ZEC500

Enterprise Computer

Product Reference Guide

ZEBRA

MN-005321-01EN Rev. B

Copyright

2025/09/30

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

About This Guide

This guide provides information about setting up and using the ZEC500 enterprise computer.

Configurations

Table 1 Value Configurations

Configuration	Description	Memory/Storage	Power Input Support
ZEC500V-NS10A11-NA	Value ZEC500 (No Fan)	6GB/64GB	DC Power Supply
ZEC500V-NE10A11-NA	Value ZEC500 (With Fan)	6GB/64GB	DC Power Supply
ZEC500V-NS10A11-A6	Value ZEC500 (No Fan)	6GB/64GB	DC Power Supply
ZEC500V-NE10A11-A6	Value ZEC500 (With Fan)	6GB/64GB	DC Power Supply

Table 2 Premium Configuration

Configuration	Description	Memory/Storage	Power Input Support
ZEC500P-YS10B22-NA	Premium ZEC500 (No Fan)	8GB/128GB	DC Power Supply, Power over Ethernet, USB-C Power Delivery Input
ZEC500P-YE10B22-NA	Premium ZEC500 (With Fan)	8GB/128GB	DC Power Supply, Power over Ethernet, USB-C Power Delivery Input
ZEC500P-YS10B22-A6	Premium ZEC500 (No Fan)	8GB/128GB	DC Power Supply, Power over Ethernet, USB-C Power Delivery Input
ZEC500P-YE10B22-A6	Premium ZEC500 (With Fan)	8GB/128GB	DC Power Supply, Power over Ethernet, USB-C Power Delivery Input

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 the Software Versions

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

1. Drag[1] down from the Status bar to open the Quick Access panel, and then select ⚙.
2. Select **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

[1] When using the ZEC500, "drag" refers to the action of clicking and dragging with a mouse on a standard monitor or touching and dragging with your finger on a touchscreen monitor, whether to move objects or swipe through screens.

Determining the Serial Number

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

1. Drag up on the screen to the app list and then select  .
2. Select **About phone**.
3. Select **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

This topic provides instructions to safely unpack your device.

1. Carefully remove the device from the box.
2. Verify the following items are in the box:
   - ZEC500
   - DC Cable Lock
   - ZEC500 Regulatory Guide
3. Inspect the equipment for any damage. If any equipment is missing or damaged, contact Zebra Support immediately.

Features

The following sections describe the features of the ZEC500-V and ZEC500-P.

ZEC500-V Features

This section describes the features for the ZEC500-V.

Figure 1 Front View Features

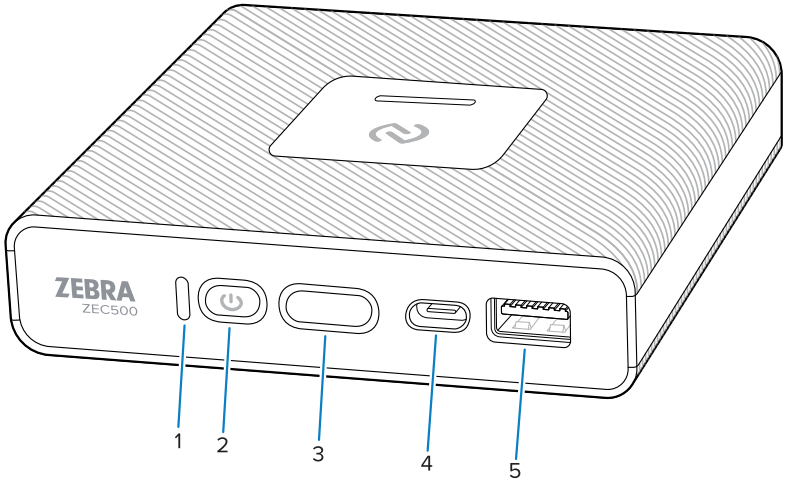


Table 3 Front View Features

Number	Item	Description
1	Power Status LED	Indicates power status. Go to LED Status Light on page 83.
2	Power Button	A button used to power on/off the device.
3	Programmable Button	A programmable button that will return to the home screen by default.
4	USB-C 3.2 Port	Supports USB-C peripherals. Supports DisplayPort output up to 3840 x 2160 @ 60fps. Used for ADB.
5	USB-A 3.2 Port	Supports USB-A peripherals.

Figure 2 Rear View

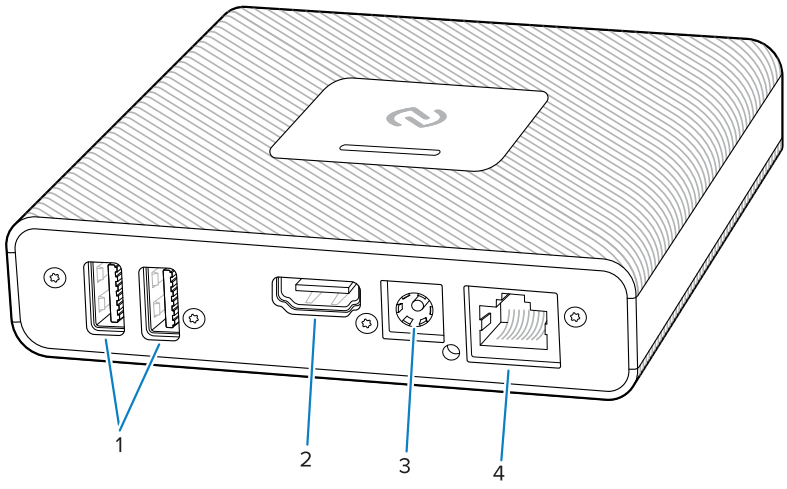


Table 4 Rear View Features

Number	Item	Description
1	USB-A 3.2 Ports	Supports USB-A peripherals.
2	HDMI	Supports HDMI output to external display. Maximum display resolution: 3840 x 2160 @ 30 fps.
3	DC Input	Input for a supported power supply.
4	RJ45 Ethernet Port	Supports speeds up to 1000 Mbps.

Figure 3 Bottom View

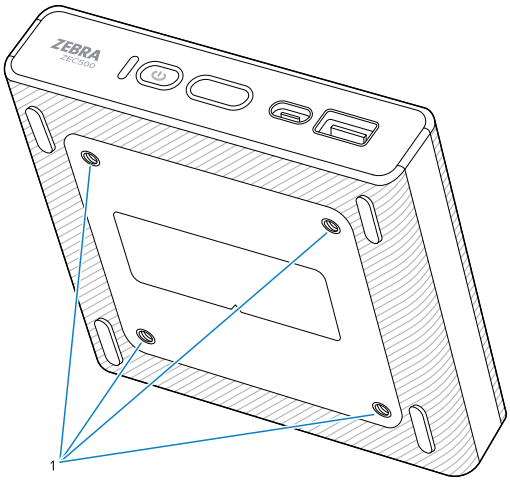


Table 5 Bottom View Features

Number	Item	Description
1	VESA	75x75mm VESA mounting holes.

NOTE: When mounting the device, use four M4 screws with a minimum length of 6mm (0.24 in.).

Figure 4 Top View

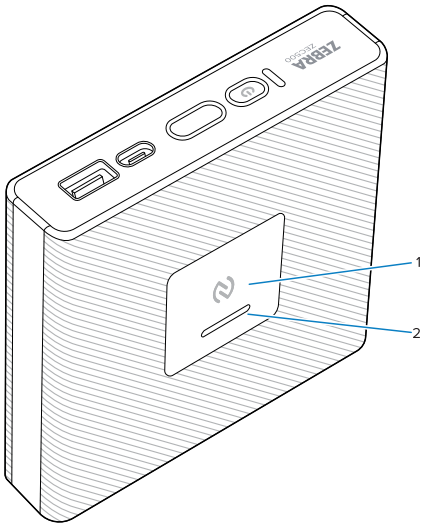


Table 6 Top View Features

Number	Item	Description
1	NFC Antenna	Provides communication with other NFC-enabled devices or NFC-enabled cards.
2	Wireless Workstation Connect Status LED	Go to LED Status Light on page 83.

ZEC500-P Features

This section describes the features for the ZEC500-P.

Figure 5 Front View Features

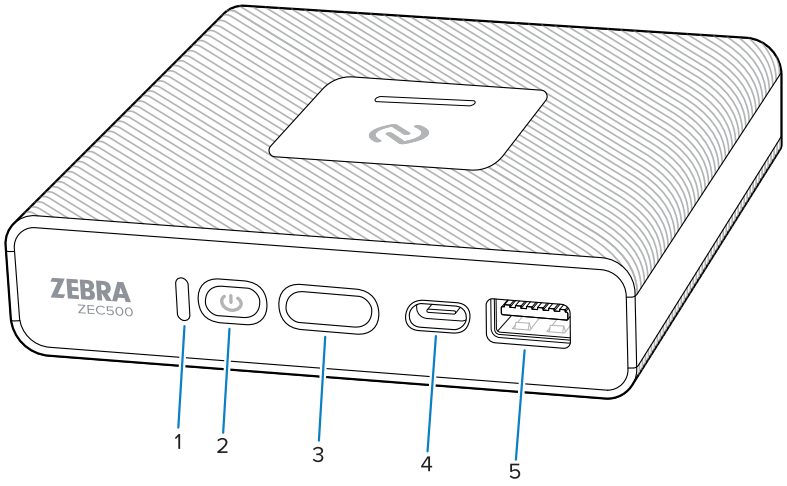


Table 7 Front View Features

Number	Item	Description
1	Power Status LED	Indicates power status. Go to LED Status Light on page 83.
2	Power Button	A button used to power on/off the device.
3	Programmable Button	A programmable button that will return to the home screen by default.
4	USB-C 3.2 Port	Supports USB-C peripherals. Supports DisplayPort output up to 3840 x 2160 @ 60fps. Capable of powering the device. Used for ADB.
5	USB-A 3.2 Port	Supports USB-A peripherals.

Figure 6 Rear View

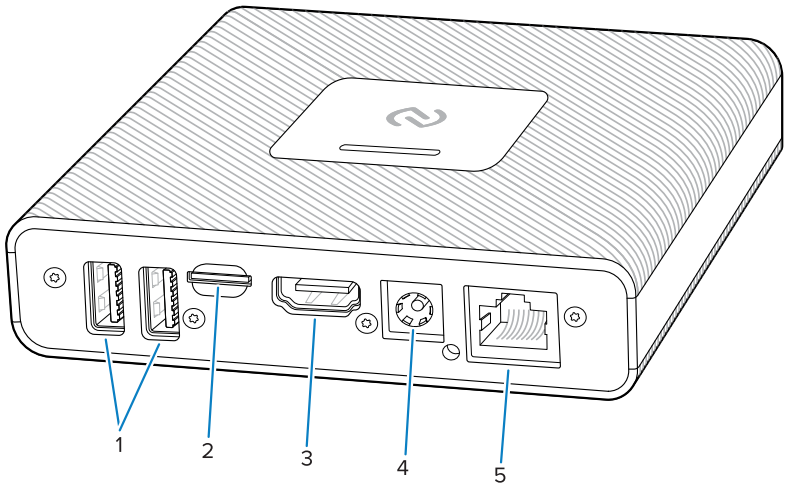


Table 8 Rear View Features

Number	Item	Description
1	USB-A 3.2 Ports	Supports USB-A peripherals.
2	MicroSD Slot	Input for microSD cards.
3	HDMI	Supports HDMI output to external display. Maximum display resolution: 3840 x 2160 @ 30 fps.
4	DC Input	Input for a supported power supply.
5	RJ45 Ethernet Port	Supports speeds up to 1000 Mbps. Capable of powering the device with compatible Power over Ethernet (PoE) injector.

Figure 7 Bottom View

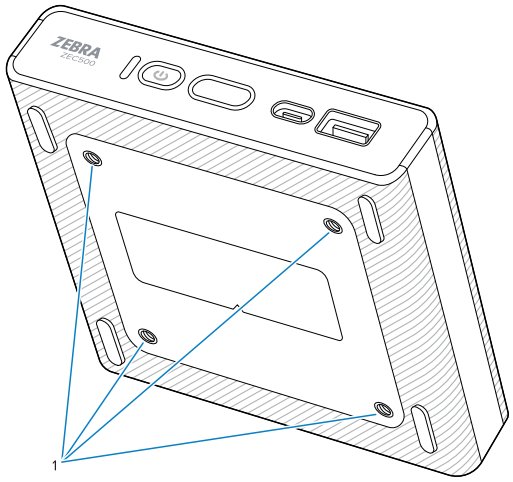


Table 9 Bottom View Features

Number	Item	Description
1	VESA	75x75mm VESA mounting holes.

NOTE: When mounting the device, use four M4 screws with a minimum length of 6mm (0.24 in.).

Figure 8 Top View

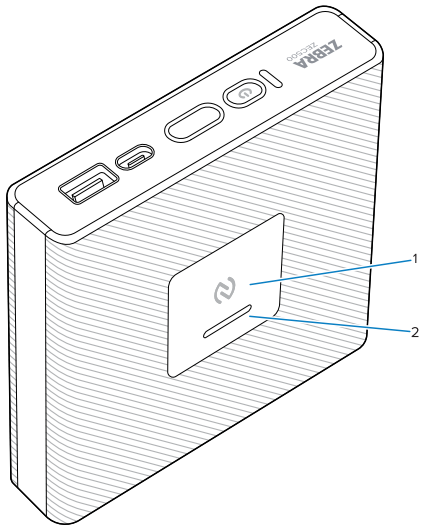


Table 10 Top View Features

Number	Item	Description
1	NFC Antenna	Provides communication with other NFC-enabled devices or NFC-enabled cards.
2	Wireless Workstation Connect Status LED	Go to LED Status Light on page 83.

Setting Up The Device

This section explains how to set up your device for a smooth and quick start.

1. (Optional) Mount the device.
2. Connect the desired peripherals: Display, mouse, keyboard, and so on.
3. Connect the device to a power supply.
4. Follow the Android Setup wizard to configure your device.

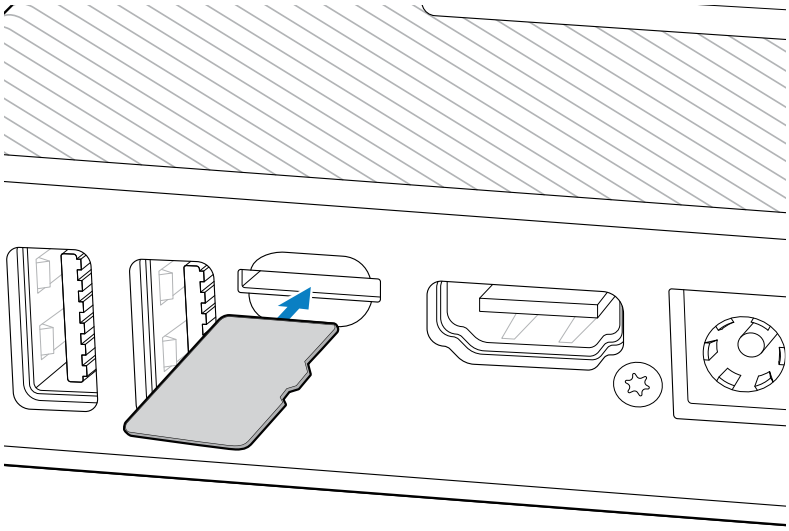
Installing a MicroSD Card

This section describes how to install a microSD card into the device.

NOTE: This applies only to the ZEC500-P.

CAUTION: If the device is powered on, be sure to safely eject the MicroSD card and turn off the device before removing.

1. Orient the microSD card with the pins face down.



2. Push the microSD card into the slot until it clicks into place.

Powering the Device

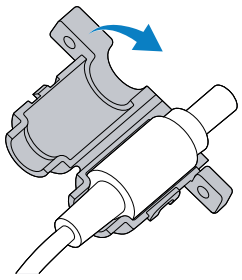
The following sections explain methods for powering the ZEC500-V and ZEC500-P.

NOTE: Ensure the power sourcing equipment is rated appropriately for the operating environment of the device.

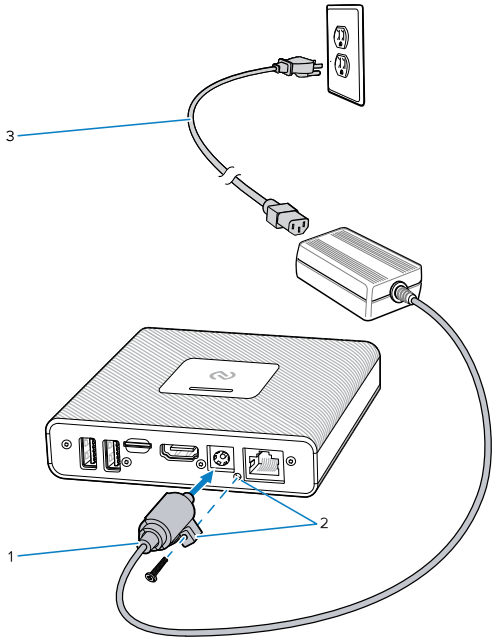
Powering the Device with a DC Power Supply

This section explains how to power the device using a DC power supply.

To properly secure the cable to the device, it is recommended that you put the cable lock on prior to powering the device.



- Connect the DC cable to the DC input (1), using a screwdriver, securely fasten the screw through the DC cable lock into the device (2), and then connect the power supply to AC power (3).



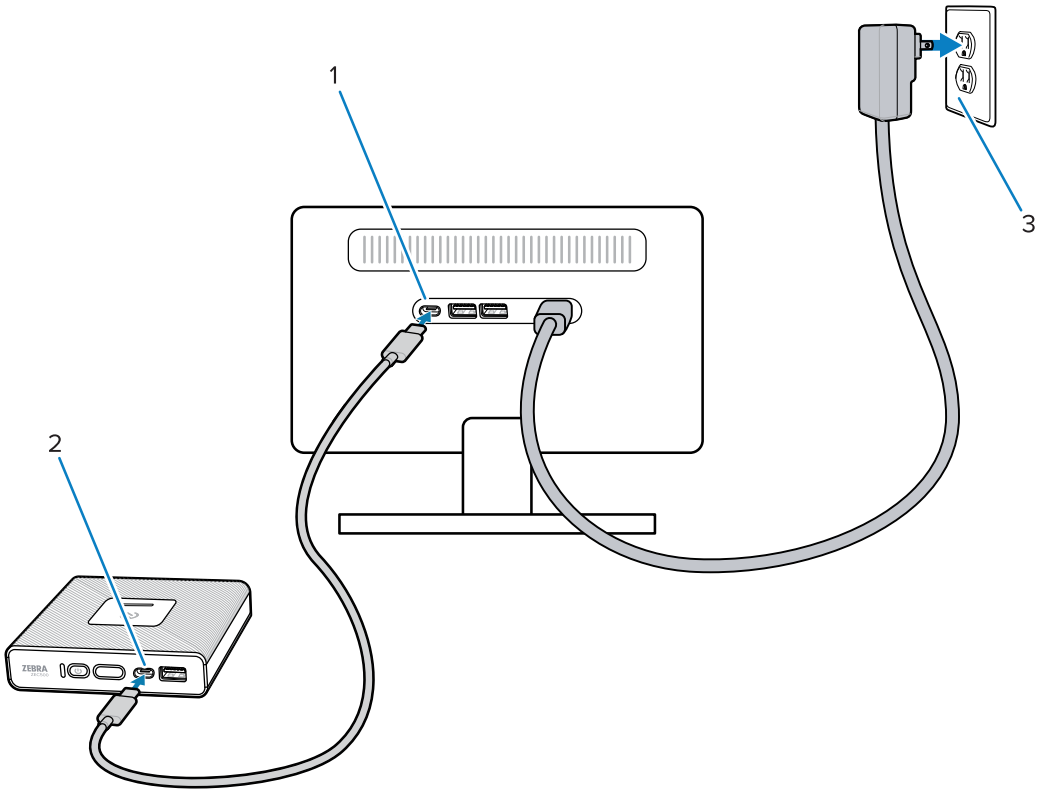
Powering the Device with a USB-C Connection

This section describes how to power the device by connecting it to a Power Delivery-capable display.

NOTE: This applies only to the ZEC500-P.

To use a USB-C cable to connect your external monitor to the device, make sure your monitor can provide USB Power Delivery (PD) of at least 60W or greater; lower values may be supported with possible limitations.

- Connect the USB-C cable to a USB Power Delivery-capable display (1), connect the USB-C cable to the device's USB-C port (2), connect the USB Power Delivery-capable display to a power source (3), and then power the device on.



The device is now powered by the display, and the display is now displaying the device's contents.

Powering the Device with Power over Ethernet (PoE)

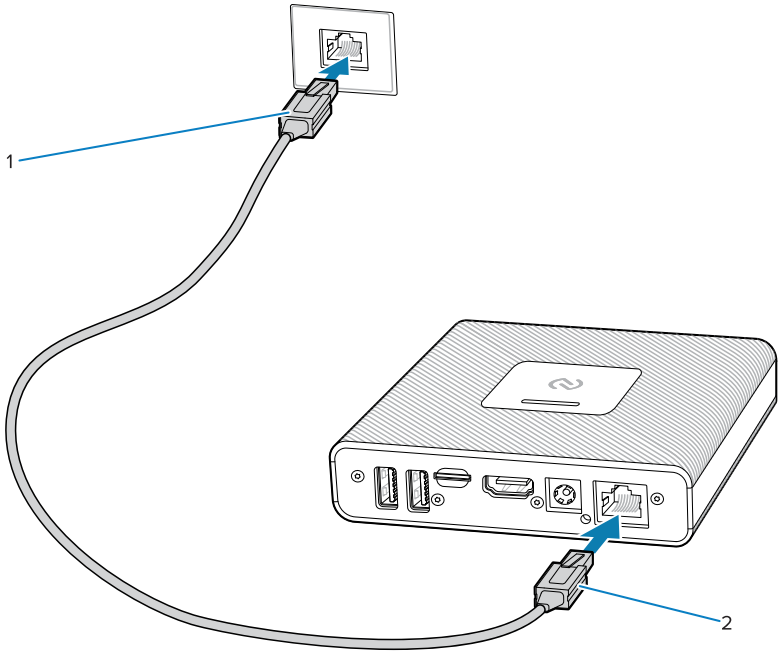
This section explains how to power the device using Power over Ethernet.

NOTE: This applies only to the ZEC500-P.

IMPORTANT: The PoE accessory must be compliant with 802.3at/bt standards and classified as Class 4 or higher Power Sourcing Equipment (PSE).

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 (PoE) section for more information.

- Connect the Ethernet cable to the PoE accessory (1), and connect the Ethernet cable to the device's Ethernet port (2).



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

Powering Off the Device

This section describes how to power off the device.

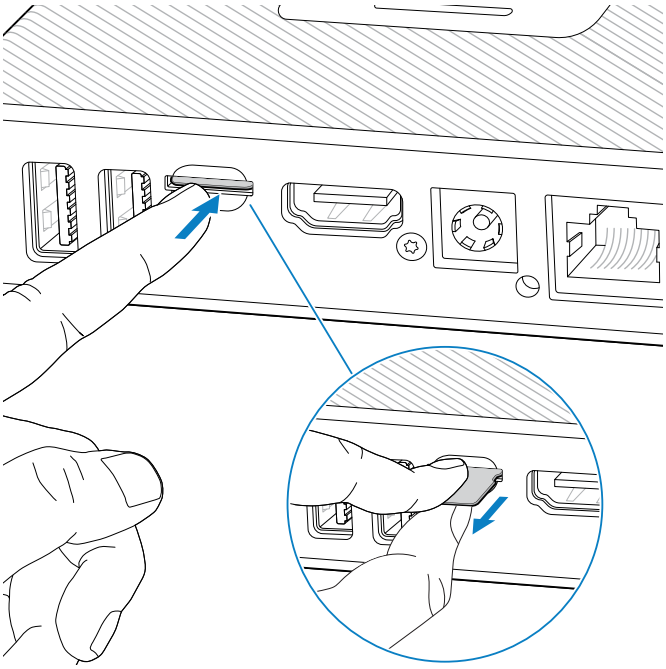
1. Press and hold the power button until the menu displays.
2. Select **Power off**.

Replacing the MicroSD Card

This section describes how to replace the microSD card.

1. Power off the device.

2. Press the microSD card, and then pull the microSD card out.



3. Install the replacement microSD card.

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** menu).

1. Press the power button.

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

2. Drag the screen up to unlock.

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

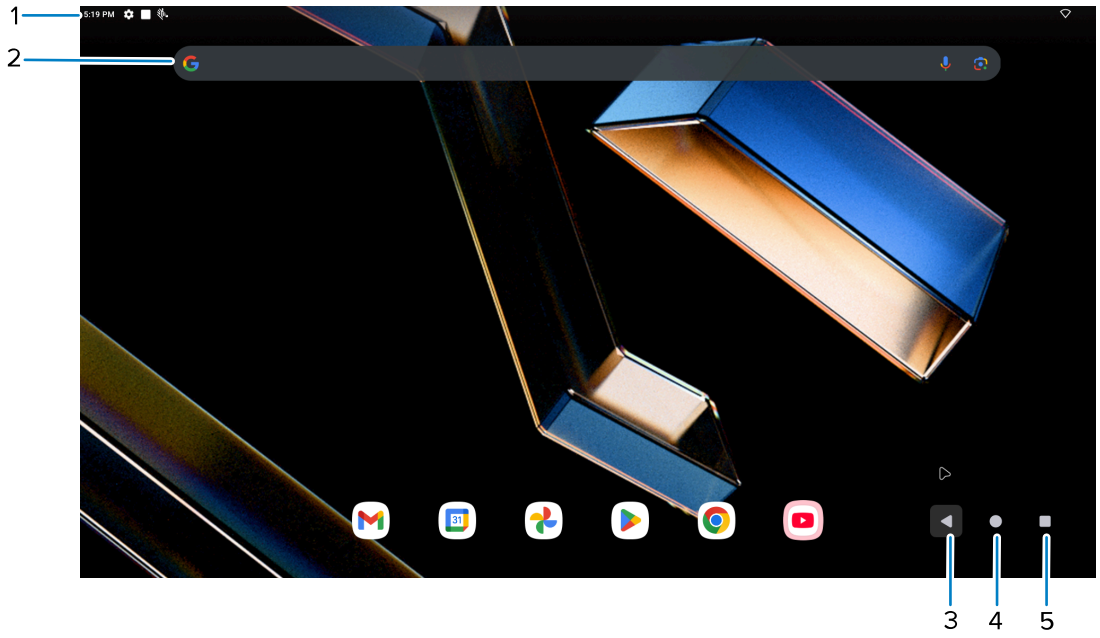
NOTE: If you enter the PIN, password, or pattern incorrectly five times, you must wait 30 seconds before trying again. If you forget the PIN, password, or pattern, contact your system administrator.

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. Press the power button and, with the mouse, drag the screen up to wake up the device. The Home screen provides four additional screens to place widgets and shortcuts. Select and hold an icon, and move it for the option to place the icon on one of the other screens. Drag the Home screen left or right to view the additional screens.

Figure 9 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.

Status Bar

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

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

Figure 10 Notifications and Status Icons

1	Notification icons
2	Status icons

Notification Icons

Notification icons indicate app events and messages.

Table 11 Notification Icons

Icon	Description
	More notifications are available for viewing.
	Data is synching.
	Indicates an upcoming event.
	An Open Wi-Fi network is available. The device is not connected to it.
	Audio is playing.
	A problem with sign-in or sync has occurred.
	The device is uploading data.
	Animated: the device is downloading data. Static: the download is complete.
	The device is connected to or disconnected from a virtual private network (VPN).
	Preparing internal storage by checking it for errors.
	USB debugging is enabled on the device.
	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.

Table 11 Notification Icons (Continued)

Icon	Description
	A device is connected via USB cable.

Status Icons

Status icons display system information for the device.

Table 12 Status Icons

Icon	Description
	Alarm is active.
	All sounds except media and alarms are muted.
	Do Not Disturb mode active.
	Airplane Mode is active. All radios are turned off.
	Bluetooth is on.
	Connected to a Bluetooth device.
	Connected to a Wi-Fi network. Indicates the Wi-Fi version number.
	Not connected to a Wi-Fi network or no Wi-Fi signal.
	Connected to an Ethernet network.
	Indicates that a 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 select a notification. The Notification panel closes, and the corresponding app opens.
- To manage recent or frequently used notifications, open the Notification panel and then select **Manage** > **App notifications**.
  - Select the toggle switch next to an app to turn off all notifications, or select an app for more notification options.
- To clear all notifications, open the Notification panel and then select **Clear all**. All event-based notifications are removed. Ongoing notifications remain in the list.
- To close the Notification panel, drag 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 drag down once.
- If the device is unlocked, drag down once.
- If the Notification panel is open, drag down from the Quick Settings bar.

Quick Access Panel Icons

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

Table 13 Quick Access Panel Icons

Icon	Description
	Internet - Turn Wi-Fi on or off. To open Wi-Fi settings, select the Wi-Fi network name.
	Bluetooth - Turn Bluetooth on or off. To open Bluetooth settings, select Bluetooth.
	Do Not Disturb - Control how and when to receive notifications.
	Alarm - Opens the Alarm app.
	Airplane mode - Turn Airplane mode on or off. When Airplane mode is on, the device does not connect to Wi-Fi or Bluetooth.
	Quick Share - Send files to nearby devices when they have the Quick Share feature enabled and their screens on.
	Screen Cast - Share device content on Chromecast or a television with Chromecast built-in. On the Cast screen, check the **Enable Wireless Display** option, and then select **Cast Screen** to display a list of devices. Select a device in the list to begin casting.

Table 13 Quick Access Panel Icons (Continued)

Icon	Description
	**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.
	**Device Controls** - Manages smart home devices from the device's power menu or quick settings.
	**Wallet** - Opens Android wallet.

Editing the Quick Access Tiles

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

1. Open the Quick Access panel.
2. Drag down on the notifications bar to minimize it.
3. Select ✎ to edit, add, or remove settings tiles.

USB Communication

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

NOTE: To ensure the device performs as expected, power on the device first before connecting a USB cable from the host computer.

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

Transferring Files

Use the Transfer files option to copy files between the device and 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, select **File Transfer**.
   - To transfer photos, select **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 Computer

This section describes how to disconnect a USB device from the host computer.

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

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

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

Power over Ethernet (PoE)

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 the 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 Powering the Device with Power over Ethernet (PoE).

- Select a power class that will power your required ports and peripherals.
- Each power class profile defines default restrictions on USB ports and peripherals. Go to techdocs.zebra.com/wwc/usage 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 ZEC500	Incompatible with ZEC500
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.

- Drag down from the top of the Home screen to open the Quick Access panel and select ⚙.
- Drag up from the bottom of the Home screen to view all apps and select **Settings**.

Display Settings

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

Setting Screen Timeout

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

1. Go to **Settings**.
2. Select **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)

Setting Font Size

Set the size of the font in systems apps.

1. Go to **Settings**.
2. Select **Display** > **Display size and text**.
3. Select 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. Select **Display** > **Display size and text**.
3. Select 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 WLAN does not support Network Time Protocol (NTP) or when not connected to a wireless network.

1. Go to **Settings**.
2. Select **System** > **Date & time**.
3. Toggle **Set time automatically** off to manually set the date and time.
4. Select **Date** to select the date in the calendar.
5. Select **OK**.
6. Select **Time**.
   a) Select the circle, drag to the current hour, and then release.
   b) Select the circle, drag to the current minute, and then release.
   c) Select **AM** or **PM**.
7. Select **OK**.
8. Select **Time zone** to select the current time zone from the list.
9. Select **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 options for the device.

NOTE: The device does not have an internal microphone or speaker. Sound options apply only when combined with an external speaker.

1. Go to **Settings**.
2. Select **Sound**.

3. Use the sliders to control the media, call, notification, and alarm volume on the device.

Sound Options

The options for sound types are found in this section.

NOTE: Zebra Enterprise Computers do not support haptic feedback, so they will not vibrate.

- **Zebra volume controls:**
  - **Media volume** - Controls the music, games, and media volume.
  - **Call volume** - Controls the volume during a call.
  - **Ring volume** - Controls the ringtone volume.
  - **Notifications volume** - Controls the notification volume.
  - **Alarm volume** - Controls the alarm clock volume.
- **Do Not Disturb** - Mutes some or all sounds and vibrations.
- **Live Caption** - Automatically caption speech.
- **Media** - Shows the media player in Quick Settings while sound is playing, allowing quick access.
- **Shortcut to prevent ringing** - Select how the shortcut method prevents ringing (default – enabled).
- **Default notification sound** - Select a sound to play for all system notifications.
- **Default alarm sound** - Select a sound to play for alarms.
- **Other sounds:**
  - **Screen locking sounds** - Play a sound when locking and unlocking the screen (default – enabled).
  - **Charging sounds** - Play a sound when power is applied to the device (default – enabled).
  - **Tap & click sounds** - Play a sound when making taps or clicks (default – enabled)

Setting Wake-Up Sources

This section describes the process to set up wake-up sources for the device.

NOTE: ZEC500 supports Wake on Touch with Zebra TD50 display only (enabled by default). For information on waking the device with the TD50, go to Touch Display TD50.

By default, the device wakes from Sleep mode when the user presses the power button or the programmable button and wakes from suspend mode with the following:

1. Go to **Settings**.
2. Select **Wake-Up Sources**.
   - Toggle on **Home** if you want it to be 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/keymappingmgr/.

1. Go to **Settings**.

2. Select **Key Programmer**.

   A list of programmable buttons displays.

3. Select the button to remap.
4. Select 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.

Keyboards

The device provides multiple keyboard options.

- On-screen Keyboard
  - Gboard
  - Google Voice Typing
- Enterprise Keyboard
- USB Keyboard
- Bluetooth Keyboard

Keyboard Configuration

This section describes configuring the device's keyboard.

Enabling Keyboards

This section describes how to enable keyboards.

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

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

This section describes the steps to take in order to change the language setting.

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

   A list of available languages displays.
4. If the desired language is not listed, select **Add a language** and select a language from the list.
5. Select 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. Select **System** > **Languages & input** > **Personal dictionary**.
3. If prompted, select the language where this word or phrase is stored.

4. Select + 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, select **Settings** > **Notifications**.

To view app notifications, select **Settings** > **Apps** > **All apps**, and then select an app.

Setting App Notifications

Configure the notifications settings for a specific app.

1. Go to **Settings**
2. Select **Apps** > **All apps**, and then select an app.
3. Select **Notifications**.

   Options vary depending on the app selected.
4. Select the switch to turn on or off notifications for this app.
   - **Allow notification dot** - Do not allow this app to add a notification dot to the app icon.
   - **Additional settings in the app** - Open the app settings.

Viewing Notifications

This section describes the steps to take in order to view notifications.

1. Go to **Settings**.
2. Select **Notifications** > **App Settings**.

   The **App notifications** screen appears.
3. Select **Turned off** to view how many app notifications are turned off.

Controlling Lock Screen Notifications

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

1. Go to **Settings**.
2. Select **Notifications** > **Notifications on lock screen** and select one of the following:
   - **Show conversations, default, and silent** (default)
   - **Hide silent conversations and notifications**
   - **Don't show any notifications**

Applications

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

Installed Applications

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

Table 14 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.
	**DWDemo** - Provides a way to demonstrate the data capture features using the imager.
	**ZLicenseMGR** - Use to manage software licenses on the device.
	**RxLogger** - Use to diagnose device and app issues.
	**Settings** - Use to configure the device.
	**StageNow** - Allows the device to stage a device for initial use by initiating the deployment of settings, firmware, and software.

Table 14 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, email 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.
	**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, drag up from the bottom of the screen.
2. Drag the **APPS** window up or down to view more app icons.
3. Select an icon to open the app.

Viewing Recent Apps

Use the shortcut to view and access recently used apps.

1. Select ■.

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

DataWedge Demonstration

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

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

NOTE: DataWedge on the ZEC500 will only work if a Bluetooth scanner is paired or a USB scanner is connected.

DataWedge Demonstration Icons

This section provides information on DataWedge Demonstration Icons.

Table 15 DataWedge Demonstration Icons

Category	Icon	Description
Illumination		Imager illumination is on. Select to turn illumination off.
Illumination		Imager illumination is off. Select to turn illumination on.
Data Capture		The data capture function is through the internal imager.
Data Capture		The data capture function is through the rear camera.
Data Capture		Indicates a USB scanner is connected to the device.
Data Capture		Indicates a USB scanner is not connected to the device.
Data Capture		A Bluetooth scanner is connected.
Data Capture		A Bluetooth scanner is not connected.
Scan Mode		Imager is in picklist mode. Select to change to normal scan mode.
Scan Mode		Imager is in normal scan mode. Select 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

This section describes the steps to take to initiate the main chat head.

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

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

Removing the Main Chat Head

This section describes the steps to take to remove the main chat head.

1. Select and drag the icon.

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

Viewing Logs

This section describes the steps to take to view logs.

1. Select the Main Chat Head icon.

   The RxLogger Utility screen displays.
2. Select 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. Select a Sub Chat Head to display the log contents.

Removing a Sub Chat Head Icon

This section describes the step to take to remove sub chat head icons.

- To remove a Sub Chat Head icon, select 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. Select 💾.

   The Backup dialog box appears.
2. Select **Yes** to create the backup.

Data Capture

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

The ZEC500 supports both Bluetooth pairing and USB connectivity for scanners.

Refer to the corresponding Bluetooth or USB scanner Product Reference Guide on zebra.com for specific scanner information.

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 scanner farther away for larger symbols.
- Move the scanner 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.

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

Enabling DataWedge

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

1. Drag up from the bottom of the Home screen and select .
2. Select > **Settings**.
3. Select 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. Drag up from the bottom of the Home screen and select .
2. Select > **Settings**.
3. Select the **DataWedge enabled** checkbox.

   The blue checkmark disappears in the checkbox indicating that DataWedge is disabled.

Wireless

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

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

Wireless Local Area Networks

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

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

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **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/WPA3 Enterprise (EAP)
  - Lightweight Extensible Authentication Protocol (LEAP) - Only available with mDNA Enterprise Bundle upgrade.
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
  - Transport Layer Security (TLS)
  - Tunneled Transport Layer Security (TTLS) - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.
  - Flexible Authentication via Secure Tunneling (EAP-FAST) - with 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

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. Select **Network & internet**.
3. Select **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, select the profile once or press and hold and then select **Connect** or for secure networks, enter the required password or other credentials, then select **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, go to 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 16 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. Select **Network & internet** > **Internet**.
3. Scroll down to the bottom of the list and select **Saved networks**.
4. Select the name of the network.
5. Select **FORGET**.

   The device automatically disconnects from the Wi-Fi network.

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. Select **Network & Internet**.
3. Select **Internet**.
4. Toggle **ON**.

   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. Select the desired network. If the network security is **Open**, the device automatically connects to the network. For all other network securities, a dialog box opens.

7. If network security is **WPA/WPA2/WPA3 Enterprise**:
   a) Select the **EAP method** drop-down list and select one of the following:
      - **PEAP**
      - **TLS**
      - **TTLS**
      - **WD**
      - **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.
      - Select **Advanced options** to display additional network options
8. If the network security is **WPA3-Enterprise 192-bit**:
   - Select **CA certificate** and select a Certification Authority (CA) certificate.

NOTE: Certificates are installed using the Security settings.

   - Select **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.

9. Select **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. Select **Network & internet** > **Internet**.
3. Toggle 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**, select **Save**.
8. If the network security is **None**, select **Save**.
9. If the network security is **WEP**, **WPA3-Personal**, or **WPA/WPA2-Personal**, enter the required password and then select **Save**.
10. If the network security is **WEP** or **WPA/WPA2-Personal**, enter the required password and then select **Save**.

NOTE: By default, the network Proxy server is set to **None** and the IP setting is set to DHCP. Go to 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) Select 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.
       - Select **Advanced options** to display additional network options.

12. If the network security is WPA3-Enterprise 192-bit:
    - Select **CA certificate** and select a Certification Authority (CA) certificate.

NOTE: Certificates are installed using the Security settings.

    - Select **User certificate** and select a user certificate.

NOTE: User certificates are installed using the Security settings.

    - In the **Identity** text box, enter the user name credentials.
13. Select **Save**. To connect to the saved network, select 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. Select **Network & Internet** > **Internet**.
3. Toggle the Wi-Fi switch to the **On** position.
4. In the network dialog box, select a network.
5. If configuring the connected network, select to edit the network details and then select the down arrow to hide the keyboard.
6. Select **Advanced options**.
7. Select **Proxy**.
8. Select **Manual**.
9. In the **Proxy hostname** text box, enter the address of the proxy server.
10. In the **Proxy port** text box, enter the port number for the proxy server.
11. In the **Bypass proxy for** text box, enter addresses for websites that are not required to go through the proxy server. Use a comma “,” between addresses. Do not use spaces or carriage returns between addresses.
12. If configuring the connected network, select **Save**; otherwise, select **Connect**.
13. Select **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. Select **Settings**.
2. Select **Network & Internet** > **Internet**.
3. Drag the Wi-Fi switch to the **On** position.
4. In the network dialog box, select a network.
5. If configuring the connected network, select to edit the network details and then select the down arrow to hide the keyboard.
6. Touch **Advanced options**.
7. Select **IP settings** and select **Static**.
8. In the **IP address** text box, enter an IP address for the device.
9. If required:
   - In the **Gateway** text box, enter a gateway address for the device.
   - In the **Network prefix length** text box, enter the prefix length.
   - In the **DNS 1** text box, enter a Domain Name System (DNS) address.
   - In the **DNS 2** text box, enter a DNS address
10. If configuring the connected network, select **Save** otherwise, select **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 select **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** - Select to view additional Wi-Fi settings.
- **Install Certificates** - Select to install certificates.

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 select **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)** - Select to display the **Available channels** menu. Select specific channels and select **OK**.
  - **Available channels (5 GHz)** - Select to display the **Available channels** menu. Select specific channels and select **OK**.
  - **Available channels (5 GHz)** - Select to display the **Available channels** menu. Select specific channels and select **OK**. Only available with mDNA Enterprise Bundle upgrade.
  - **Available channels (6 GHz)** - Select to display the **Available channels** menu. Select specific channels and select **OK**.
- **Logging**
  - **Advanced Logging** - Select to enable advanced logging or change the log directory.
  - **Wireless logs** - Use to capture Wi-Fi log files.
    - **Fusion Logger** - Select 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** - Select to display live status of WLAN state. Also provides information about the device and connected profile.
- **About**
  - **Version** - Displays the current version information. Select the version to display addition version details.

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 17 Bluetooth Profiles

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

Table 17 Bluetooth Profiles (Continued)

Profile	Description
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.
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.

Table 17 Bluetooth Profiles (Continued)

Profile	Description
Dial Up Networking (DUN)	Provides a standard to access the Internet and other dial-up services over Bluetooth.
Generic Access Profile (GAP)	Use for device discovery and authentication.
OBject EXchange (OBEX)	Facilitates the exchange of binary objects between devices.

Bluetooth Power States

The Bluetooth radio is off by default.

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

Bluetooth Radio Power

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

Enabling Bluetooth

This section describes the steps to take to enable Bluetooth.

1. Drag down from the Status bar to open the Notification panel.
2. Select to turn Bluetooth on.

Disabling Bluetooth

This section describes the steps to take to disable Bluetooth.

1. Drag down from the Status bar to open the Notification panel.
2. Select 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. Select **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the **Paired Devices** list, select next to the device name.
4. Select **FORGET**.

Selecting Profiles on the Bluetooth Device

Some Bluetooth devices have multiple profiles.

1. Go to **Settings**.
2. Select **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the **Paired Devices** list, select 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. Select **Connected devices** > **Connection preferences** > **Bluetooth**.
3. In the list, select 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. Select **Connected devices** > **Connection preferences** > **Bluetooth**.
3. If Bluetooth is not on, move the switch to turn Bluetooth on.
4. Select **Device name**.
5. Enter a name and select **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. Drag down from the Status bar to open the Quick Access panel.
5. Select and hold **Bluetooth**.
6. Select **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. Select **Pair** on both devices.
9. The Bluetooth device is added to the **Paired devices** list and a trusted (“paired”) connection is established.

Near Field Communications

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

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

The device supports the following operating modes:

- Reader mode

Using NFC, the device can:

- Read contactless cards, such as contactless tickets, ID cards, and ePassport.
- Read and write information to contactless cards, such as SmartPosters and tickets, as well as devices with an NFC interface, such as vending machines.
- Read information from supported medical sensors.
- Pair with supported Bluetooth devices such as printers, ring scanners (for example, RS6000), and headsets (for example, HS3100).
- 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.

The device's NFC antenna is positioned to read NFC cards from the top of the device while the device is on a flat surface.

Enterprise NFC Settings

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

- **Card Detection Mode** - Select a card detection mode.
  - **Standard** - Provides the optimal NFC detection speed.
- **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, go to: techdocs.zebra.com/nfcmgr/.

Accessories

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

Supported Accessories are as follows:

- TD50

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 11 TD50 Rear View with Back Cover Removed Features

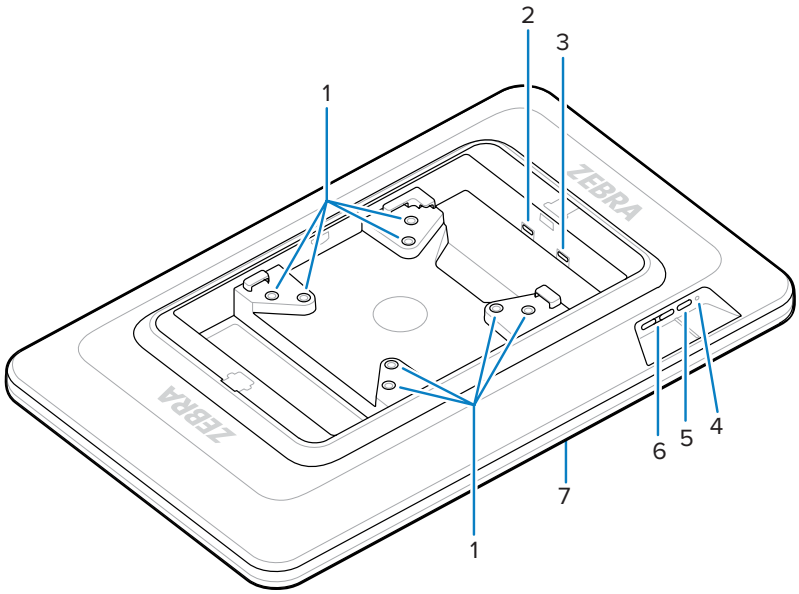


Table 18 Rear View Features

Number	Item	Description
1	VESA-compliant Mounting Inserts	M4 threaded inserts - 100 mm (3.94 in.) and 75 mm (2.95 in.) squares.
2	USB-C Port	Accepts power if the source device is insufficient to power the device.
3	USB-C Display Port	Accepts power and display information. **NOTE:** Cable requirements: • USB 3.1 GEN 1 super speed data transmission. • Less than 2 meters in length. • Signal lines including SBU1, SBU2, CC1 and CC2. • The combined four pins of VBus and GND are capable of carrying a minimum of 2 A of current. The Zebra cable CBL-EC5X-USBC3A-01 is recommended for use with the ZEC500.[a]
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.

[a] Other cables, such as Zebra TC2X/TC52/TN28 cables, do not have the necessary superspeed or other signal lines needed for the ZEC500 to function with the TD50 secondary monitor.

Connecting the TD50

The TD50 connects to the ZEC500 for an additional display configuration.

The USB-C cable needs to meet the following requirements:

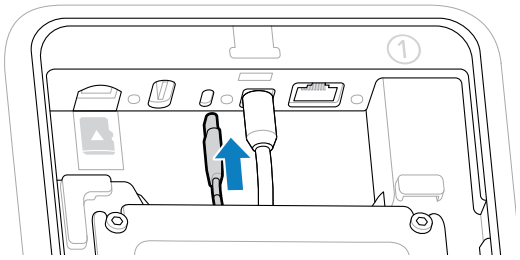
- USB 3.1 GEN 1 super speed data transmission.
- Less than 2 meters in length.
- Signal lines including SBU1, SBU2, CC1 and CC2.
- The combined four pins of VBus and GND are capable of carrying a minimum of 2 A of current.

These cable requirements ensure that the video display transmits to the TD50.

NOTE: The Zebra cable CBL-EC5X-USBC3A-01 is recommended for use with ZEC500.

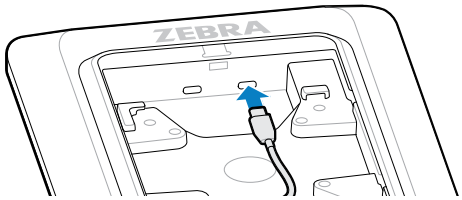
NOTE: When using the TD50 or any DisplayPort display as the sole display with the ZEC500, set the screen lock to **None** before connecting, as the screen lock is only supported on HDMI displays.

1. Connect a USB-C cable to the USB-C port on the ZEC500.



2. Connect the other end of the USB-C cable to the DP 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 websites.

Secure Certificates

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

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

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

Installing a Secure Certificate

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

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory.
2. Go to **Settings**.
3. Select **Security** > **More security settings** > **Encryption & credentials**.
4. Select **Install a certificate** and select the type of certificate.
5. Navigate to the location of the certificate file.

6. Select the filename of the certificate to install.
7. If prompted, enter the certificate's password and select **OK**.
8. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.
9. Select **OK**.

Configuring Credential Storage Settings

Configure credential storage from the device settings.

1. Go to **Settings**.
2. Select **Security** > **More security settings** > **Encryption & credentials**.
3. Select an option:
   - Select **Trusted credentials** to display the trusted system and user credentials.
   - Select **User credentials** to display user credentials.
   - Select **Install from storage** to install a secure certificate from the microSD card or internal storage.
   - Select **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. Select **About phone**.
3. Scroll down to **Build number**.
4. Select **Build number** seven times.

   The message **You are now a developer!** appears.
5. Select **Back**.

6. Select **System** > **Developer options**.
7. Toggle the **USB debugging** switch to the **ON** position.

EMDK for Android

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

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

For more information, go to techdocs.zebra.com/emdk-for-android/about/.

StageNow for Android

StageNow is Zebra's 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/stagenow/.

GMS Restricted

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

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

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

ADB USB Setup

To use the Android Debug Bridge (ADB), install the development SDK on the host computer then install the ADB and USB drivers.

NOTE: To ensure the device performs as expected, power on the device first before connecting a USB cable from the host computer.

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. Select **About phone**.
3. Scroll down to **Build number**.
4. Select **Build number** seven times.

   The message **You are now a developer!** appears.
5. Select **Back**.
6. Select **System** > **Developer options**.
7. Toggle the **USB debugging** switch to the **ON** position.
8. Select **OK**.
9. Connect the device to the host computer using the USB Cable.

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

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

NOTE: An HDMI display is required for using Recovery mode. The Recovery Menu will not appear on a display connected over DisplayPort.

IMPORTANT: When accessing recovery mode, avoid connecting a USB keyboard, as it will prevent using the programmable button.

1. Press and hold the power button until the menu appears.
2. Select **Power Off**.
3. Press the power button so the device boots.
4. Press and hold the programmable button until the device boots into the Recovery menu.

NOTE: To navigate the Android Recovery menu, use the programmable button to navigate and the power button to select.

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. Drag the screen up and select to view files on the USB drive.
6. Select **General USB drive**.

7. Locate the application APK file.
8. Select the application file.
9. Select **Continue** to install the app or **Cancel** to stop the installation.
10. To confirm installation and accept what the application affects, select **Install** otherwise, select **Cancel**.
11. Select **Open** to open the application or **Done** to exit the installation process.

    The application appears in the App list.
12. 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.

NOTE: This method is not recommended due to limited Internal Storage.

1. Connect the device to a host computer using the USB-C cable.
2. Select **File Transfer**.
3. On the host computer, open a file explorer application.
4. 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.

5. Disconnect the device from the host computer.
6. Drag the screen up and select to view files on the microSD card or Internal Storage.
7. Locate the application APK file.
8. Select the application file.
9. Select **Continue** to install the app or **Cancel** to stop the installation.
10. To confirm installation and accept what the application affects, select **Install**. Otherwise, select **Cancel**.
11. Select **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

NOTE: 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. Select **Settings**.
4. Select **System** > **Developer options**.
5. Enable **Developer options**.
6. Select the **USB Debugging** toggle to enable it.
7. Select **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. Select **OK** or **Allow**.
10. On the host computer, navigate to the platform-tools folder and open a command prompt window.
11. Type `adb install <application>`.

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

Installing Applications Using Wireless ADB

Use ADB commands to install an application onto the device.

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

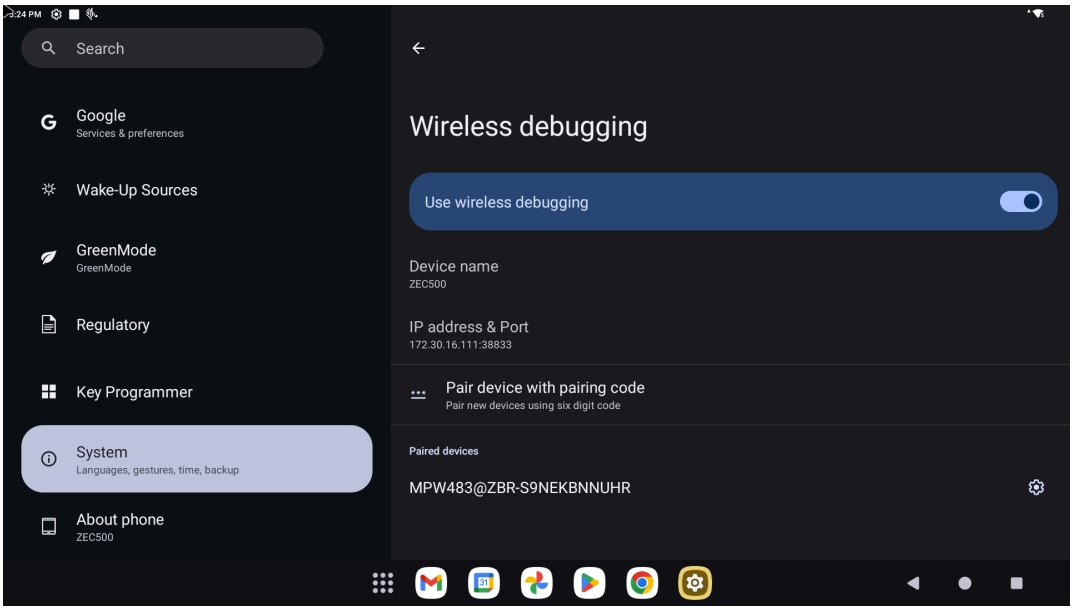
1. Go to **Settings**.
2. Select **System** > **Developer options**.

IMPORTANT: If **Developer options** does not appear in the advanced system settings on your device, perform the steps in Enabling Developer Options on page 62.

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) Select **ALLOW**.

6. Select **Wireless debugging**.

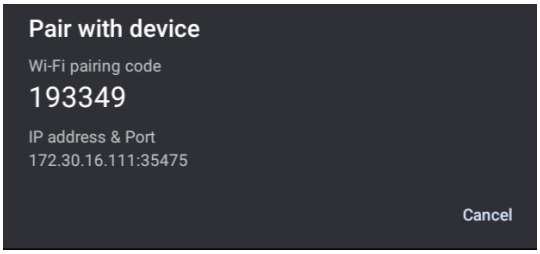
   The Wireless debugging screen displays.



NOTE: Observe the IP address and Port on the **Wireless debugging** screen.

7. Select **Pair device with pairing code**.

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



NOTE: The Port on the **Pair with device** dialog box will be different than the one on the **Wireless debugging** screen. The IP address will be the same.

8. On the host computer, navigate to the **platform-tools** folder and open a command prompt window.
9. 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.
10. Press **Enter**.
11. Type the pairing code from the **Pair with device** dialog box.
12. Press **Enter**.
13. 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.

14. Press **Enter**.

    The device is now connected to the host computer.

15. 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.

16. Press **Enter**.
17. Type `adb install <file>`.

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

18. Press **Enter**.
19. 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.

NOTE: This section only applies to premium models.

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. Press and hold the power button on the device until the menu appears.
6. Select **Power off**.
7. Insert the microSD card into the device.
8. Press and hold the power button to turn on the device.

9. Drag the screen up and select to view files on the microSD card.
10. Select **SD card**.
11. Locate the application APK file.
12. Select the application file.
13. Select **Continue** to install the app or **Cancel** to stop the installation.
14. To confirm installation and accept what the application affects, select **Install**. Otherwise, select **Cancel**.
15. Select **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. Select **See all apps** to view all apps in the list.
3. Scroll through the list to the app.
4. Select the app.

   The **App info** screen displays.
5. Select **Uninstall**.
6. Select **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 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 and hold the power button until the menu appears.
3. Select **Restart**.
4. Press and hold the programmable button until the device vibrates.

5. Press the programmable button to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
6. Press the power button.
7. Press the programmable button to navigate to the System Update file.
8. Press the power button.

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

Performing a System Update Using ADB

Use ADB to perform a system update.

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

NOTE: To ensure the device performs as expected, power on the device first before connecting a USB cable from the host computer.

1. Connect the device to a host computer using a USB cable.
2. Go to **Settings**.
3. Select **System** > **Developer options**.
4. Toggle the USB debugging switch to the **ON** position.
5. Select **USB Debugging**. A check mark appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Select **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 the programmable button to navigate to **Apply upgrade from ADB**.
12. Press the power button.
13. On the host computer command prompt window type `adb sideload file`

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

14. Press **Enter**.

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

Performing a System Update Using a USB Drive

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

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

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 the power button until the menu appears.
7. Select **Restart**.
8. Press and hold the programmable button until the Zebra logo screen appears.

   The System Recovery screen appears.
9. Press the programmable button to navigate to **apply upgrade from USB drive**.
10. Press the power button.
11. Use the programmable button to navigate to the System Update zip file.
12. Press the power button.

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

Verifying System Update Installation

Verify that the system update was successful.

1. Go to **Settings**.
2. Select **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

Perform an enterprise reset from the device settings.

1. Go to **Settings**.
2. Select **System** > **Reset Options** > **Erase all data (enterprise reset)**.
3. Select **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 and hold the power button until the menu appears.
3. Select **Restart**.
4. Press and hold the programmable button until the device vibrates.
5. Press the programmable button to navigate to **Apply upgrade from SD card**.
6. Press the power button.
7. Press the programmable button to navigate to the Enterprise Reset file.
8. Press the power button.

   The Enterprise Reset occurs and then the device returns to the Recovery screen.
9. Press the power button 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.

NOTE: To ensure the device performs as expected, power on the device first before connecting a USB cable from the host computer.

1. Connect the device to a host computer using a USB cable.
2. Go to **Settings**.
3. Select **System** > **Developer options**.
4. Slide the **USB debugging** switch to the **ON** position.
5. Select **System** > **Developer options**.
6. Select **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. On the device, press the programmable button to navigate to **Apply upgrade from ADB**.
12. Press the power button.
13. On the host computer command prompt window type `adb sideload <file>`

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

    The Enterprise Reset package installs and then the 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. On the device, navigate to **Reboot system now** and press the power button to reboot the device.
18. Disconnect the USB cable from the device.

Performing an Enterprise Reset Using USB Drive

Perform 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 the power button until the menu appears.
3. Select **Restart**.
4. Press and hold **Blue** until the Zebra boot screen appears.

   The Android Recovery screen appears.
5. Press the programmable button to navigate to **apply update from USB drive**.
6. Press the power button.
7. Press the programmable button to navigate to the Enterprise Reset file.
8. Press the power button.

   The Enterprise Reset occurs and then the device returns to the Recovery screen.
9. Press the power button to reboot the device.

See Also

USB Communication

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 a 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 and hold the power button until the menu appears.
3. Select **Restart**.
4. Press and hold the programmable button until the device vibrates.
5. Press the programmable button to navigate to **Apply upgrade from SD card** or **Apply downgrade from SD card**.
6. Press the power button.
7. Press the programmable button to navigate to the Factory Reset file.
8. Press the power button.

   The Factory Reset occurs, and then the device returns to the Recovery screen.
9. Navigate to **Reboot system now** and press the power button to reboot the device.

Performing a Factory Reset Using ADB

Perform a factory reset using ADB.

Go to the Zebra Support & Downloads website at zebra.com/support and download the appropriate Factory Reset file to a host computer.

NOTE: To ensure the device performs as expected, power on the device first before connecting a USB cable from the host computer.

1. Connect the device to a host computer using a USB-C cable.
2. Go to **Settings**.
3. Select **System** > **Developer options**.
4. Slide the **USB debugging** switch to the **ON** position.
5. Select **USB Debugging**. A check mark appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Select **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 the programmable button to navigate to **Apply upgrade from ADB** or **Apply downgrade from ADB**.
12. Press the power button.
13. On the host computer command prompt window type `adb sideload <file>`.

    where: <file> = the path and filename of the zip file.
14. Press the power button.

    The Factory Reset package installs, and then the **System Recovery** screen appears on the device.
15. Press the power button to reboot the device.
16. Disconnect the USB-C cable from the device.

Performing a Factory Reset Using USB Drive

Perform a Factory Reset using a USB drive.

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 USB drive.
   - Copy the zip file to a USB drive using a host computer and then installing the USB drive into the device.
   - Connect the device with a USB drive already installed to the host computer and copy the zip file to the USB drive. Disconnect the device from the host computer.
2. Press and hold the power button until the menu appears.
3. Select **Restart**.

   The device resets.
4. Press and hold the programmable button until the Zebra boot screen.

   The System Recovery screen appears.
5. Press the programmable button to navigate to the **apply update from USB drive**.
6. Press the power button.
7. Press the programmable button to navigate to the Android Reset file.
8. Press the power button.

   The Factory Reset occurs and then the device returns to the Recovery screen.
9. Press the power button to reboot the device.

See Also

USB Communication

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

NOTE: It is recommended to install a microSD card on the device due to limited internal storage space.

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** - Select to view RAM usage by individual apps.

Viewing Memory

View the amount of memory used and free RAM.

1. Go to **Settings**.
2. Select **System** > **Developer options**.
3. Select **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. Select **Storage**.

   The external screen displays the total amount of space on internal storage and the amount used.

   If the device has removable storage installed, select **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. Select **Storage**.

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

   Select **SD card** to view the contents of the card.
3. To unmount the microSD card, select ⏏.
4. To unmount the USB drive, select ⏏.

Formatting a microSD Card as Portable Storage

Format a microSD card as portable storage for the device.

1. Select **SD card**.
2. Select ⋮ > **Storage settings**.
3. Select **Format**.
4. Select **ERASE & FORMAT**.
5. Select **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. Select **SD card**.
2. Select ⋮ > **Storage settings**.
3. Select **Format as internal**.
4. Select **ERASE & FORMAT**.
5. Select **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 (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. Select **Apps**.
3. Select **See all XX apps** to view all apps on the device.
4. Select ⋮ > **Show system** to include system processes in the list.
5. Select 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. Drag the screen up and select .
2. Select > **Downloads**.
3. Select and hold an item to delete, and then select .

   The item is deleted from the device.

Maintenance and Troubleshooting

This section explains how to maintain and troubleshoot the device.

Device Maintenance

To ensure device longevity, Zebra recommends ways to maintain your device.

- Regularly clean the device using compressed air to remove dust from vents and ports.
- Use a microfiber cloth to remove smudges.
- Avoid keeping the device in an enclosed space with poor ventilation.
- Protect the device from extreme temperatures.
- Avoid mounting the device in areas prone to vibrations.
- Organize and secure cables to prevent tangling and strain on ports.
    - Use cable ties to manage cables neatly.
- Regularly inspect for wear and tear.
- Keep the system updated with the latest firmware and software patches to ensure security and optimal performance.
- Do not store the device in any dusty, damp, or wet location.

Cleaning Instructions

This section provides instructions for cleaning the device.

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

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

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

Approved Cleaning and Disinfectant Agents

This section lists the 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 the following important note)
- 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.

Device Troubleshooting

This section provides information on troubleshooting the device.

- If the red LED on your ZEC500 device is blinking, you may need to connect a display to view the error message and select the appropriate option to resolve the issue.

LED Status Light

These sections explain the LED status light and what each color represents.

Power Status LED

This section describes the power status LED lights.

Table 19 LED Status Indicators

State	LED Color	Indications
Solid	Amber	The ZEC500 is on and has no issues.
Flashing	Amber	A staging/OS upgrade is in progress.
Solid	Green	The ZEC500 is booting up.
Blinking	Green	The ZEC500 is in sleep mode.

Table 19 LED Status Indicators (Continued)

State	LED Color	Indications
NOTE: If you are performing a staging/OS upgrade, the status light will be solid green once the upgrade completes.		
Flashing	Red	The ZEC500 had a critical bootup error.
Fast Blinking	Red	A critical staging failure occurred.
Flashing (Red and Green)	Mixed Colors	This indicates a PoE error.

Wireless Workstation Connection Status LED

This section describes the wireless connection status LED lights.

Table 20 LED Status Indicators

State	LED Color	Indications
Fast Blinking	Blue	The ZEC500 is connecting to a host device.
Solid	Blue	The ZEC500 is connected to a host device.
Flashing (Red and Blue)	Mixed Colors	This indicates an attempted connection to the host error.

Resetting the Device

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

Performing a Soft Reset

Perform a soft reset if applications stop responding.

1. Press and hold the power button until the menu appears.
2. Select **Restart**.

   The device reboots.

Performing an Enterprise Reset

Perform an enterprise reset from the device settings.

1. Go to **Settings**.
2. Select **System** > **Reset Options** > **Erase all data (enterprise reset)**.
3. Select **Erase all data** twice to confirm the enterprise reset.

Technical Specifications

This section provides information on the technical specifications of the ZEC500.

Table 21 Value Tier - ZEC500-V

Processor	Qualcomm® 5430-FP2
Memory	6GB LPDDR5 RAM
Storage	64GB UFS 3.1 Flash
OS Version	Android
Ethernet	10/100/1000 Mbps via RJ45
WLAN	WiFi6E 2x2 Mu-MIMO
WPAN	Bluetooth 5.3 Class 2 with Bluetooth Low Energy (BLE)
NFC	ISO 14443 Type A and B; MIFARE, FEliCa, and ISO 15693 cards; Card Emulation via Host
Connectivity Options	HDMI USB-C 3.2 w/DisplayPort 1.4 USB-A 3.2 (3x) RJ45 Ethernet
Maximum Display Resolution Supported	HDMI: 3840 x 2160 @ 30fps USB-C: 3840 x 2160 @ 60fps Concurrent HDMI & USB-C: 3840 x 2160 @30fps  **NOTE:** When USB-C is used for DisplayPort output, communication speed on this port switches to High Speed.
Power	12V-24V DC input, 60W minimum 5.5x2.5mm plug
Operating Temperature	0°C (32°F) to +40°C (104°F) and -29°C (-20°F) to +60°C (140°F) (Extended Temperature SKUs)

Table 21 Value Tier - ZEC500-V (Continued)

Sealing	IP54
Dimensions	• **Standard SKU**: 120 mm (4.72 in.) L x 120 mm (4.72 in.) W x 28 mm (1.10 in.) H • **Extended Temperature SKU**: 120 mm (4.72 in.) L x 120 mm (4.72 in.) W x 35 mm (1.38 in.) H
	• **Standard SKU**: 9.88 oz (280g) • **Extended Temperature SKU**: 11.64 oz (330g)

Table 22 Premium Tier - ZEC500-P

Processor	Qualcomm® 5430-FP2
Memory	8GB LPDDR5 RAM
Storage	128GB UFS 3.1 Flash
OS Version	Android
Ethernet	10/100/1000 Mbps via RJ45
WLAN	WiFi6E 2x2 Mu-MIMO
WPAN	Bluetooth 5.3 Class 2 with Bluetooth Low Energy (BLE)
NFC	ISO 14443 Type A and B; MIFARE, FEliCa, and ISO 15693 cards; Card Emulation via Host
Connectivity Options	HDMI USB-C 3.2 w/DisplayPort 1.4, Power Delivery Input USB-A 3.2 (3x) RJ45 Ethernet MicroSD Card slot
Maximum Display Resolution Supported	HDMI: 3840 x 2160 @ 30fps USB-C: 3840 x 2160 @ 60fps Concurrent HDMI & USB-C: 3840 x 2160 @30fps **NOTE:** When USB-C is used for DisplayPort output, communication speed on this port switches to High Speed.

Table 22 Premium Tier - ZEC500-P (Continued)

Power	12V-24V DC input, 60W minimum 5.5x2.5mm plug Power Delivery Input via USB-C Port • 9V 3A, 15V 3A, 20V 3A supported, with possible limitations. Power over Ethernet: IEEE 802.3at/bt • Class 8 recommended.
Operating Temperature	0°C (32°F) to +40°C (104°F) and -29°C (-20°F) to +60°C (140°F) (Extended Temperature SKUs)
Sealing	IP54
Dimensions	• **Standard SKU**: 120 mm (4.72 in.) L x 120 mm (4.72 in.) W x 28 mm (1.10 in.) H • **Extended Temperature SKU**: 120 mm (4.72 in.) L x 120 mm (4.72 in.) W x 35 mm (1.38 in.) H
Weight	• **Standard SKU**: 10.93 oz (310g) • **Extended Temperature SKU**: 12.7 oz (360g)