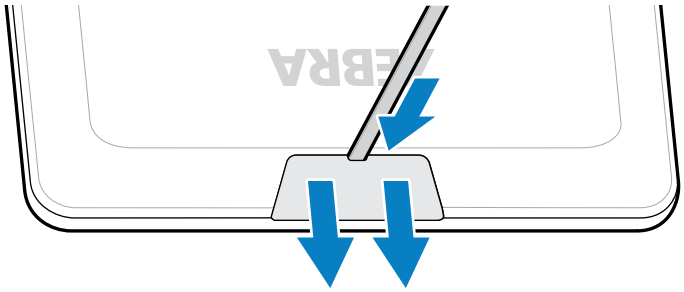
Accessories List

For a complete list of the accessories available for the device, go to zebra.com/kc50 and select the **Accessories** tab.

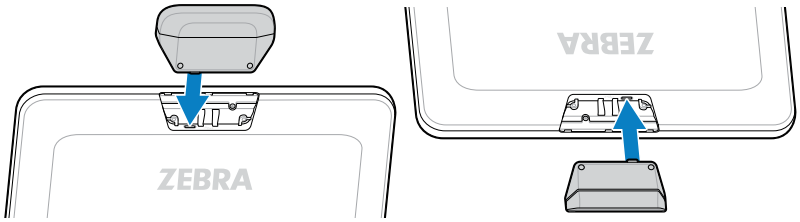
Connecting the Z-Flex Scanner and Light Bar

The optional Z-Flex scanner and light bar accessories enhance the device's usability applications. The scanner adds barcode scanning capability while the light bar provides quick visual feedback about the device based on app specifications.

1. Determine the desired position for the accessories. The modular design allows you to pick any one of the accessory ports to install the accessories.
2. Insert the MC18 removal tool in the accessory cover slot, and push the cover off of the device.



3. Align the connector with the port.



4. Press the accessory firmly until the connector is in place.

5. Secure the captive M2 screws with a Philips head screwdriver.

6. Repeat this process for all accessories.

Open a relevant app, such as DWDemo, to ensure that the accessories are powered and functioning. The Light bar behavior depends on the app and its settings.

Touch Display TD50

The TD50 is a monitor that accepts display data from a host device. It is an interactive device that accepts touch input from users.

TD50 Features

This section lists the features of the TD50.

Figure 5 TD50 Rear View with Back Cover Removed Features

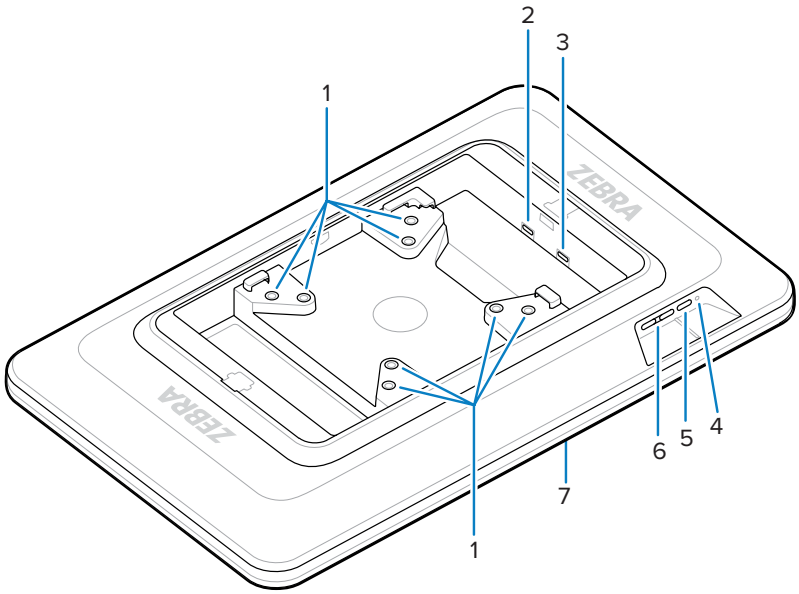


Table 21 Rear View Features

Number	Item	Description
1	VESA-compliant mounting inserts	M4 threaded inserts - 100 mm (3.94 in.) and 75 mm (2.95 in.) squares.

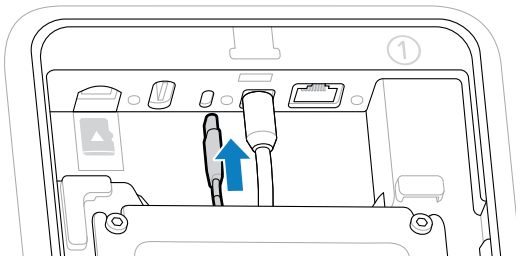
Table 21 Rear View Features (Continued)

Number	Item	Description
2	USB-C Port	Accepts power if the source device is insufficient to power the device. **NOTE:** The KC50 provides sufficient power through the DP port.
3	USB-C Display Port	Accepts power and display information.
4	Power LED	Displays device power status.
5	Power button	Turns display on and off.
6	Brightness control buttons	Increases and decreases screen brightness.
7	Touch screen	Displays input from the host device and accepts touch input.

Connecting the TD50

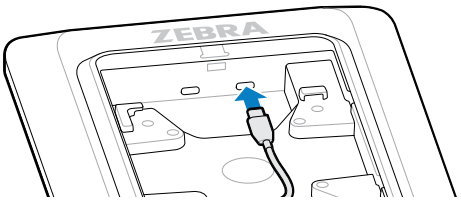
The TD50 connects to the KC50 for a dual display configuration.

1. Connect a USB-C cable to the USB-C port on the KC50.



2. Connect the other end of the USB-C cable to the port of the TD50. This port provides power and display input from the host device.

IMPORTANT: The TD50 screen will not turn on if the USB-C cable is connected to the wrong port. Ensure the cable is connected to the display port.



NOTE: Use proper cable management and tie-down practices in your installation to ensure the cables are not pulled out during final assembly and normal use.

Application Deployment

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

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

Android Security

The device implements a set of security policies that determine whether an application is allowed to run and, if allowed, with what level of trust. To develop an application, you must know the security configuration of the device, and how to sign an application with the appropriate certificate to allow the application to run (and to run with the needed level of trust).

NOTE: Ensure the date is set correctly before installing certificates or when accessing secure web sites.

Secure Certificates

If the VPN or Wi-Fi networks rely on secure certificates, obtain the certificates and store them in the device's secure credential storage before configuring access to the VPN or Wi-Fi networks.

If downloading the certificates from a web site, set a password for the credential storage. The device supports X.509 certificates saved in PKCS#12 key store files with a .p12 extension (if key store has a .pfx or other extension, change to .p12).

The device also installs any accompanying private key or certificate authority certificates contained in the key store.

Installing a Secure Certificate

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

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory.
2. Copy the certificate from the host computer to the root of the device's internal memory.
3. Touch **Security** > **Encryption & credentials**.
4. Touch **Install a 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**.
9. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.
10. Touch **OK**.

Configuring Credential Storage Settings

Configure credential storage from the device settings.

1. Go to **Settings**.
2. Touch **Security** > **More security settings** > **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 from storage** to install a secure certificate from the microSD card or 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. Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

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

Enabling Developer Options

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

1. Go to **Settings**.
2. Touch **About phone**.
3. Scroll down to **Build number**.
4. Tap **Build number** seven times.

   The message **You are now a developer!** appears.

5. Touch **Back**.
6. 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.

StageNow for Android

StageNow is Zebra's next-generation Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles and can deploy to devices simply by scanning a barcode 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 easily create staging profiles for configuring device components, and perform other staging actions such as checking the condition of a target device to determine suitability for software upgrades or other activities. The StageNow Workstation stores profiles and other created content for later use.
- The StageNow Client resides on the device and provides a user interface for the staging operator to initiate staging. The operator uses one or more of the desired staging methods (print and scan a barcode or read an NFC tag) to deliver staging material to the device.

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

GMS Restricted

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

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

For more information on StageNow, go to techdocs.zebra.com.

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 web site 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!** appears.
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 Rugged Charge/USB Cable.

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

   If the device and host computer are connected for the first time, the **Allow USB debugging?** dialog box with the **Always allow from this computer** check box displays. Select the check box, if required.
10. Touch **OK**.
11. Touch **OK** or **Allow**.
12. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
13. Type `adb devices`.

    The following displays:

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

    Where XXXXXXXXXXXXXXX is the device number.

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

14. Return to the Home screen.

Entering Android Recovery Manually

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

1. Press and hold the Power button until the menu appears.
2. Touch **Restart**.

3. Press and hold the volume up button until the device vibrates.

   The System Recovery screen appears.

Application Installation Methods

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

- USB drive
- USB connection
- 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 a USB Drive

Use a USB drive to install applications on the device.

IMPORTANT: USB Drive must have FAT32 format.

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

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

4. Eject the USB drive from the host computer.
5. Plug the USB drive into the USB port on the device.
6. Swipe the screen up and select to view files on the USB drive.
7. Touch **General USB drive**.
8. Locate the application APK file.
9. Touch the application file.
10. Touch **Continue** to install the app or **Cancel** to stop the installation.
11. To confirm installation and accept what the application affects, touch **Install** otherwise, touch **Cancel**.
12. Touch **Open** to open the application or **Done** to exit the installation process.

    The application appears in the App list.
13. Disconnect the USB drive from the host computer.

Installing Applications Using the USB Connection

Use the USB connection to install applications onto the 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. Connect the device to a host computer using the USB-C cable.
2. On the device, pull down the Notification panel and touch **Charging 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.

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

6. Disconnect the device from the host computer.
7. Swipe the screen up and select to view files on the microSD card or Internal Storage.
8. Locate the application APK file.
9. Touch the application file.
10. Touch **Continue** to install the app or **Cancel** to stop the installation.
11. To confirm installation and accept what the application affects, touch **Install**. Otherwise, touch **Cancel**.
12. Touch **Open** to open the application or **Done** to exit the installation process.

    The application appears in the App list.

Installing Applications Using the Android Debug Bridge

Use the USB connection to install applications onto the 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. 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.
9. Touch **OK** or **Allow**.

10. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
11. Type `adb install <application>`.

    where: <application> = the path and filename of the apk file.
12. Disconnect the device from the host computer.
13. Disconnect the USB-C cable from the device.

Installing Applications Using Wireless ADB

Use ADB commands to install an application onto the device.

Go to the Zebra Support & Downloads web site at zebra.com/support 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 on page 70.

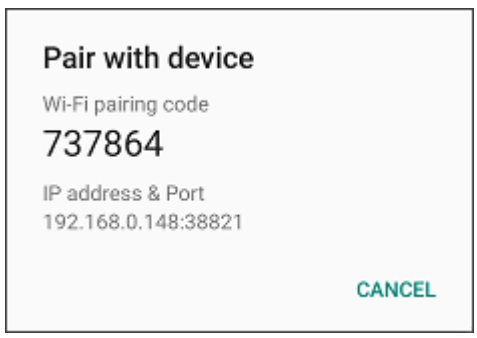
3. Slide the **USB debugging** switch to the **ON** position.
4. At the prompt, tap **OK**
5. Slide the **Wireless debugging** switch to the **ON** position.

   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
device
```

    Where XXXXXXXXXXXXXXX is the device number.

NOTE: If the device number does not appear, ensure that the 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`.

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.

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

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 Replacing the microSD Card 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. Connect the device to a host computer using USB.
3. Copy the application APK file from the host computer to the microSD card.
4. Remove the microSD card from the host computer.
5. Power off the device.
6. Insert the microSD card into the slot.
7. Power on the device.
8. Swipe the screen up and select to view files on the microSD card.
9. Touch **SD card**.
10. Locate the application APK file.
11. Touch the application file.
12. Touch **Continue** to install the app or **Cancel** to stop the installation.
13. To confirm installation and accept what the application affects, touch **Install**. Otherwise, touch **Cancel**.
14. Touch **Open** to open the application or **Done** to exit the installation process.

    The application appears in the App list.

Uninstalling an Application

Free up device memory by removing unused apps.

1. Go to **Settings**.
2. On Android 11, touch **Apps & notifications**.
3. On Android 13, touch **Apps**.
4. Touch **See all apps** to view all apps in the list.
5. Scroll through the list to the app.
6. Touch the app.

   The **App info** screen displays.
7. Touch **Uninstall**.
8. Touch **OK** to confirm.

Android System Update

System Update packages can contain either partial or complete updates for the operating system. Zebra distributes the System Update packages on the Zebra Support & Downloads website. Perform a system update using either a microSD card or using ADB.

Performing a System Update using microSD Card

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

Go to the Zebra Support & Downloads website at zebra.com/support 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. Go to Installing a microSD Card for more information.
   - 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 **Volume Up** and **Volume Down** to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
3. Press **Power**.
4. Press **Volume Up** and **Volume Down** to navigate to the System Update file.
5. Press **Power**.

   The System Update installs, and then the device returns to the Recovery screen.
6. Navigate to **Reboot system now** and press **Power** to reboot the device.

Performing a System Update Using ADB

Use ADB to perform a system update.

Go to the Zebra Support & Downloads web site at zebra.com/support 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 **USB debugging** switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Touch **OK**.
7. On the host computer, 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. Press **Volume Up** and **Volume Down** to navigate to **Apply upgrade from ADB**.
12. On the host computer command prompt window type `adb sideload <file>`.

    where: <file> = the path and filename of the zip file.
13. Press **Enter**.

    The System Update installs (progress appears as a percentage in the Command Prompt window) and then the System Recovery screen appears on the device.
14. Navigate to **Reboot system now** and press the Enter key or Power button to reboot the device.
15. Press **Power**.
16. Disconnect the USB cable from the device.

Performing a System Update using USB Drive

Update the operating system on the device using a USB drive.

NOTE: Use the rear USB-C connecter for system updates.

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

IMPORTANT: USB drive must have FAT32 format.

1. Install the USB drive into the host computer USB port.
2. Copy the System Update zip file to the root of a USB drive.
3. Properly eject the USB drive from host computer and remove the USB drive.
4. Remove the dust cover from the back of the device.
5. Insert the USB drive into the USB port.
6. Press and hold **Power** until the menu appears.
7. Touch **Restart**.
8. Press and hold **Volume Up** until the device vibrates.

   The System Recovery screen appears.

9. Press **Volume Up** and **Volume Down** to navigate to **apply upgrade from USB drive**.
10. Press **Power**
11. Use **Volume Up** and **Volume Down** to navigate to the System Update zip file.
12. Press **Power**.

    The System Update installs and then the device returns to the Recovery screen.
13. Press **Power** to reboot the device.

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 (emulated storage), while preserving the contents of the /enterprise folder and its subfolders. 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 a microSD Card

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

Go to the Zebra Support & Downloads website at zebra.com/support 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. Go to Installing a microSD Card for more information.
   - 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 **Volume Up** and **Volume Down** to navigate to **Apply upgrade from SD card**.
3. Press **Power**.

4. Press **Volume Up** and **Volume Down** to navigate to the Enterprise Reset file.
5. Press **Power**.

   The Enterprise Reset occurs and then the device returns to the Recovery screen.
6. Press **Power** 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 **USB debugging** switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Touch **OK**.
7. On the host computer, 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. Press **Volume Up** and **Volume Down** to navigate to **Apply upgrade from ADB**.
12. Press **Power**.
13. On the host computer command prompt window type `adb sideload <file>`

    where: <file> = the path and filename of the zip file.
14. Press **Enter**.

    The Enterprise Reset package installs and then the System Recovery screen appears on the device.
15. Navigate to **Reboot system now** and press the Enter key or Power button to reboot the device.
16. Press **Power** to reboot the device.
17. Disconnect the USB cable from the device.

Performing an Enterprise Reset using a USB Drive

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 USB drive.
   - Copy the zip file to a USB drive using a host computer and then install the USB drive into the device.
   - Connect the device with a USB drive already installed to the host computer and copy zip file to the USB drive. Disconnect the device from the host computer.
2. Press and hold **Power** until the menu appears.
3. Touch **Restart**.
4. Press and hold **Power** until the Zebra boot screen appears.

   The Android Recovery screen appears.
5. Press **Volume Up** and **Volume Down** to navigate to **apply update from USB drive**.
6. Press **Power**.
7. Press **Volume Up** and **Volume Down** to navigate to the Enterprise Reset file.
8. Press **Power**.

   The Enterprise Reset occurs and then the device returns to the Recovery screen.
9. Press **Power**.

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. Go to Installing a microSD Card 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 **Volume Up** and **Volume Down** to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
3. Press **Power**.
4. Press **Volume Up** and **Volume Down** to navigate to the Factory Reset file.

5. Press **Power**.

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

6. Navigate to **Reboot system now** and press the Enter key or Power button to reboot the device.

Performing a Factory Reset using ADB

Perform a factory reset using ADB.

Go to the Zebra Support & Downloads web site 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-C cable.
2. Go to **Settings**.
3. Touch **System** > **Developer options**.
4. Slide the **USB debugging** switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Touch **OK**.
7. On the host computer, 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. Press **Volume Up** and **Volume Down** to navigate to **Apply upgrade from ADB** or **Apply downgrade from ADB**.
12. Press **Power**.
13. On the host computer command prompt window type`adb sideload <file>`.

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

14. Press **Power**.

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

15. Press **Power** to reboot the device.
16. Disconnect the USB-C cable from the device.

Performing a Factory Reset using a USB Drive

Go to the Zebra Support & Downloads web site 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 USB drive.
   - Copy the zip file to a USB drive using a host computer and then installing the USB drive into the device.
   - Connect the device with a USB drive already installed to the host computer and copy the zip file to the USB drive. Disconnect the device from the host computer.
2. Press and hold **Power** until the menu appears.
3. Touch **Restart**.

   The device resets.
4. Press and hold **Volume Up** while the device restarts.

   The System Recovery screen appears.
5. Press **Volume Up** and **Volume Down** to navigate to **apply update from USB drive**.
6. Press **Power**.
7. Press **Volume Up** and **Volume Down** to navigate to the Android Reset file.
8. Press **Power**.

   The Factory Reset occurs and then the device returns to the Recovery screen.
9. Press **Power**.

Android Storage

The device contains multiple types of file storage.

- Random Access Memory (RAM)
- On-device Storage
- Internal storage
- External storage (microSD card)
- Enterprise folder.

Random Access Memory

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

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

The screen displays the amount of used and free RAM.

- **Performance** - Indicates memory performance.
- **Total memory** - Indicates the total amount of RAM available.

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

Viewing Memory

View the amount of memory used and free RAM.

1. Go to **Settings**.
2. Touch **System** > **Developer options**.
3. Touch **Memory**.

Internal Storage

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

Viewing Internal Storage

View available and used internal storage on the device.

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

   It displays the total amount of space on internal storage and amount used.

   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 or USB drive. The contents of the removable storage device can be viewed and 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 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.

NOTE: The suggested maximum SD card size is 128 GB when using internal storage.

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

Enterprise Folder

The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset.

The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 MB (formatted). Applications can persist data after an Enterprise Reset by saving data to the enterprise/user folder. The folder is ext4 formatted and is only accessible from a host computer using ADB or from an MDM.

Managing Apps

Apps use two kinds of memory: storage memory and RAM. Apps use storage memory for themselves and any files, settings, and other data they use. They also use RAM when they are running.

1. Go to **Settings**.
2. Touch **Apps & notifications**.
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.
- **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 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 and accessories.

Device Maintenance

Follow these guidelines for maintaining the device to maximize its lifespan and reduce wear and tear.

- 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's screen.
- The touch-sensitive screen of the device is glass. Ensure the device does not fall or sustain a strong impact.
- Protect the device from temperature extremes.
- Do not store the device in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the device. If the surface of the device screen becomes soiled, clean it with a soft cloth moistened with an approved cleanser.

Cleaning Instructions

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 Cleaning and Disinfectant Agents

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

- Mild dish soap

IMPORTANT:

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. Because of the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidation (corrosion) when exposed to this chemical in liquid form (including wipes).

If 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.

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.

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.

Cleaning Frequency

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

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

Cleaning the Device

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. Before use, allow the unit to air dry.

For a thorough cleaning, first remove all accessory attachments, such as the Light bar and ZFLX scanner, from the device and clean them separately.

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.

Housing

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

Troubleshooting

This section provides information for resetting and troubleshooting the device and accessories.

Resetting the Device

There are two reset functions: soft reset and hard reset.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

1. Press and hold Power until the menu appears.
2. Touch **Restart**.

   The device reboots.

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.

Troubleshooting the Device

The following table includes basic troubleshooting information.

Table 22 Troubleshooting the Device

Problem	Cause	Solution
Accessories are not working.	Insufficient power supplied over PoE	Use a higher-class PoE injector.
	Accessories are improperly seated.	Remove and reinsert accessories into the USB-C port, then reset the KC50.
No power to a USB port when using PoE	PSE power class is too low.	Go to zebra.com/techdocs-kc50 to see how to create customized power managmeent restriction.

Table 22 Troubleshooting the Device (Continued)

Problem	Cause	Solution
The KC50 turns off unexpectedly.	The network switch has demoted the KC50 to sufficient power to the upstream device.	Reconfigure the system to ensure that the device is upstream of other devices.
The KC50 turns off unexpectedly; the power LED is flashing red.	The PSE is not providing sufficient power to the KC50.	Verify cabling from the PSE to the KC50 has been field tested by a qualified cable technician to the ANSAI/TIA 568.2-D standard.
Barcodes are not decoded when scanned.	A scanning application is not loaded.	Load a scanning application on the KC50, or enable DataWedge. See the system administrator.
	Unreadable barcode.	Ensure the symbol is not defaced.
	The distance between the exit window and the barcode is incorrect.	Place the barcode within the correct scanning range.
	The KC50 is not programmed to generate a beep.	If the scanner does not beep on a good decode, set the application to generate a beep on a good decode.
	The KC50 is not programmed for the barcode.	Program the KC50 to accept the type of barcode being scanned. Refer to the EMDK or DataWedge applicaton.
The display is off.	The KC50 is not powered.	Ensure the KC50 is plugged into a power source.
		Press the power button.
Data communication with host computer fails to transfer data, or data transfer is incomplete.	Communication software was incorrectly installed or configured.	Perform setup.
During data communication over Wi-Fi, no data was transmitted, or transmitted data was incomplete.	The Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	The devices are too far away from one another.	Move the Bluetooth device within 10 m (32.8 ft.) of the KC50.
A message appears stating the the KC50 memory is full.	Too many files are stored on the device.	Delete unused files. If necessary, transfer them to a different device or use a microSD card for additional memory.
	Too many applications are installed on the KC50.	Remove user-installed applications. Select **Storage** > **FREE UP SPACE** > **REVIEW RECENT ITEMS**. Select the unused program(s) and tap **FREE UP**.

Table 22 Troubleshooting the Device (Continued)

Problem	Cause	Solution
The KC50 cannot find any Bluetooth devices nearby.	Too far away from other Bluetooth devices.	Move the Bluetooth device within a range of 10 m (32.8 ft.) of the device.
	The Bluetooth device(s) nearby are turned off.	Turn on the Bluetooth device(s).
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to their user documentation for help.

Technical Specifications

For device technical specifications, go to zebra.com/kc50 and select **Full Specifications**.

SE4720 Decode Distances

The following table provides the decode distances for the SE4720 scan engine.

Table 23 SE4720 Decode Distances

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
4 mil Code 39	8.4 cm (3.3 in.)	22.4 cm (8.8 in.)
5.0 mil Code 128	7.1 cm (2.8 in.)	20.8 cm (8.2 in.)
5 mil Code 39	5.08 cm (2.0 in.)	34.3 cm (13.5 in.)
5 mil PDF417	7.9 cm (3.1 in.)	21.3 cm (8.4 in.)
10 mil Data Matrix	7.4 cm (2.9 in.)	25.7 cm (10.1 in.)
100% UPCA	4.6 cm* (1.8 in.)	66.0 cm (26.0 in.)
20 mil Code 39	5.08 cm* (2.0 in.)	76.2 cm (30.0 in.)
20 mil QR Code	8.1 cm (3.2 in.)	40.1 cm (15.8 in.)
*Limited by width of bar code in field of view. Notes: Photographic quality bar code at 15° tilt pitch angle under 30 fcd ambient illumination. Distances measured from front edge of scan engine chassis.		

Z-Flex Scanner Specifications

The following table lists the Z-Flex scanner's technical specifications.

Table 24 Z-Flex Technical Specifications

Item	Description
Dimensions	Height: 85 mm (3.35 in.) Width: 43.8 mm (1.72 in.) Width with USB-C: 48.6 mm (1.91 in.) Depth: 21.2 mm (0.83 in.) Depth with screws: 22.7 mm (0.89 in.)
Weight	51 g (1.8 lbs)
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 V air +/- 8 V contact

Light Bar Specifications

The following table lists the light bar's technical specifications

Table 25 Light Bar Technical Specifications

Item	Description
Dimensions	Height: 100 mm (3.94 in.) Width: 55.86 mm (2.2 in.) Width with USB-C: 60.1 mm (2.4 in.) Depth: 20.8 mm (0.82 in.) Depth with USB: (0.89 in.)
Weight	52 g (1.8 oz)
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 V air +/- 8 V contact

TD50 Specifications

The following table lists the TD50 specifications.

Table 26 TD50 Technical Specifications

Item	Description
Dimensions	Height: 38.3 mm(1.51 in.) Width: 239.4 mm (9.43 in.) Length: 385.2 mm (15.17 in.)
Weight	2.4 kg (5.3 lbs)
Input Voltage	5 VDC
Power Consumption	up to 10 W
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	5% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 V air discharge +/- 8 V contact discharge