Maintenance and Service Guide

SUMMARY

This guide provides information about spare parts, removal and replacement of parts, security, backing up, and more.

Legal information

AMD is a trademark of Advanced Micro Devices, Inc. Bluetooth is a trademark owned by its proprietor and used by HP Inc. under license. Corning and Gorilla are registered trademarks of Corning Incorporated and its subsidiaries. Intel, Core, Optane, and Thunderbolt are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. microSD™ is a trademark or registered trademark of SD-3C LLC. USB Type-C and USB-C are registered trademarks of USB Implementers Forum. DisplayPort and the DisplayPort logo are trademarks owned by the Video Electronics Standards Association (VESA) in the United States and other countries.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: November 2022

Document Part Number: N25493-001

Product notice

This guide describes features that are common to most models. Some features may not be available on your computer.

Not all features are available in all editions or versions of Windows. Systems may require upgraded and/or separately purchased hardware, drivers, software or BIOS update to take full advantage of Windows functionality. Windows 10 is automatically updated, which is always enabled. ISP fees may apply and additional requirements may apply over time for updates. Go to http://www.microsoft.com for details.

To access the latest user guides, go to http://www.hp.com/support, and follow the instructions to find your product. Then select **Manuals**.

Software terms

By installing, copying, downloading, or otherwise using any software product preinstalled on this computer, you agree to be bound by the terms of the HP End User License Agreement (EULA). If you do not accept these license terms, your sole remedy is to return the entire unused product (hardware and software) within 14 days for a full refund subject to the refund policy of your seller.

For any further information or to request a full refund of the price of the computer, please contact your seller.

Not all features are available in all editions of Windows. This computer may require upgraded and/or separately purchased hardware, drivers and/or software to take full advantage of Windows functionality. Go to http://www.microsoft.com for details.

Safety warning notice

Reduce the possibility of heat-related injuries or of overheating the computer by following the practices described.

⚠ **WARNING!** To reduce the possibility of heat-related injuries or of overheating the computer, do not place the computer directly on your lap or obstruct the computer air vents. Use the computer only on a hard, flat surface. Do not allow another hard surface, such as an adjoining optional printer, or a soft surface, such as pillows or rugs or clothing, to block airflow. Also, do not allow the AC adapter to come into contact with the skin or a soft surface, such as pillows or rugs or clothing, during operation. The computer and the AC adapter comply with the user-accessible surface temperature limits defined by applicable safety standards.

Table of contents

1 Computer features

This chapter provides you with an overview of your computer's features.

Standard features

To identify a typical computer configuration, read this section. Features vary depending on the model.

Mobile system with grip

Convertible system with grip

Convertible system with grip and fingerprint reader, without payment system

Convertible system with grip, without fingerprint reader or payment system

The HP Engage Go 13.5 is designed for long-term deployment within general retail, hospitality, and other markets. It includes the following features:

- Integrated connecting form factor available in mobile and connecting systems, both with a grip.
- **34.3 cm** (13.5 in) display panel; high definition (1920 × 1280) resolution, 340 nit, multitouch, Corning® Gorilla® Glass 5
- Docking stand
- Major integrated peripherals:
  - Optional barcode scanner with integrated audio/video feedback and trigger button (configurable as upward facing or downward facing)
  - Optional fingerprint reader
  - NFC authentication
  - Optional contactless payment card scanner (available in the US only)
- Basic I/O connectivity base
  - Three powered serial ports (0 V, 5 V, 12 V)

  - Four USB 2.0 ports
  - Two USB SuperSpeed 5 Gbps ports
  - RJ-11 (modem) jack
  - RJ-45 (network) jack
  - Video-out USB Type-C® port
  - USB Type-C power connector
  - Security cable slot
  - microSD card reader
  - Audio-out (headset) jack
  - Power connector
- Advanced I/O connectivity base
  - Two powered serial ports (0 V, 5 V, 12 V)
  - Two 12 V powered USB ports
  - 24 V powered USB port
  - Four USB SuperSpeed 5 Gbps ports
  - RJ-11 (cash drawer) jack
  - RJ-45 (network) jack
  - Video-out USB Type-C port
  - USB Type-C power port
  - Security cable slot
  - microSD card reader
  - Audio-out (headset) jack
  - Power connector

Mobile head unit features

To identify the mobile head unit features, use this illustration and table.

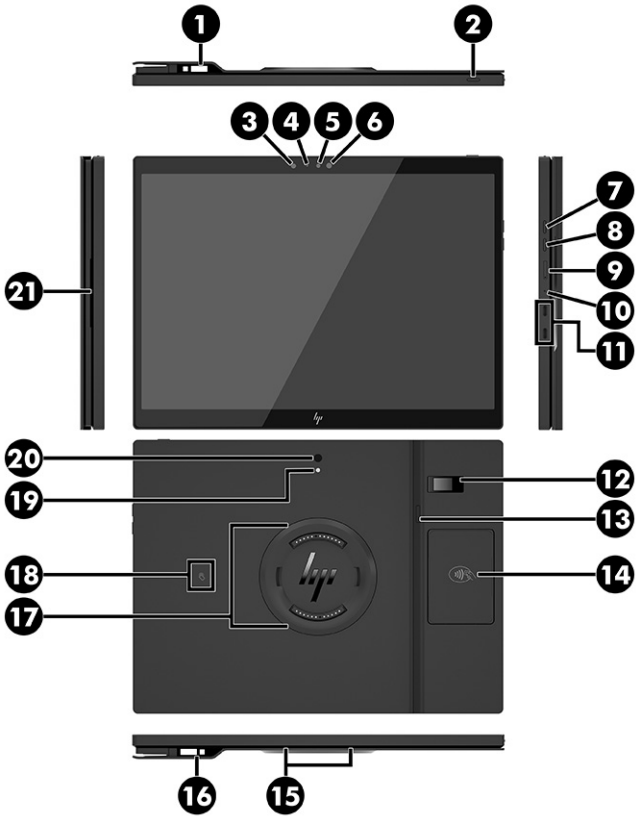


Table 1-1 Identifying the mobile head unit features

Features			
1	Upward-facing laser barcode scanner* (optional)	12	Fingerprint reader (optional)
2	Power button	13	Barcode scanner button (optional)
3	Ambient light sensor	14	Contactless payment card scanner (optional)**
4	Camera light	15	Microphones (2)
5	Camera	16	Downward-facing laser barcode scanner* (optional)
6	Infrared light	17	Docking connector (optional)
7	Volume up button	18	Near-field communication (NFC)
8	Volume down button	19	Rear-facing camera light
9	SIM card slot (optional)	20	Rear-facing camera
10	Charging LED	21	Payment card slot (optional)**
11	USB Type-C ports (2)		
	* The barcode scanner button is always active when the computer is docked or undocked.		
	**Only available in the US.		

Integrated features

To identify the computer features, use this illustration and table.

NOTE: The integrated devices shown are optional.

Table 1-2 **Identifying the integrated features**

Features			
1	**34.3 cm** (13.5 in), 1920 × 1280, high definition display	3	I/O connectivity base
2	Docking release button	4	Biometric fingerprint reader (optional)

Docking stand

You can use the mobile system with the docking stand.

NOTE: You can use the docking stand only with convertible models.

Basic I/O connectivity base components

To identify the basic I/O connectivity base features, use this illustration and table.

Table 1-3 Identifying the basic I/O connectivity base features

Features			
1	RJ-11 (modem) jack	7	USB Type-C port
2	Power connector	8	RJ-45 (network) jack
3	USB Type-C® powered port	9	Security cable slot
4	Powered serial ports (3)	10	microSD™ card reader (select products only)
5	USB 2.0 ports (4)	11	Headset jack
6	USB SuperSpeed 5 Gbps ports (2)		
IMPORTANT: To avoid damage to the computer, **do not** plug a telephone cable into the modem jack.			

Advanced I/O connectivity base components

To identify the advanced I/O connectivity base features, use this illustration and table.

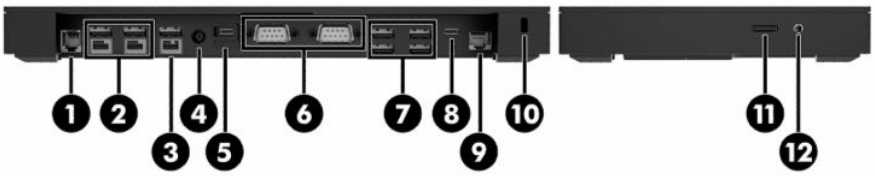


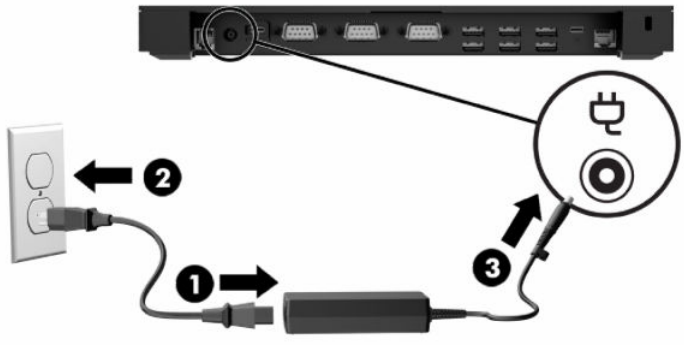
Table 1-4 Advanced I/O connectivity base features

Features			
1	RJ-11 (modem) jack	7	USB SuperSpeed 5 Gbps ports (4)
2	Powered USB 12 V ports (2)	8	USB Type-C port
3	Powered USB 24 V port	9	RJ-45 (network) jack
4	Power connector	10	Security cable slot
5	USB Type-C powered port	11	microSD card reader (select products only)
6	Powered serial ports (2)	12	Headset jack
IMPORTANT: To avoid damage to the computer, **do not** plug a telephone cable into the modem jack.			

Connecting an AC adapter to power

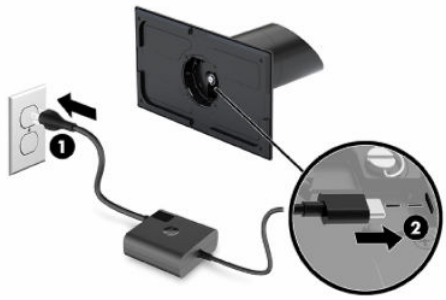
To connect an AC adapter to the I/O connectivity base, use this procedure and illustration.

- To connect an AC adapter to the I/O connectivity base, connect one end of the power cord to the AC adapter **(1)** and the other end to a grounded AC outlet **(2)**, and then connect the AC adapter to the power connector on the I/O connectivity base **(3)**.



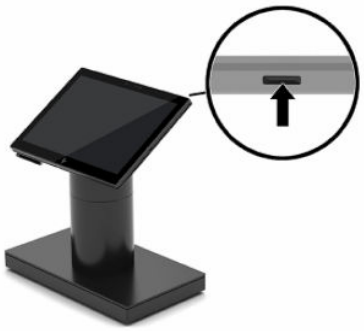
- To connect an AC adapter to the mobile system when it is not connected to an I/O connectivity base, connect the AC adapter to a grounded AC outlet **(1)**, and then connect the power adapter's USB Type-C connector to the USB Type-C power port on the underside of the stand or stability base **(2)**.

NOTE: The power light illuminates when a valid AC adapter is used. If an invalid AC adapter is used, the light does not turn on, even if the adapter is plugged into a wall socket.



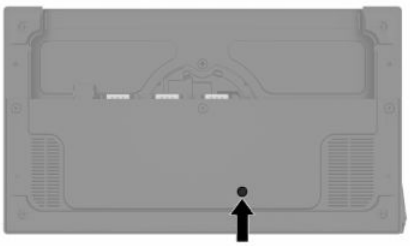
Locating the mobile system power button

The computer power button is located on the top-right edge of the bezel.



Locating the I/O connectivity base power button

The power button is located on the underside of the I/O connectivity base.



The head unit controls the I/O connectivity base. When the head unit is turned off, the I/O connectivity base is turned off, and power is not available from the I/O connectivity base ports. The exception is the I/O connectivity base USB port that connects to the head unit. That port remains powered so that it can continue to communicate with the head unit and allow the I/O connectivity base to turn back on when the head unit is turned on.

After the system is turned off, you can press the power button on the underside of the I/O connectivity base to allow power to be available on the I/O connectivity base ports while the head unit remains turned off.

Adjusting the mobile head unit

You can tilt the mobile head unit by as much as 10° when you set the angle between 50° and 60°.

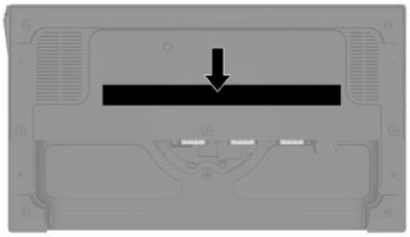
You can swivel the mobile head unit 180° in either direction.

Mobile system serial number location

Each computer has a unique serial number and a product ID number that are located on the exterior of the computer. Keep these numbers available when you contact customer service for assistance.

I/O connectivity base serial number location

Each I/O connectivity base has a unique serial number and a product ID number that is located on the exterior of the base. Keep these numbers available when you contact customer service for assistance.



Regulatory information is located in the base plate or wall mount. To see this information, you must disassemble the base plate or wall mount. Be sure to reassemble the base plate or wall mount after disassembly.

2 Hardware setup

Use these sections to set up and configure your mobile system.

Tools needed

You need a Phillips screwdriver and a Torx T15 screwdriver to complete the procedures described in this guide.

Warnings and cautions

Before performing upgrades, be sure to carefully read all of the applicable instructions, cautions, and warnings in this guide.

⚠ **WARNING!** To reduce the risk of personal injury from electric shock, hot surfaces, or fire:

- Disconnect the power cord from the AC outlet before removing the enclosure. Energized parts are inside.
- Allow the internal system components to cool before you touch them.
- Replace and secure the enclosure before restoring power to the equipment.
- Do not connect telecommunications or telephone connectors to the network interface controller (NIC) receptacles.
- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) AC outlet that is easily accessible at all times.

For your safety, do not place anything on power cords or cables. Arrange them so that no one can accidentally step on or trip over them. Do not pull on a cord or cable. When unplugging from the AC outlet, grasp the cord by the plug.

To reduce the risk of serious injury, read the *Safety & Comfort Guide*. It describes proper workstation setup and provides guidelines for posture and work habits that increase your comfort and decrease your risk of injury. It also provides electrical and mechanical safety information. This guide is located on the web at http://www.hp.com/ergo.

IMPORTANT: Static electricity can damage the electrical components of the computer or optional equipment. Before beginning these procedures, be sure that you are discharged of static electricity by briefly touching a grounded metal object.

When the computer is plugged into an AC power source, voltage is always applied to the system board. You must disconnect the power cord from the power source and wait 30 seconds before opening the computer to prevent damage to internal components.

Locking and releasing the mobile head unit

The mobile head unit automatically locks to the dock when attached. To release the mobile head unit, press the lock release button on the front of the dock's column.

You can use two authentication methods to release the mobile head unit. Set up the authentication methods using the HP SureLock wizard.

- Windows® user authentication: You can define a group that allows users to release the mobile head unit based on their Windows login password.
- PIN authentication: A PIN is required to release the mobile head unit.

NOTE: You can require one, both, or no authentication method to release the mobile head unit. The default setting requires no authentication.

The light on the dock lock release button indicates the locking status.

- Amber: The mobile head unit is locked and cannot be released without the proper Windows login permission.
- White: The mobile head unit is locked and might require a PIN to release it.
- Green: The mobile head unit is not locked and can be removed.

Attaching the mobile head unit to the dock

To attach the mobile head unit to the dock, use this procedure and illustration.

To attach the mobile head unit to the dock:

- Align the rear of the mobile head unit with the top of the dock's column, and place the mobile head unit onto the dock. The mobile head unit automatically locks to the dock when attached.

Removing the mobile head unit from the dock

To remove the mobile head unit from the dock, use this procedure and illustration.

NOTE: Your system might require a PIN to unlock the mobile head unit from the dock. See Locking and releasing the mobile head unit on page 11.

To remove the mobile head unit from the dock:

- Press the lock release button **(1)** on the front of the dock's column, and then lift the mobile head unit **(2)** off the dock.

Attaching an I/O connectivity base to the mobile system

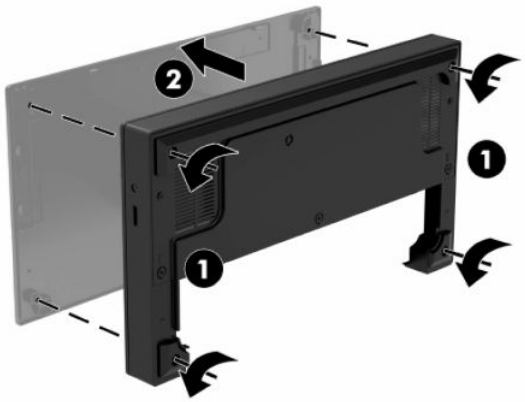
You can attach an I/O connectivity base to the bottom of the stand.

To attach an I/O connectivity base:

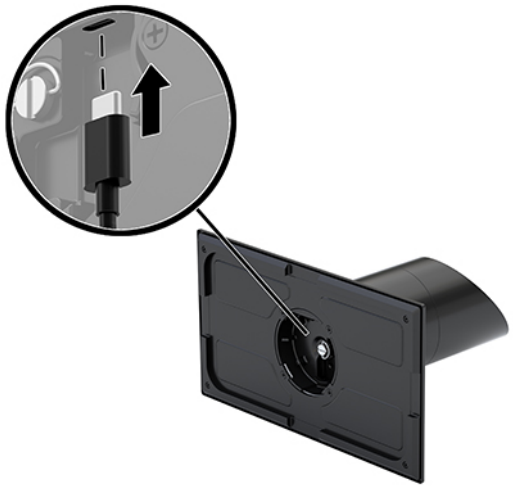
1. Turn off the mobile system properly through the operating system, and turn off any external devices.
2. Disconnect the power cords from the mobile system and I/O connectivity base.

IMPORTANT: Regardless of the power state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord and wait approximately 30 seconds for the power to drain to avoid damage to the internal components.

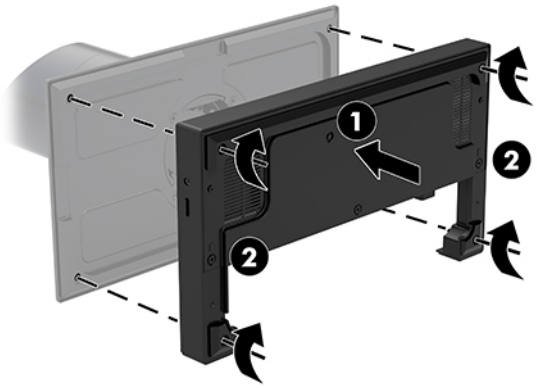
3. Remove the cover from the I/O connectivity base by removing the four screws on the underside of the I/O connectivity base **(1)** and then lifting the cover off the I/O connectivity base **(2)**.



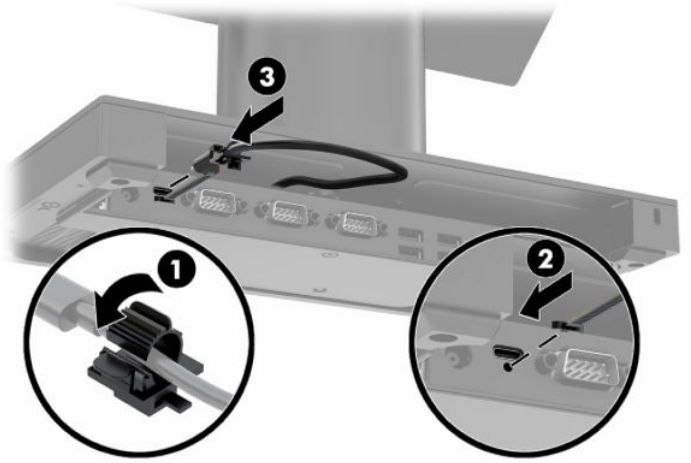
4. Connect the USB Type-C power cord to the USB Type-C port on the underside of the stand column.



5. Place the I/O connectivity base onto the bottom of the stand **(1)**, and then tighten the four screws on the underside of the I/O connectivity base **(2)** to secure the I/O connectivity base to the dock. Be sure that the USB Type-C power cable is routed through the gap between the back of the I/O connectivity base and the stand.



6. To connect and secure the USB Type-C power cable, attach the cable clip to the cable **(1)**, insert the cable tie into the hole **(2)** below the USB Type-C port on the I/O connectivity base, and then slide the cable clip onto the cable tie and connect the cable to the port **(3)**.



7. Connect the AC adapter to the I/O connectivity base and a grounded AC outlet. See Connecting an AC adapter to power on page 7.

Connecting a standalone I/O connectivity base to the mobile system

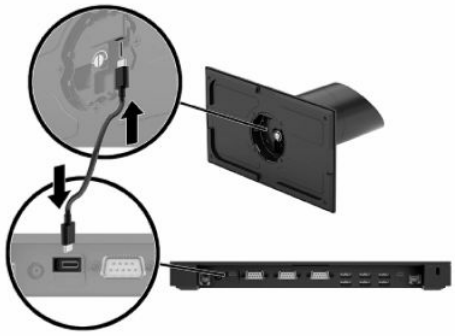
You can connect a standalone I/O connectivity base to the mobile system.

To connect a standalone I/O connectivity base:

1. Turn off the mobile system properly through the operating system, and turn off any external devices.
2. Disconnect the power cords from the mobile system and I/O connectivity base.

IMPORTANT: Regardless of the power state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord and wait approximately 30 seconds for the power to drain to avoid damage to the internal components.

3. Connect the USB Type-C power cable to the USB Type-C port on the underside of the stand's column and to the USB Type-C power port on the I/O connectivity base.



4. Connect the AC adapter to the I/O connectivity base and a grounded AC outlet. See Connecting an AC adapter to power on page 7.

Configuring the I/O connectivity base powered serial ports

You can configure the serial ports as standard (unpowered) serial ports or powered serial ports. Some devices use a powered serial port. If the serial port is configured as a powered port, devices that support a powered serial interface do not require an external power source.

IMPORTANT: The system must be turned off before connecting or disconnecting serial port devices.

NOTE: The I/O connectivity base ships with all serial ports configured in standard unpowered serial mode (0 volts) by default.

Each serial port has three voltage settings.

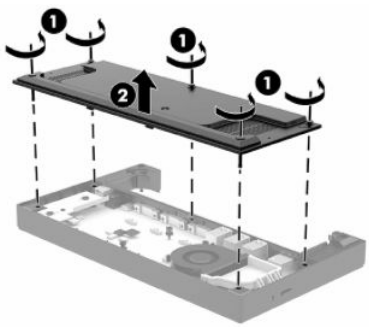
- 0 volts
- 5 volts
- 12 volts

To change the voltage settings for a powered serial port:

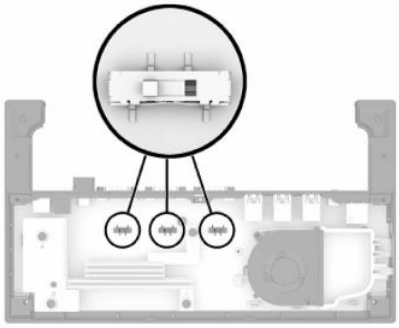
1. Turn off the mobile system properly through the operating system, and turn off any external devices.
2. Disconnect the power cord.

   NOTE: Regardless of the power state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord and wait approximately 30 seconds for the power to drain to avoid damage to the internal components of the computer.

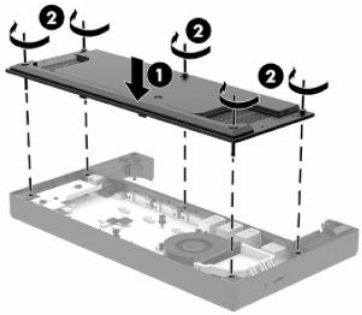
3. Remove the five screws on the underside of the I/O connectivity base **(1)** that secure the bottom plate to the I/O connectivity base, and then remove the bottom plate from the I/O connectivity base **(2)**.



4. Adjust the voltage select switch behind each serial port to the setting that you want.



5. Place the bottom plate onto the I/O connectivity base **(1)**, and then secure the plate to the I/O connectivity base with the five screws **(2)**.



6. Reconnect the I/O connectivity base power cord and peripheral devices.

Attaching an optional fingerprint reader to the I/O connectivity base

You can use the optional fingerprint reader as a standalone device, or you can attach it to the I/O connectivity base.

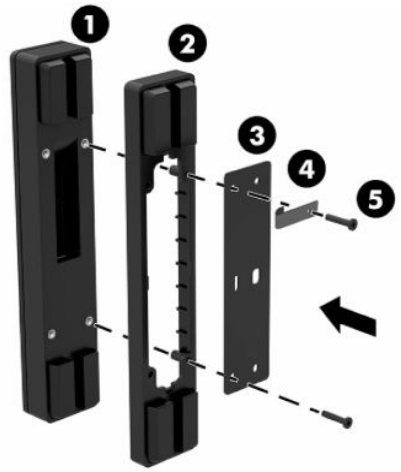
To connect an optional fingerprint reader to the I/O connectivity base.

NOTE: You can attach the fingerprint reader to either side of the I/O connectivity base, but if you attach it to the left side of the I/O connectivity base, the fingerprint reader covers the microSD slot and the headset jack on the I/O connectivity base.

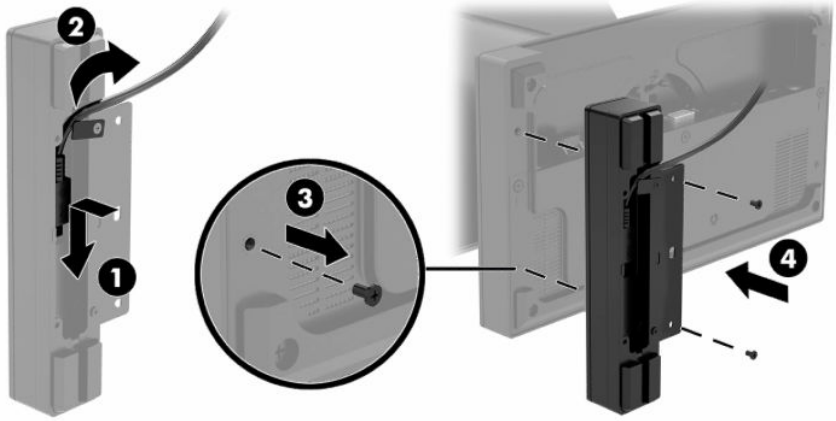
1. Turn off the mobile system properly through the operating system, and turn off any external devices.
2. Disconnect the power cords from the mobile system and I/O connectivity base.

IMPORTANT: Regardless of the power state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord and wait approximately 30 seconds for the power to drain to avoid damage to the internal components.

3. Place the fingerprint reader **(1)** on the riser **(2)**, and then attach the mounting bracket **(3)** and cable routing clip **(4)** to the fingerprint reader and riser with the two long screws **(5)** that are included with the fingerprint reader.



4. Connect the USB cable to the fingerprint reader **(1)** and route the cable under the routing clip on the fingerprint reader **(2)**. Remove the mounting screw **(3)** from the underside of the I/O connectivity base, and then attach the bracket on the fingerprint reader assembly to the underside of the I/O connectivity base **(4)** using the screw that was removed from the base and the short screw included in the kit.



5. Connect the fingerprint reader cable to a USB Type-A port on the I/O connectivity base.

6. Reconnect the I/O connectivity base and power cords.

3 Illustrated parts catalog

Use this information to determine the spare parts that are available for the computer.

NOTE: HP continually improves and changes product parts. For complete and current information about supported parts for your computer, go to http://partsurfer.hp.com, select your country or region, and then follow the on-screen instructions.

Computer major components

To identify the computer major components, use this illustration and table.

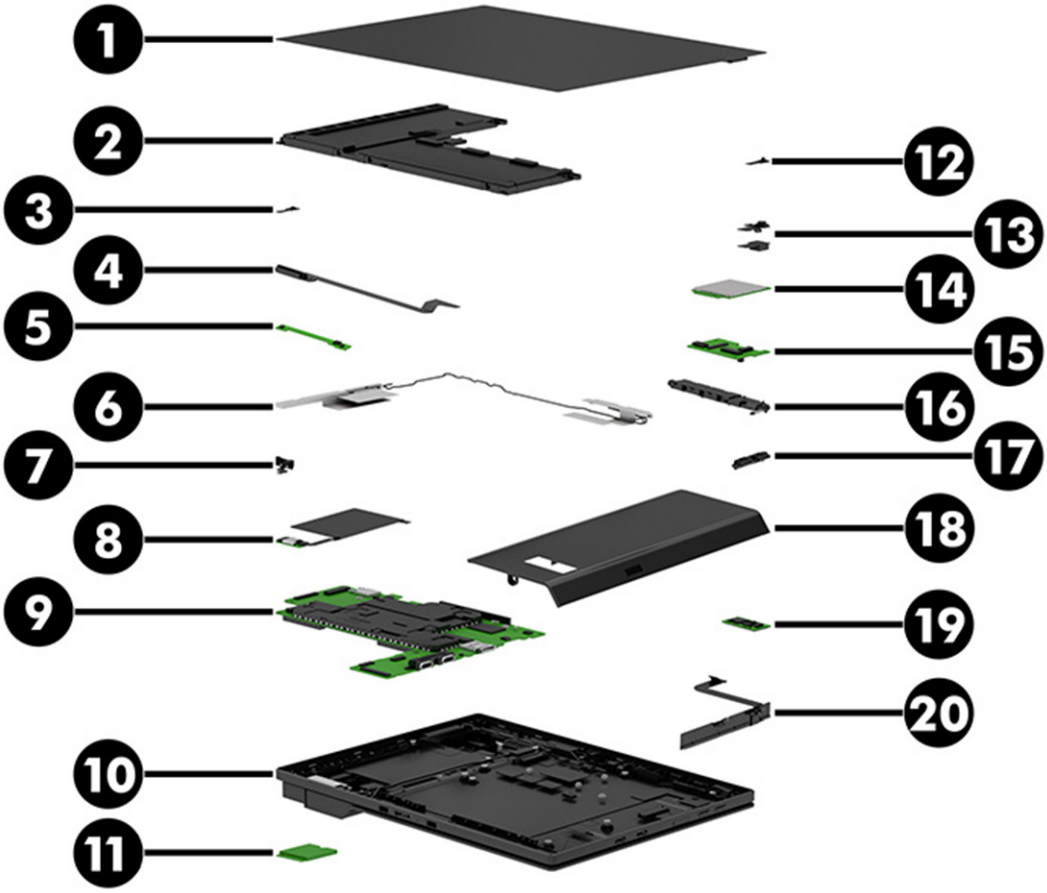


Table 3-1 Computer major components and their descriptions

Item	Description
(1)	**Display panel assembly**
(2)	**Battery** (2 cell, 42 Whr)
(3)	**Camera LED module** (includes cable)

Table 3-1 Computer major components and their descriptions (continued)

Item	Description
(4)	**Pogo connector**
(5)	**Touch board**
(6)	**Wireless antennas**
(7)	**Camera assembly** (left and right, includes cable)
(8)	**NFC module** (includes antenna)
(9)	**System board** (includes replacement thermal material) NOTE: System boards are available for computers with a non-Windows operating system, Windows IoT, and Windows
	Intel® Core® i5 processor and 16 GB of system memory
	Intel Core i5 processor and 8 GB of system memory
	Intel Core i3 processor and 8 GB of system memory
	Intel Core i3 processor and 4 GB of system memory
(10)	**Display rear cover** NOTE: Offered in black or white, for models with or without fingerprint reader, and for models with or without a pogo connector.
(11)	**Solid-state drive** (M.2 2230, PCIe)
	256 GB
(12)	**Ambient light sensor** (includes cable)
(13)	**Pogo docking connectors**
(14)	**WWAN module**
(15)	**Hub board**
(16)	**Speaker**
(17)	**Power button board**
(18)	**Bump cover**
(19)	**Volume board**
(20)	**Bump cover pogo connector**
	Fingerprint reader board (not illustrated)
	Microphone board (not illustrated)
	Side frame (not illustrated)

Optional components

To identify optional components, use this illustration and table.

Table 3-2 Optional components and their descriptions

Item	Description
(1)	**Advanced I/O connectivity base** (available with and without base cover)
(2)	**Basic I/O connectivity base** (available with and without base cover)
(3)	**Barcode scanner**
(4)	**Docking stand**
(5)	**HP Engage Go 13.5**
(6)	**Mounting device**
(7)	**Integrated payment module** (only supported in the U.S.)

Miscellaneous parts

To identify the various computer parts, use this table.

Table 3-3 Miscellaneous parts and their descriptions

Description
Screw kit
Volume button switch kit (available in black or white)
Stand column
SIM cover (available in black or white)
Plastic power button (available in black or white)
Plastic flange holder (available in black or white)
Plastic FPC holder
Plastic volume button (available in black or white)
SIM tray frame
Lens kit

Table 3-3 Miscellaneous parts and their descriptions (continued)

Description
Cables
Hub board cable
Display cable
Barcode scanner cable
Fingerprint reader cable
Volume cable
Payment device cable
Power board cable
Touch/microphone cable
USB cables
USB 3.1 Gen 1, CM 20 V/3 A, 1.8 m (6.0 ft)
USB 3.1 Gen 1, 0.43 m (16.9 in)
USB 3.1 Gen 1, 1.8 m (6.0 ft)
USB 3.1 Gen 1, CM-CM, 0.5 m (3.3 ft)
USB 3.1 Gen 1, CM-CM, 1.8 m (6.0 ft)
Power cord
C13, 1.8 m (6.0 ft)
C13, 1.0 m (3.3 ft)
C5, 1.8 m (6.0 ft)
AC adapter (7.4 mm)
200 W, power factor connecting (PFC)
180 W, PFC
120 W, slim, PFC
120 W, nonslim, PFC
65 W, nPFC
60 W, printer adapter

4 Routine care, drive guidelines, and disassembly preparation

This information provides general service information for the computer. Adherence to the procedures and precautions is essential for proper service.

IMPORTANT: When the computer is plugged into an AC power source, DC voltage is always applied to the system board. You must disconnect the power cord from the power source before opening the computer to prevent electric shock, system board, or component damage.

Electrostatic discharge information

A sudden discharge of static electricity from your finger or other conductor can destroy static-sensitive devices or microcircuitry. Often the spark is neither felt nor heard, but damage occurs.

An electronic device exposed to electrostatic discharge (ESD) might not appear to be affected at all and can work perfectly throughout a normal cycle. The device might function normally for a while, but it has been degraded in the internal layers, reducing its life expectancy.

Networks built into many integrated circuits provide some protection, but in many cases, the discharge contains enough power to alter device parameters or melt silicon junctions.

IMPORTANT: To prevent damage to the device when you are removing or installing internal components, observe these precautions:

- Keep components in their electrostatic-safe containers until you are ready to install them.
- Before touching an electronic component, discharge static electricity by using the guidelines described in this section.
- Avoid touching pins, leads, and circuitry. Handle electronic components as little as possible.
- If you remove a component, place it in an electrostatic-safe container.

Generating static electricity

This table shows how humidity affects the electrostatic voltage levels generated by different activities. A product can be degraded by 700 V of static electricity.

- Different activities generate different amounts of static electricity.
- Static electricity increases as humidity decreases.

Table 4-1 **Static electricity occurrence based on activity and humidity**

	Relative humidity		
Event	**55%**	**40%**	**10%**

Table 4-1 Static electricity occurrence based on activity and humidity (continued)

	Relative humidity		
Walking across carpet	7,500 V	15,000 V	35,000 V
Walking across vinyl floor	3,000 V	5,000 V	12,000 V
Motions of bench worker	400 V	800 V	6,000 V
Removing DIPs (dual in-line packages) from plastic tube	400 V	700 V	2,000 V
Removing DIPs from vinyl tray	2,000 V	4,000 V	11,500 V
Removing DIPs from polystyrene foam	3,500 V	5,000 V	14,500 V
Removing bubble pack from PCB (printed circuit board)	7,000 V	20,000 V	26,500 V
Packing PCBs in foam-lined box	5,000 V	11,000 V	21,000 V
Multiple electric components can be packaged in plastic tubes, trays, or polystyrene foam.			

Preventing electrostatic damage to equipment

Many electronic components are sensitive to ESD. Circuitry design and structure determine the degree of sensitivity. The following packaging and grounding precautions are necessary to prevent static electricity damage to electronic components.

- To avoid hand contact, transport products in static-safe containers such as tubes, bags, or boxes.
- Protect all electrostatic parts and assemblies with conductive or approved containers or packaging.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Place items on a grounded surface before removing them from their container.
- Always be properly grounded when touching a sensitive component or assembly.
- Avoid contact with pins, leads, or circuitry.
- Place reusable electrostatic-sensitive parts from assemblies in protective packaging or conductive foam.

Personal grounding methods and equipment

Use this equipment to prevent static electricity damage to electronic components.

- **Wrist straps** are flexible straps with a maximum of 1 MΩ ±10% resistance in the ground cords. To provide proper ground, a strap must be worn snug against bare skin. The ground cord must be connected and fit snugly into the banana plug connector on the grounding mat or workstation.
- **Heel straps/Toe straps/Boot straps** can be used at standing workstations and are compatible with most types of shoes or boots. On conductive floors or dissipative floor mats, use them on both feet with a maximum of 1 MΩ ±10% resistance between the operator and ground.

Table 4-2 Static shielding protection levels

Static shielding protection levels	
Method	Voltage

Table 4-2 **Static shielding protection levels (continued)**

Static shielding protection levels	
Antistatic plastic	1,500 V
Carbon-loaded plastic	7,500 V
Metallized laminate	15,000 V

Grounding the work area

To prevent static damage at the work area, use these precautions.

- Cover the work surface with approved static-dissipative material. Provide a wrist strap connected to the work surface and properly grounded tools and equipment.
- Use static-dissipative mats, foot straps, or air ionizers to give added protection.
- Handle electrostatic sensitive components, parts, and assemblies by the case or PCB laminate. Handle them only at static-free work areas.
- Turn off power and input signals before inserting and removing connectors or test equipment.
- Use fixtures made of static-safe materials when fixtures must directly contact dissipative surfaces.
- Keep work area free of nonconductive materials such as ordinary plastic assembly aids and polystyrene foam.
- Use field service tools, such as cutters, screwdrivers, and vacuums, that are conductive.

Recommended materials and equipment

HP recommends these materials and equipment to prevent static electricity.

- Antistatic tape
- Antistatic smocks, aprons, or sleeve protectors
- Conductive bins and other assembly or soldering aids
- Conductive foam
- Conductive tabletop workstations with ground cord of 1 MΩ ±10% resistance
- Static-dissipative table or floor mats with hard tie to ground
- Field service kits
- Static awareness labels
- Wrist straps and footwear straps providing 1 MΩ ±10% resistance
- Material handling packages
- Conductive plastic bags
- Conductive plastic tubes
- Conductive tote boxes

- Opaque shielding bags
- Transparent metallized shielding bags
- Transparent shielding tubes

Operating guidelines

This information details how to prevent overheating and to help prolong the life of the computer.

- Keep the computer away from excessive moisture, direct sunlight, and extremes of heat and cold.
- Operate the computer on a sturdy, level surface. Leave a 10.2 cm (4 inch) clearance on all vented sides of the computer and above the monitor to permit the required airflow.
- Never restrict the airflow into the computer by blocking any vents or air intakes. Do not place the keyboard, with the keyboard feet down, directly against the front of the desktop unit as this also restricts airflow.
- Occasionally clean the air vents on all vented sides of the computer. Lint, dust, and other foreign matter can block the vents and limit the airflow. Be sure to unplug the computer before cleaning the air vents.
- Never operate the computer with the cover or side panel removed.
- Do not stack computers on top of each other or place computers so near each other that they are subject to each other's recirculated or preheated air.
- If the computer is to be operated within a separate enclosure, intake and exhaust ventilation must be provided on the enclosure, and the same operating guidelines listed previously still apply.
- Keep liquids away from the computer and keyboard.
- Never cover the ventilation slots on the monitor with any type of material.
- Install or enable power management functions of the operating system or other software, including Sleep states.

Routine care

Use this information to properly care for your computer.

General cleaning safety precautions

Use this information to safely clean your computer.

⚠ CAUTION: To prevent electric shock or damage to components, never clean a product while it is turned on or plugged in.

- Never use solvents or flammable solutions to clean the computer.
- Never immerse any parts in water or cleaning solutions; apply any liquids to a clean cloth and then use the cloth on the component.
- Always unplug the computer when cleaning with liquids or damp cloths.
- Always unplug the computer before cleaning the keyboard, mouse, or air vents.

- Disconnect the keyboard before cleaning it.
- Wear safety glasses equipped with side shields when cleaning the keyboard.

Cleaning the HP Engage Go 13.5" case

Follow all safety precautions before cleaning the computer case.

To clean the computer case, follow these procedures:

- To remove light stains or dirt, use plain water with a clean, lint-free cloth or swab.
- For stronger stains, use a mild dishwashing liquid diluted with water. Rinse well by wiping it with a cloth or swab dampened with clear water.
- For stubborn stains, use isopropyl (rubbing) alcohol. No rinsing is needed because the alcohol evaporates quickly and does not leave a residue.
- After cleaning, always wipe the unit with a clean, lint-free cloth.
- Occasionally clean the air vents on the computer. Lint and other foreign matter can block the vents and limit the airflow.

Cleaning the keyboard

Use this information to properly clean the keyboard. Follow all safety precautions before cleaning the keyboard.

To clean the tops of the keys or the keyboard body, follow the procedures described in {Xref Error! Target does not exist.}Cleaning the computer case.

When cleaning debris from under the keys, review all rules in General cleaning safety precautions on page 26 before following these procedures.

⚠ **CAUTION:** Use safety glasses equipped with side shields before attempting to clean debris from under the keys.

- You can remove visible debris underneath or between the keys by vacuuming or shaking.
- You can use canned, pressurized air to clean debris from under the keys. Use caution because too much air pressure can dislodge lubricants applied under the wide keys.
- If you remove a key, use a specially designed key puller to prevent damage to the keys. This tool is available through many electronic supply outlets.

IMPORTANT: Never remove a wide leveled key (like the space bar) from the keyboard. If these keys are improperly removed or installed, the keyboard might not function properly.

- You can clean under a key with a swab moistened with isopropyl alcohol and squeezed out. Be careful not to wipe away lubricants necessary for proper key functions. Use tweezers to remove any fibers or dirt in confined areas. Allow the parts to air dry before reassembly.

Cleaning the monitor

Follow all safety precautions before cleaning dirt and debris from your computer. Use this information to properly clean the monitor.

- Wipe the monitor screen with a clean cloth moistened with water or with a towelette designed for cleaning monitors. Do not use sprays or aerosols directly on the screen; the liquid can seep into the housing and damage a component. Never use solvents or flammable liquids on the monitor.
- To clean the monitor body, follow the procedures in {Xref Error! Target does not exist.}Cleaning the computer case.

Cleaning the mouse

Follow all safety precautions before cleaning dirt and debris from your computer. Use this information to properly clean the mouse.

- Clean the mouse ball by first removing the retaining plate and the ball from the housing. Pull out any debris from the ball socket and wipe the ball with a clean, dry cloth before reassembly.
- To clean the mouse body, follow the procedures in {Xref Error! Target does not exist.}Cleaning the computer case.

Service considerations

Keep these considerations in mind during the disassembly and assembly of the computer.

Tools and software requirements

Servicing the computer requires these tools.

- Torx T-15 screwdriver
- Flat-bladed screwdriver (can sometimes be used in place of the Torx screwdriver)
- Phillips P1 screwdriver
- Nonconductive, nonmarking pry tool
- Diagnostics software

Screws

The screws used in the computer are not interchangeable. They could have standard or metric threads and might be of different lengths.

If you use an incorrect screw during the reassembly process, it can damage the unit. HP strongly recommends that you keep all screws that you remove during disassembly with the removed part and then return them to their proper locations.

IMPORTANT: As you remove each subassembly from the computer, place it away from the work area to prevent damage.

Cables and connectors

Use this information to properly handle cables.

Apply only the tension required to seat or unseat the cables during insertion or removal from the connector. Handle cables by the connector whenever possible. In all cases, avoid bending or twisting

the cables, and route the cables so that they cannot be caught or snagged by parts being removed or replaced.

IMPORTANT: When servicing this computer, be sure to place cables in their proper location during the reassembly process. Improper cable placement can damage the computer.

Hard drives

Handle hard drives as delicate, precision components, and avoid all physical shock and vibration. This advice applies to failed drives as well as replacement spares.

- If a drive must be mailed, place the drive in a bubble-pack mailer or other suitable protective packaging and label the package “Fragile: Handle With Care.”
- Do not remove hard drives from the shipping package for storage. Keep hard drives in their protective packaging until they are actually mounted in the computer.
- Avoid dropping drives from any height onto any surface.
- If you are inserting or removing a hard drive, turn off the computer. Do not remove a hard drive while the computer is on or in standby mode.
- Before handling a drive, ensure that you are discharged of static electricity. While handling a drive, avoid touching the connector.
- Do not use excessive force when inserting a drive.
- Avoid exposing a hard drive to liquids, temperature extremes, or products that have magnetic fields such as monitors or speakers.

Lithium coin cell battery

The battery that comes with the computer provides power to the real-time clock and has a minimum lifetime of approximately three years.

See the removal and replacement chapter for replacement instructions.

WARNING! This computer contains a lithium battery. There is a risk of fire and chemical burn if the battery is handled improperly. Do not disassemble, crush, puncture, short external contacts, dispose of in water or fire, or expose it to temperatures higher than 140°F (60°C). Do not attempt to recharge the battery.

NOTE: Do not dispose of batteries, battery packs, and accumulators with general household waste. To forward them to recycling centers or proper disposal, use the public collection system or return them to HP, their authorized partners, or their agents.

SATA hard drives

The Self Monitoring Analysis and Recording Technology (SMART) ATA drives for the HP Personal Computers have built-in drive failure prediction that warns the user or network administrator of an impending failure or crash of the hard drive.

The SMART drive tracks fault prediction and failure indication parameters such as reallocated sector count, spin retry count, and calibration retry count. If the drive determines that a failure is imminent, it generates a fault alert.

Table 4-3 SATA hard drive characteristics

Serial ATA hard drive characteristics	
Number of pins/conductors in data cable	7/7
Number of pins in power cable	15
Maximum data cable length	100 cm (39.37 in)
Data interface voltage differential	400 mV–700 mV
Drive voltages	3.3 V, 5 V, 12 V
Jumpers for configuring drive	N/A
Data transfer rate	6.0 Gbps

Always use an HP-approved SATA 6.0 Gbps cable because it is fully backwards compatible with the SATA 1.5 Gbps drives. Current HP desktop products ship with SATA 6.0 Gbps hard drives.

SATA data cables are susceptible to damage if overflexed. Never crease a SATA data cable and never bend it tighter than a 30 mm (1.18 in) radius.

The SATA data cable is a thin, seven-pin cable designed to transmit data for only a single drive.

Cable management

Always follow good cable management practices when working inside the computer.

- Keep cables away from major heat sources like the heat sink.
- Keep cables clear of sliding or moveable parts to prevent them from being cut or crimped when the parts are moved.
- When folding a flat ribbon cable, never fold to a sharp crease. Sharp creases can damage the wires.
- Do not bend any cable sharply. A sharp bend can break the internal wires.
- Never bend a SATA data cable tighter than a 30 mm (1.18 in) radius.
- Never crease a SATA data cable.

5 Removal and replacement procedures

Adherence to these procedures and precautions is essential for proper service. After completing all necessary removal and replacement procedures, run the Diagnostics utility to verify that all components operate properly.

NOTE: Not all features listed in this guide are available on all computers.

NOTE: HP continually improves and changes product parts. For complete and current information about supported parts for your computer, go to https://partsurfer.hp.com/partsurfer/, select your country or region, and then follow the on-screen instructions.

Preparation for disassembly

Use this information to properly prepare to disassemble and reassemble the computer.

See Routine care, drive guidelines, and disassembly preparation on page 23 for initial safety procedures.

1. Turn off the computer. If you are unsure whether the computer is off or in Hibernation, turn the computer on, and then shut it down through the operating system.

   IMPORTANT: Turn off the computer before disconnecting any cables.

   Regardless of the power state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. In some systems, the cooling fan is on even when the computer is in the Standby or Suspend modes. Always disconnect the power cord before servicing a unit.

2. Disconnect the power from the computer by unplugging the power cord from the computer.
3. Disconnect all external devices from the computer

CAUTION: Beware of sharp edges inside the chassis.

NOTE: During disassembly, label each cable as you remove it, and note its position and routing. Keep all screws with the removed components.

Display assembly

To remove the display assembly, use these procedures and illustrations.

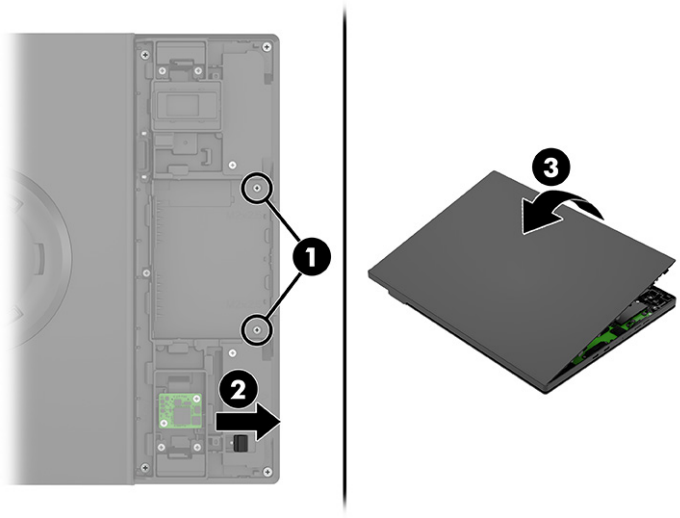
Before removing the display assembly, follow these steps:

- Prepare the computer for disassembly (see Preparation for disassembly on page 31).

Remove the display assembly:

1. Remove the two Phillips screws **(1)** that secure the display to the computer.

2. Slide the release switch **(2)**, and then lift the display panel and place it next to the computer **(3)**.

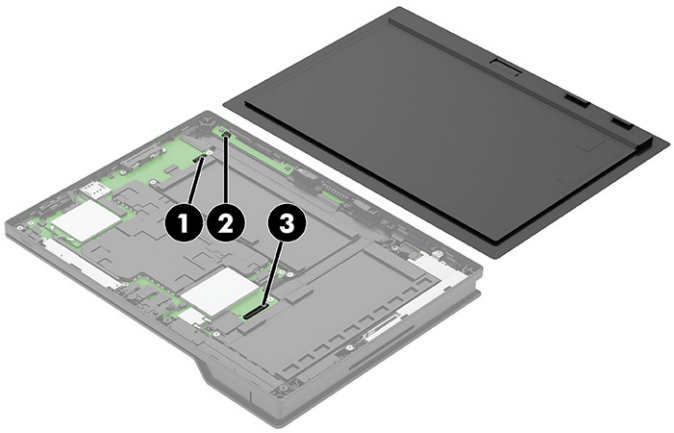


3. Disconnect the battery cable from the system board (see Battery on page 32).
4. Disconnect the following display cables:

   (1) Touch cable from the touch board reverse ZIF connector.

   (2) Touch cable from the system board reverse ZIF connector.

   (3) Display cable from the system board.



To install the display assembly, reverse the removal procedure.

Battery

To remove the battery, use this procedure and illustration.

⚠ **WARNING!** To avoid personal injury and damage to the product:

- Do *not* puncture, twist, or crack the battery.

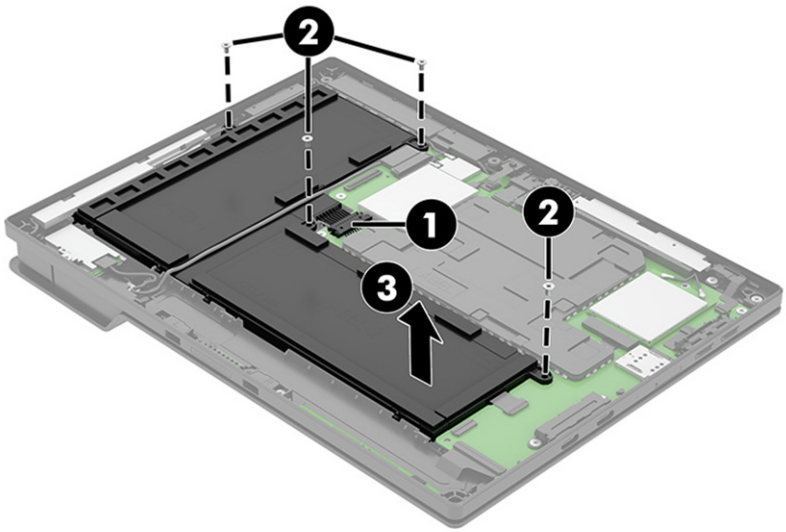
- Do *not* cause an external puncture or rupture to the battery. They can cause a short inside the battery, which can result in battery thermal runaway.
- Do *not* handle or touch the battery enclosure with sharp objects such as tweezers or pliers, which might puncture the battery.
- Do *not* compress or squeeze the battery case with tools or heavy objects stacked on top of the case. These actions can apply undue force on the battery.
- Do *not* touch the connectors with any metallic surface or object, such as metal tools, screws, or coins, which can cause shorting across the connectors.

Before removing the battery, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).

Remove the battery:

1. Disconnect the battery cable from the system board **(1)**.
2. Remove the four Phillips screws from the battery **(2)**.
3. Remove the battery from the computer **(3)**.



To install the battery, reverse the removal procedure.

Solid-state drive

To remove the solid-state drive, use this procedure and illustration.

For a list of available solid-states drives, see Computer major components on page 19.

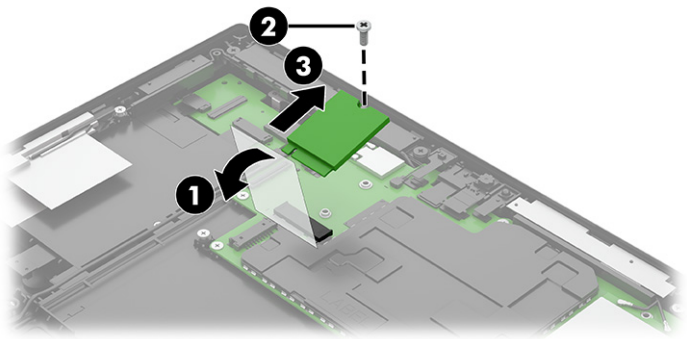
Before removing the solid-state drive, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).

3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the solid-state drive:

1. Use the tab to pull the plastic cover off the top of the drive **(1)**.
2. Remove the screw that secures the drive **(2)**.
3. Pull the drive out of the socket **(3)**.



To install the solid-state drive, reverse the removal procedure.

Touch board

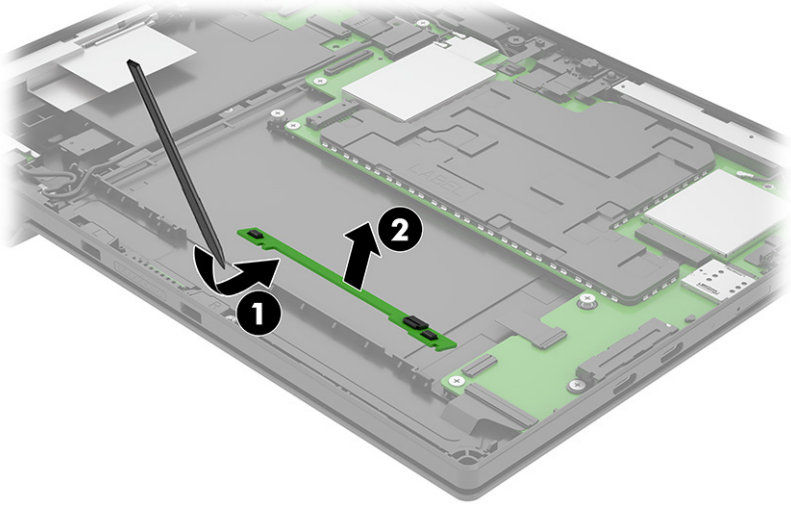
To remove the touch board, use this procedure and illustration.

Before removing the touch board, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the touch board:

- Use a flat tool **(1)** to release the board out from the computer **(2)**. The board is secured with adhesive.



To install the touch board, reverse the removal procedure.

Hub board

To remove the hub board, use this procedure and illustration.

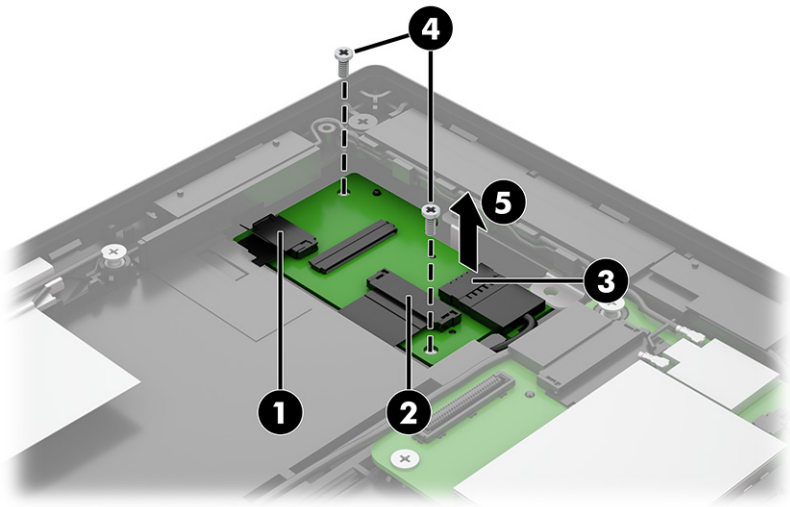
Before removing the hub board, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the hub board:

1. Disconnect the cable from the ZIF connector on the left side of the board **(1)**.
2. Disconnect the cable from the reverse ZIF connector on the right side of the board **(2)**.
3. Disconnect the lower cable, located under the top cable, on the right side of the board **(3)**.
4. Remove the two Phillips screws from the board **(4)**.

5. Remove the board from the computer **(5)**.



To install the hub board, reverse the removal procedure.

Speaker

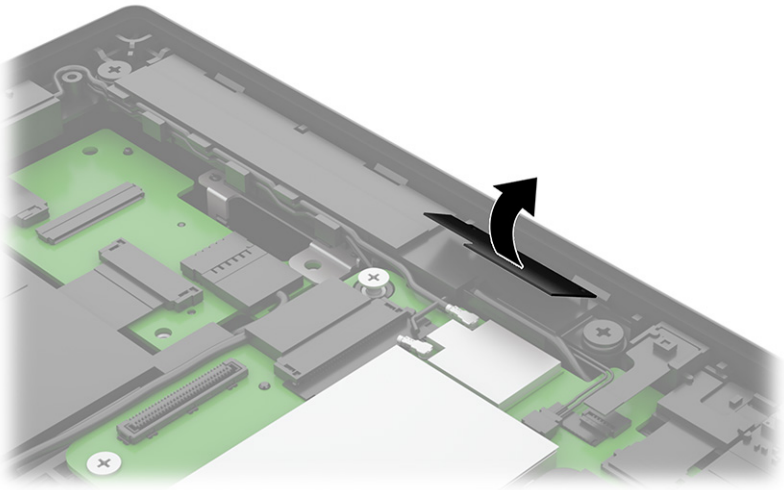
To remove the speaker, use this procedure and illustration.

Before removing the speaker, follow these steps:

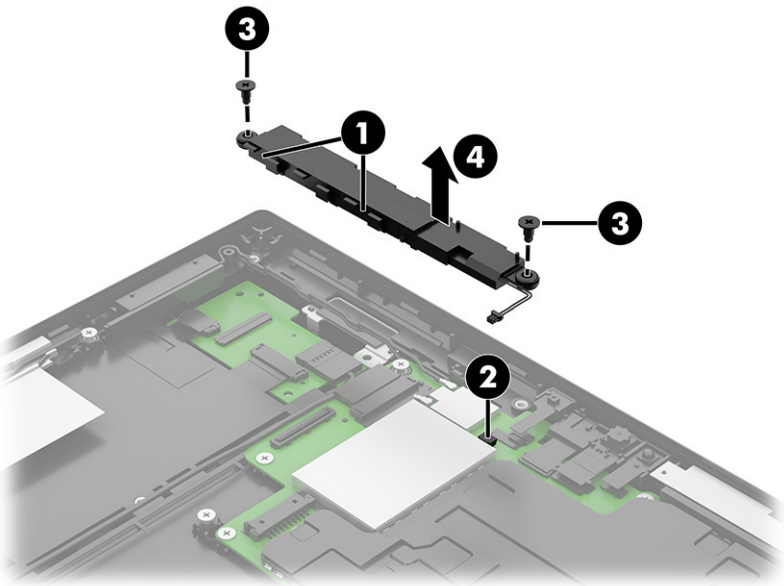
1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the speaker:

1. Rotate the top WLAN antenna up.



2. Remove the antenna cable from the clips on the bottom of the speaker **(1)**.
3. Disconnect the speaker cable from the system board **(2)**.
4. Remove the two Phillips screws from the speaker **(3)**.
5. Remove the speaker from the computer **(4)**.



To install the speaker, reverse the removal procedure.

Volume board and buttons

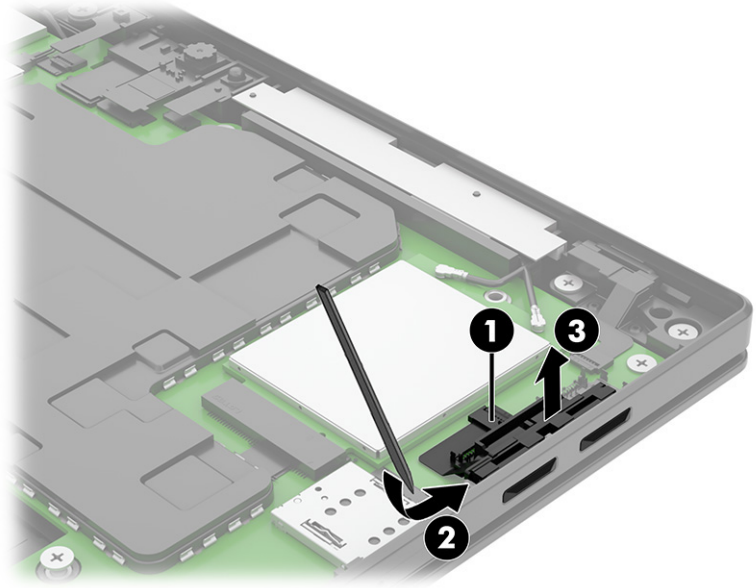
To remove the volume board and buttons, use this procedure and illustration.

Before removing the volume board and buttons, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the volume board and buttons:

1. Disconnect the cable from the reverse ZIF connector on the system board **(1)**.
2. Use a flat tool to release and remove the board from between the side of the computer and the system board **(2)**.
3. Use tweezers to grasp and lift the power buttons out of the computer **(3)**.



To install the volume board and buttons, reverse the removal procedure.

WWAN module

To remove the WWAN module, use this procedure and illustration.

IMPORTANT: To prevent an unresponsive system, replace the wireless module only with a wireless module authorized for use in the computer by the governmental agency that regulates wireless devices in your country or region. If you replace the module and then receive a warning message, remove the module to restore device functionality, and then contact technical support.

Before removing the WWAN module, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

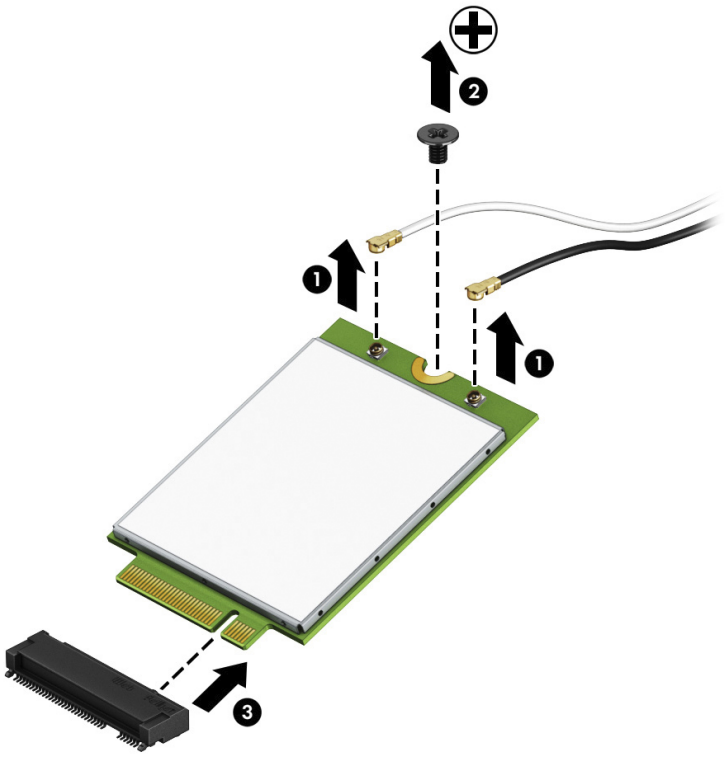
Remove the WWAN module:

1. Disconnect the WWAN antenna cables **(1)** from the terminals on the WWAN module.

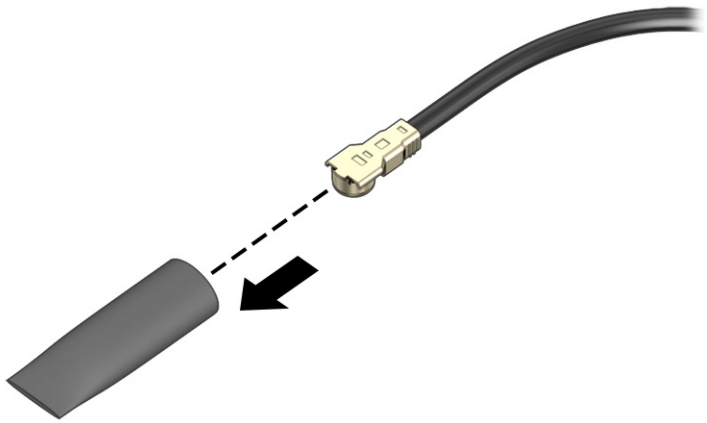
2. Remove the Phillips M2.0 × 2.0 screw **(2)** that secures the WWAN module to the bottom cover. (The WWAN module tilts up.)

3. Remove the WWAN module **(3)** by pulling the module away from the slot at an angle.

NOTE: Models have either one or two WLAN antennas. On models with two antennas, the #1 white WLAN antenna cable connects to the WLAN module #1 Main terminal. The #2 black WLAN antenna cable connects to the WLAN module #1 Aux terminal.



4. If the WWAN antenna is not connected to the terminal on the WWAN module, a protective sleeve must be installed on the antenna connector, as shown in the following illustration.



To install the WWAN module, reverse this procedure.

Ambient light sensor (ALS)

To remove the ambient light sensor, use this procedure and illustration.

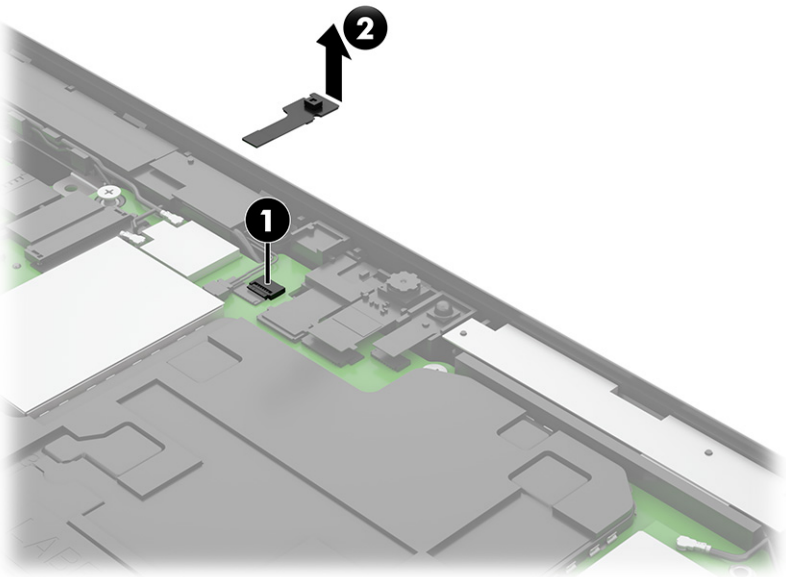
Before removing the ambient light sensor, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the ambient light sensor:

1. Use tweezers to disconnect the cable from the reverse ZIF connector on the system board **(1)**.

2. Use tweezers to lift the sensor out of the computer **(2)**. The sensor is secured with adhesive.



To install the ambient light sensor, reverse the removal procedure.

Cameras

To remove the cameras, use this procedure and illustration.

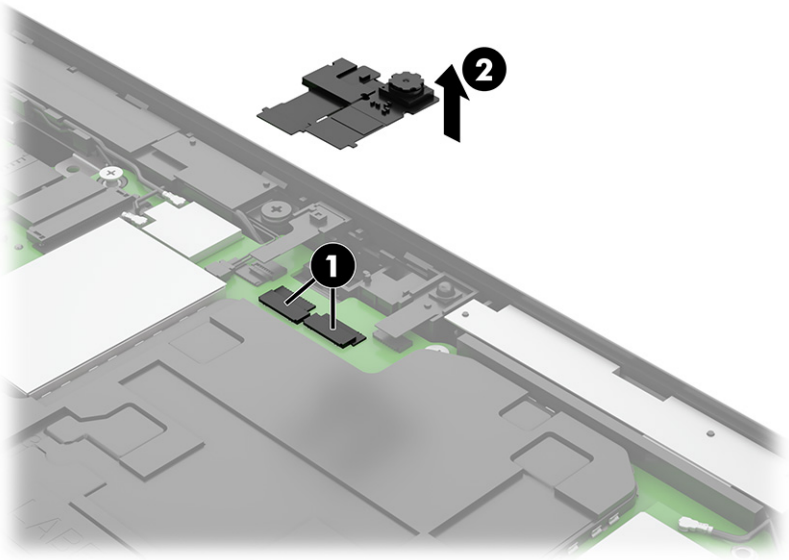
Before removing the cameras, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the cameras:

1. Use tweezers to disconnect the camera cables from the reverse ZIF connectors on the system board **(1)**.

2. Use tweezers to lift the cameras out of the computer **(2)**. The cameras are secured with adhesive.



To install the cameras, reverse the removal procedure.

Camera LED module

To remove the camera LED module, use this procedure and illustration.

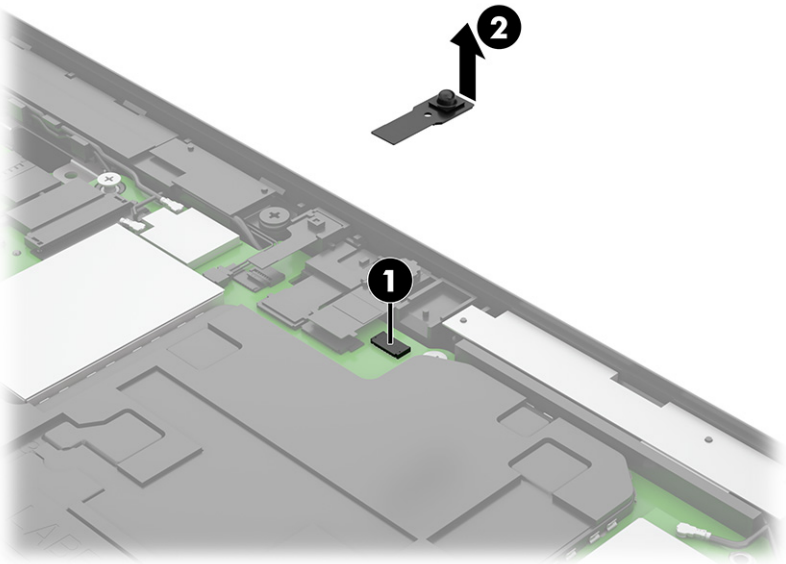
Before removing the camera LED module, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the camera LED module:

1. Use tweezers to disconnect the camera LED module from the reverse ZIF connector on the system board **(1)**.

2. Use tweezers to lift the module out of the computer **(2)**. The module is secured with adhesive.



To install the camera LED module, reverse the removal procedure.

Rear camera

To remove the rear camera, use this procedure and illustration.

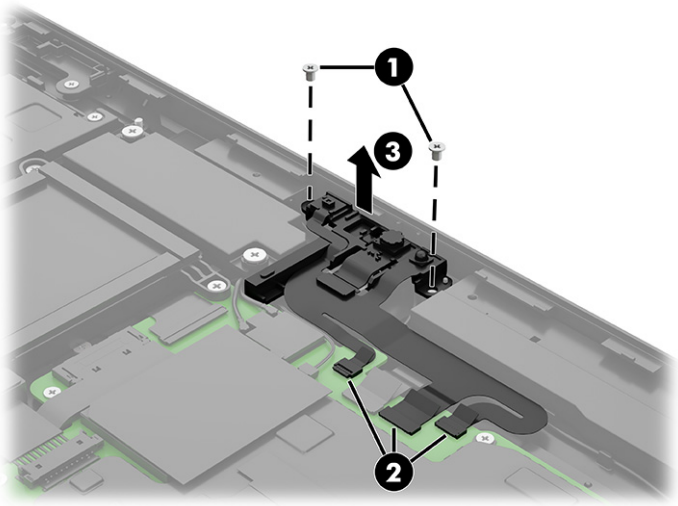
Before removing the rear camera, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

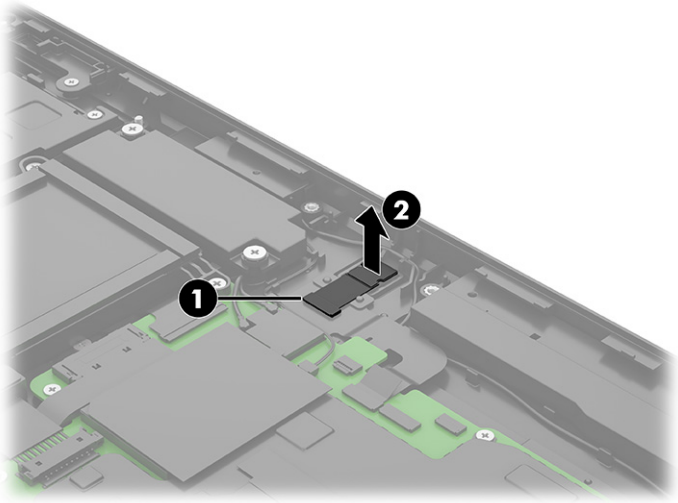
Remove the rear camera:

1. Remove the two Phillips screws **(1)** that secure the camera holder.
2. Disconnect the cables from the system board **(2)**.

3. Remove the camera holder **(3)**.



4. Disconnect the camera cable from the system board **(1)**, and then remove the camera from the computer **(2)**.



To install the rear camera, reverse the removal procedure.

Pogo connector

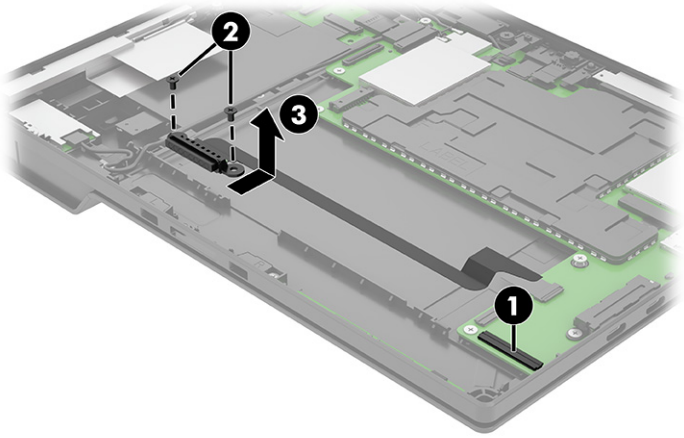
To remove the pogo connector, use this procedure and illustration.

Before removing the pogo connector, follow these steps:

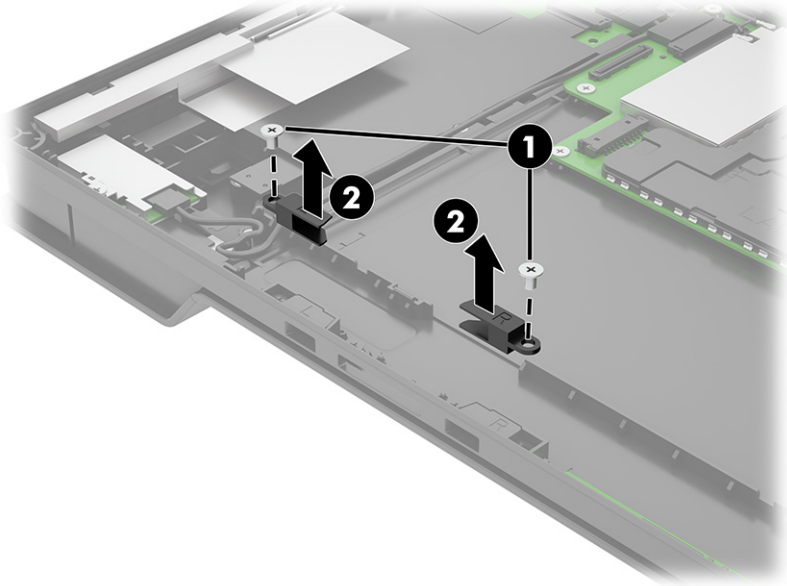
1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the pogo connector:

1. Disconnect the cable from the reverse ZIF connector on the system board **(1)**.
2. Remove the two Phillips screws **(2)** from the connector.
3. Pull the pogo connector into the computer slightly, and then remove it from the computer **(3)**.



4. If you need to remove the pogo docking connectors, remove the Phillips screw **(1)** from each holder, and then remove the holders from the computer **(2)**.



To install the pogo connector and docking connectors, reverse the removal procedures.

Power button board

To remove the power button board, use this procedure and illustration.

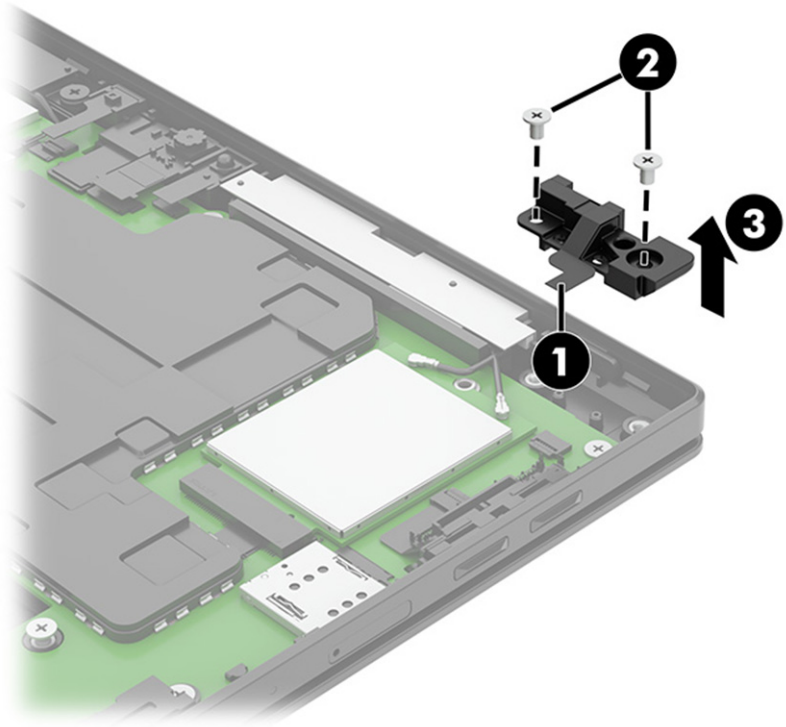
Before removing the power button board, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).

3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the power button board:

1. Disconnect the cable from the reverse ZIF connector on the system board **(1)**.
2. Remove the two Phillips screws **(2)** from the board.
3. Remove the board from the computer **(3)**.



To install the power button board, reverse the removal procedure.

System board

To remove the system board, use this procedure and illustration.

NOTE: All system board spare part kits include replacement thermal material.

Before removing the system board, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Remove the battery (see Battery on page 32).
4. Remove the solid-state drive (see Solid-state drive on page 33).
5. Remove the WWAN module (see WWAN module on page 38).

Remove the system board:

1. Disconnect the following cables from the system board:

   (1) Daughter board cable

   (2) Fingerprint reader cable

   (3) WLAN antennas cables

   (4) Ambient light sensor cable

   (5) Rear camera cable

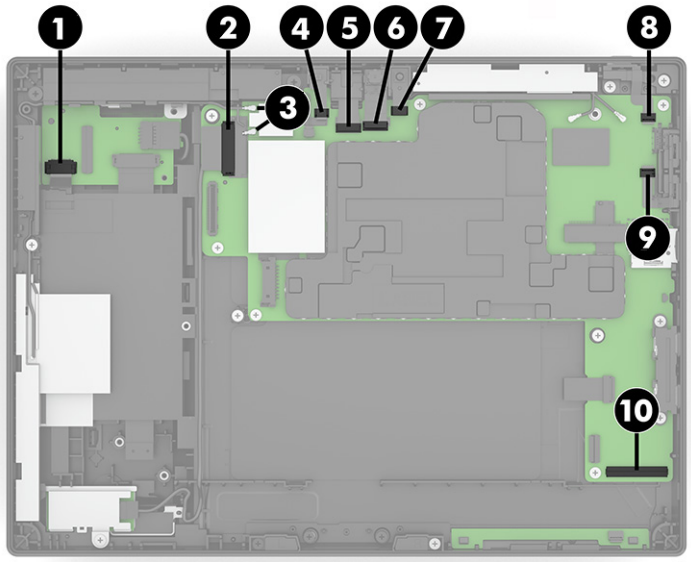
   (6) Front camera cable

   (7) Camera LED cable

   (8) Power button board cable

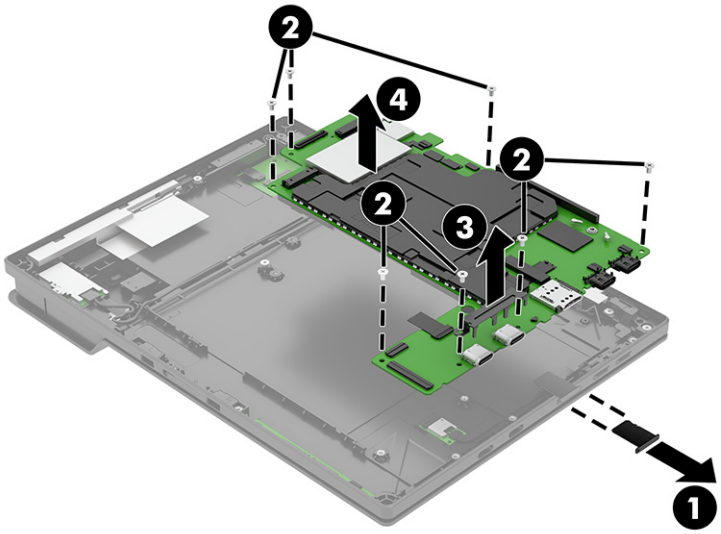
   (9) Volume board cable

   (10) Pogo connector cable



2. Remove the card reader insert **(1)**.
3. Remove the seven Phillips screws from the board **(2)**.
4. Remove the USB bracket from the board **(3)**.

5. Lift the system board up slightly, and then pull the board away from the USB ports and out of the computer **(4)**.



To install the system board, reverse the removal procedure.

NOTE: When replacing the system board, you must change the chassis serial number in the BIOS.

When replacing the system board, you must reprogram the SMBIOS information about the affected computer. Failure to reprogram the board will result in eventual failure, such as an activation failure (when you would have to reactivate the computer) or a system recovery failure.

Update the SMBIOS information in Computer Setup.

WLAN antennas

To remove the WLAN antennas, use this procedure and illustration.

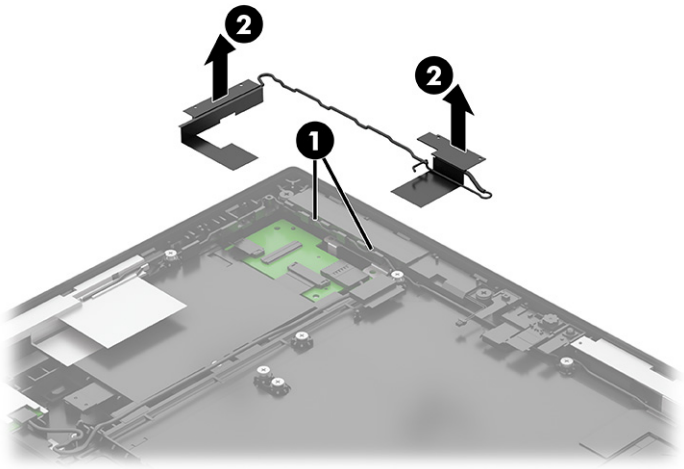
Before removing the WLAN antennas, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).
4. Remove the system board (see System board on page 46).

Remove the WLAN antennas:

1. Remove the antenna cables from the clips along the bottom of the speaker **(1)**.

2. Peel the antennas off the computer **(2)**. The right antenna is secured to the speaker.



To install the WLAN antennas, reverse the removal procedure.

NFC module

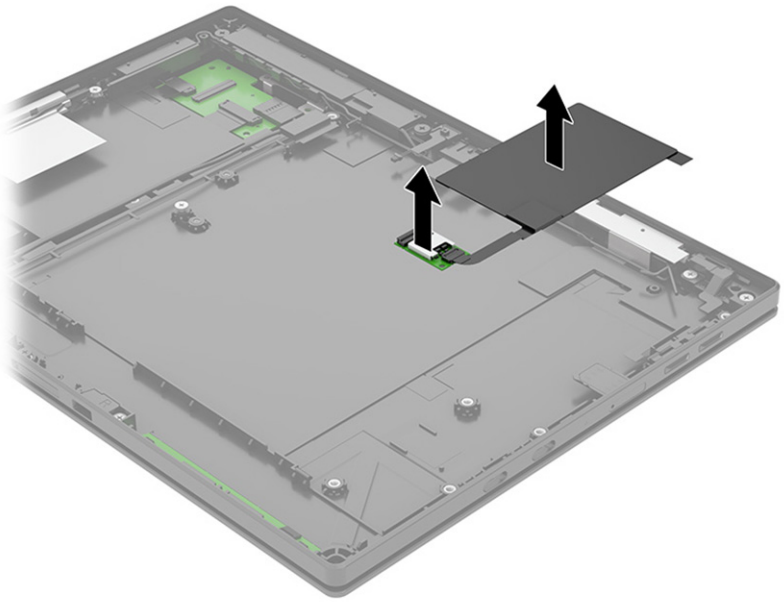
To remove the NFC module, use this procedure and illustration.

Before removing the NFC module, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Remove the battery (see Battery on page 32).
4. Remove the WWAN module (see WWAN module on page 38).
5. Remove the system board (see System board on page 46).

Remove the NFC module:

- Peel the NFC module, cable, and antenna off the inside of the computer. These components are secured with adhesive.



To install the NFC module, reverse the removal procedure.

Bump cover and pogo connector

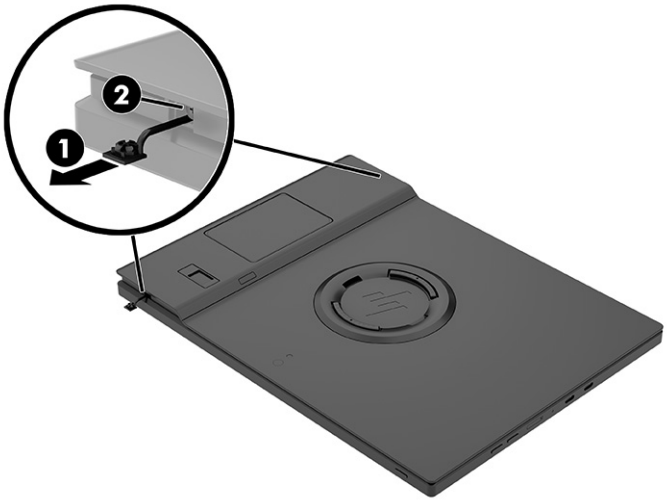
To remove the bump cover and pogo connector, use this procedure and illustration.

Before removing the bump cover and pogo connector, follow these steps:

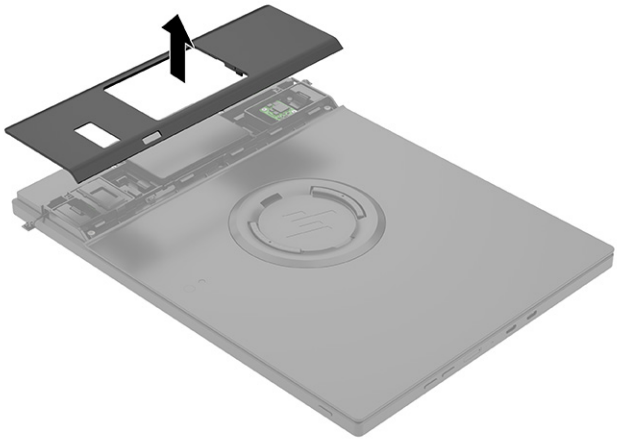
1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the bump cover:

1. Remove the captive barcode scanner sides covers **(1)**, and then loosen the two captive Phillips screws from under the covers **(2)**.

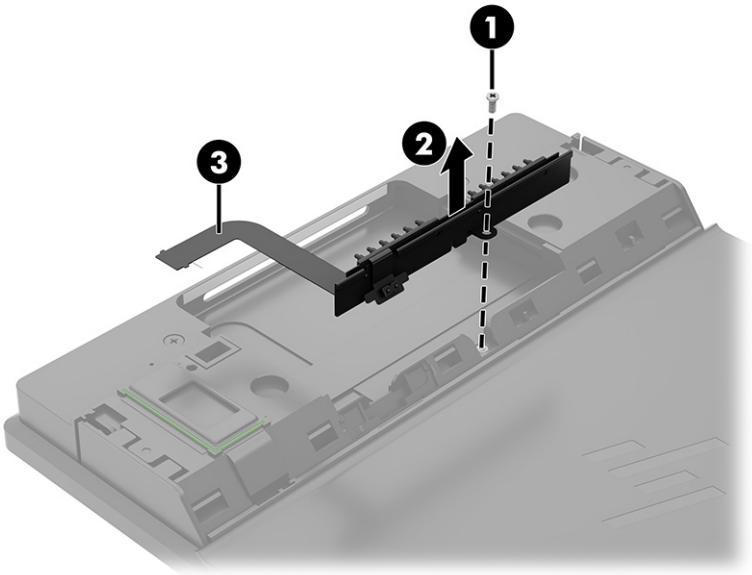


2. Use a tool to lift and release the edges of the bump cover, and the lift the cover straight up to remove it.



3. Remove the Phillips screw that secures the connector **(1)**.
4. Peel the cable off the computer **(2)**.

5. Pull the cable through the hole in the computer to remove it **(3)**.



To install the bump cover and pogo connector, reverse the removal procedure.

Fingerprint reader

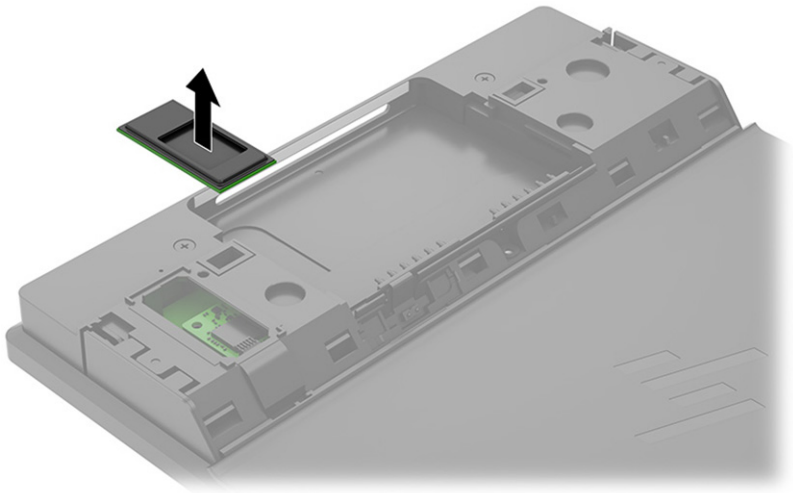
To remove the fingerprint reader, use this procedure and illustration.

Before removing the fingerprint reader, follow these steps:

1. Prepare the computer for disassembly (see Preparation for disassembly on page 31).
2. Remove the display assembly (see Display assembly on page 31).
3. Disconnect the battery cable from the system board (see Battery on page 32).

Remove the fingerprint reader:

- From the inside, push up on the fingerprint reader to remove it. The reader is secured with adhesive.



To install the fingerprint reader, reverse the removal procedure.

6 Computer Setup (F10) Utility

This information provides details of the Computer Setup Utility.

- Change settings from the defaults or restore the settings to default values.
- View the system configuration, including settings for processor, graphics, memory, audio, storage, communications, and input devices.
- Modify the boot order of bootable devices such as hard drives or USB flash media devices.
- Enter the Asset Tag or property identification number assigned by the company to this computer.
- Enable the power-on password prompt during system restarts (warm boots) as well as during startup.
- Establish an administrator password that controls access to the Computer Setup (F10) Utility and the settings described in this section.
- Establish minimum requirements for valid passwords, including length and required types of characters.
- Secure integrated I/O functionality, including the serial, USB, or audio, or embedded NIC, so that they cannot be used until they are unsecured.
- Enable or disable different types of boot sources.
- Configure features such as Secure Boot, power management, virtualization support, and language and keyboard type used in Setup and POST.
- Replicate the system setup by saving system configuration information about a USB device and restoring it on one or more computers.
- Enable or disable DriveLock security or securely erase a hard drive.

Using Computer Setup (F10) Utilities

You can access Computer Setup only by turning the computer on or restarting the system.

To access the Computer Setup Utilities menu, complete these steps:

1. Turn on or restart the computer.
2. Repeatedly press f10 when the power button light turns white to access the utility.

   You can also press esc to see a menu that allows you to access different options available at startup, including the Computer Setup utility.

   A choice of four headings appears in the Computer Setup Utilities menu: Main, Security, Advanced, and UEFI Drivers.

NOTE: If you do not press f10 at the appropriate time, you must restart the computer and again repeatedly press f10 when the power button light turns white to access the utility.

NOTE: Selecting UEFI Drivers restarts the computer into the third-party option ROM management application. You can access this application directly by pressing f3 during startup.

3. Use the arrow (left and right) keys to select the appropriate heading. Use the arrow (up and down) keys to select the option you want, and then press enter. To return to the Computer Setup Utilities menu, press esc.

4. To apply and save changes, select **Main** > **Save Changes and Exit**.

   - If you have made changes that you do not want applied, select **Ignore Changes and Exit**.
   - To restore settings from the Advanced and Main menus to original values, select **Apply Factory Defaults and Exit**.
   - To restore settings from the Advanced and Main menus to those previously saved by **Save Custom Defaults**, select **Apply Custom Defaults and Exit**. If no custom defaults have been saved, factory defaults are used.

NOTE: You cannot modify settings in the Security menu by selecting **Apply Defaults**. You reset those values by selecting **Restore Security Settings to Factory Defaults** at the bottom of the **Security** menu.

NOTE: Not all settings shown in the following sections are available for all models.

IMPORTANT: Do not turn computer power off while the BIOS is saving the Computer Setup (F10) changes because the settings could become corrupted. It is safe to turn off the computer only after exiting the F10 Setup screen.

Computer Setup Main

This table provides information about the Computer Setup Main menu.

NOTE: Support for specific Computer Setup options can vary, depending on the hardware configuration.

Table 6-1 Computer Setup Main

Option	Description
System Information	Lists all information in following list if **Advanced System Information** is selected. Lists smaller subset if **Basic System Information** is selected. • Product name • Installed memory size • Processor type • Processor cache size (L1/L2/L3) • Processor speed • MicroCode revision • Processor stepping • Memory speed • DIMM size (for each installed module) • System BIOS version • ME Firmware version (Intel only) • Video BIOS version • Reference code revision • Super I/O firmware version • USB Type-C® controller firmware version • Born on date • Serial number • SKU number • UUID (Universally Unique Identifier) • Asset tracking number • Feature byte • Build ID • Product family • System board ID • System board CT number • Panel type • Panel serial number • Integrated MAC Address

Table 6-1 Computer Setup Main (continued)

Option	Description
System Diagnostics	If the hard drive has the HP Advanced Diagnostics installed, the application launches. If HP Advanced Diagnostics is not installed, a basic version that is built into the BIOS provides the capability to perform the following functions: • Memory Test • Hard Drive Check • Language
BIOS Event Log	**View BIOS Event Log** Displays a list of events, alerts, or warnings that have been logged since the log was last cleared. **Export to USB Key** Saves a file named BiosEventLog.txt containing the log entries to an inserted USB storage device. **Clear BIOS Event Log on Next Boot** When selected, the BIOS clears the event log when the user saves and exits. Default is disabled.

Table 6-1 Computer Setup Main (continued)

Option	Description
Update System BIOS	Lets you update the system BIOS from www.hp.com or another network server, from a removable USB drive, or from a file located on the hard drive. **Check [current selection] for BIOS Updates** The string that appears here depends on the setting in **BIOS Update Preferences**. **Lock BIOS Version** If this option is selected, the system is locked to the current BIOS version, and updates are not allowed. **Native OS Firmware Update Service** Allows the operating system to drive firmware updates (for example, Windows Update). **BIOS Rollback Policy** • Unrestricted Rollback to older BIOS: Lets you roll back to any previous version of BIOS. • Restricted Rollback to older BIOS: If selected, **Minimum BIOS Version** becomes active, which lets you manually enter the minimum BIOS version that you can roll back to. **Minimum BIOS Version** Defaults to current version. Read-only unless restricted rollback is selected. **Allow BIOS Updates Using a Network** Lets you configure scheduled, automatic BIOS updates through the network. **BIOS Update Preferences** • Check for Update on Next Reboot: Default is disabled. • BIOS Source: Lets you select either HP.com or a custom URL. If **Custom URL** is selected, **Edit Custom URL** becomes active. HP recommends using a custom URL only for a managed IT environment. **Automatic BIOS Update Setting** Allows configuration of a periodic check for updates: NOTE: If Windows BitLocker Drive Encryption (BDE) is enabled, it must be temporarily suspended before the BIOS is flashed. • Do not update • Checking for updates and prompt the user to accept or reject the update at that time • Checking for updates and install all new versions • Checking for updates and install only new versions marked important **BIOS Update Frequency** • Daily • Weekly • Monthly (default)

Table 6-1 Computer Setup Main (continued)

Option	Description
Update System BIOS	**Network Configuration Settings** Lets you configure the network connection to the server that is the host for system firmware updates. **Update BIOS Using Local Media** Lets you access files on either USB storage or the hard drive. The HP BIOS Update and Recovery application included in BIOS Softpaqs at www.hp.com copies the BIOS file to the correct location on the hard drive or USB device.
Change date and time	Lets you update system date and time.
System IDs	Let you set the following values: • Asset Tracking Number • Ownership Tag
Replicated Setup	**Back up current settings to USB device** Saves system configuration to a formatted USB flash media device. **Restore current settings from USB device** Restores system configuration from a USB flash media device.
Save Custom Defaults	Saves the current system configuration settings as the custom default set.
Apply Custom Defaults and Exit	Applies the custom default settings to the computer after rebooting. Does not apply to options in the **Security** menu.
Apply Factory Defaults and Exit	Restores the factory system configuration settings to the computer after rebooting. Does not apply to options in the **Security** menu.
Ignore Changes and Exit	Exits Computer Setup without applying or saving any changes.
Save Changes and Exit	Saves changes to current system configuration, exits Computer Setup, and reboots.

Computer Setup Security

This table provides information about the Computer Setup Security menu.

NOTE: Support for specific Computer Setup options can vary, depending on the hardware configuration.

Table 6-2 Computer Setup Security

Option	Description
Create BIOS Administrator Password	Lets you set and enable a BIOS administrator password, which controls access to the following features: • Setup Menu (F10) • Third-Party Option ROM Management (F3) • Update system ROM • WMI commands that change system settings • BIOS Configuration Utility (BCU) • Alternative power-on password NOTE: Creating a BIOS user disables the Fast Boot option.
Change BIOS Administrator Password (This selection is active only if a BIOS administrator password is set.)	Lets you change the BIOS administrator password. You must know the current password to be able to change it.
Create POST Power-On Password	Lets you change or delete power-on password. The power-on password prompt appears after a power cycle or reboot. If the user does not enter the correct power-on password, the unit will not boot.
Change POST Power-On Password (This selection is active only if a BIOS administrator password is set.)	Lets you change the POST power-on password. You must know the current password to be able to change it.
Password Policies	Let you set the guidelines for a valid password. Options include: • Password minimum length • Requires at least one symbol • Requires at least one number • Requires at least one uppercase character • Requires at least one lowercase character • Allow spaces
Administrator Authentication Policies	Let you set limitations on some boot features restricting them to admin only, including: • Prompt for administrator authorization to access: – Boot menu in POST – System Recovery – Network boot – BIOS update • Allow the use of administrator credentials to modify the power-on password.

Table 6-2 Computer Setup Security (continued)

Option	Description
Security Configuration	**TPM Embedded Security** • **TPM Specification Version** Displays the current Trusted Platform Module (TPM) version. • **TPM Device** Lets you set the TPM as available or hidden. Default is available. • **TPM State** Select to enable the TPM. Default is disabled. • **Clear TPM** Select to reset the TPM to an unowned state. After the TPM is cleared, it is also turned off. To temporarily suspend TPM operations, turn the TPM off instead of clearing it. Default is no. IMPORTANT: Clearing the TPM resets it to factory defaults and turns it off. You will lose all created keys and data protected by those keys. • **TPM Activation Policy** ○ F1 to boot ○ Allow user to reject (default) ○ No prompts **BIOS Sure Start** • Verify Boot Block on every boot: Select to enable HP Sure Start. Default is disabled. • BIOS Data Recovery Policy: Select Automatic or Manual to determine data recovery process. Manual recovery is intended only for situations when you want forensic analysis before HP Sure Start recovery. When this policy is set to manual, HP Sure Start will not correct any issues that are found until the local user enters the manual recovery key sequence. This can result in a computer that cannot boot until the manual recovery key sequence is entered. • Network Controller Configuration Restore: Select to restore the network controller parameters to the factory state saved in the HP Sure Start Private nonvolatile (flash) memory. This setting is available only on computers with built-in NIC. NOTE: This process can take up to 30 seconds. You need to restore this only when the Network Controller Configuration mismatch warning is set. • Dynamic Runtime Scanning of Boot Block: Verifies the integrity of the BIOS boot block region several times each hour while the computer is running. Default is enabled. • Sure Start BIOS Settings Protection: When enabled, HP Sure Start locks all critical BIOS settings and provides enhanced protection for these settings using nonvolatile (flash) memory. Default is off. NOTE: An administrator password must be set to activate this setting. • Sure Start Secure Boot Keys Protection: Saves a backup copy of Secure Boot Keys so that they can be recovered if someone attempts to alter them in an unauthorized manner. • Enhanced HP Firmware Runtime Intrusion Prevention and Detection: Enables monitoring of HP system firmware executing out of main memory while the operating system is running. Any anomalies detected in HP system firmware that is active while the operating system is running will result in a Sure Start security event being generated.

Table 6-2 Computer Setup Security (continued)

Option	Description
Security Configuration	• Sure Start Security Event Policy. Controls HP Sure Start behavior upon identifying a critical security event, such as any modification to HP firmware, while the operating system is running. – Log Event Only: HP Sure Start will log all critical security events in the HP Sure Start audio log within the HP Sure Start nonvolatile (flash) memory. – Log Event and notify user: In addition to logging all critical security events, HP Sure Start will notify the user within the operating system that a critical event has occurred. – Log Event and power off system: In addition to logging all critical security events, HP Sure Start turns off the computer upon detecting a HP Sure Start Security Event. Because of the potential for data loss, HP recommends this setting only in situations where security integrity of the system is a higher priority than the risk of potential data loss. • Sure Start Security Event Boot Notification: Lets you enable a warning message on the startup screen if a Sure Start event, such as BIOS recovery or Memory intrusion, occurs. **Secure Boot Configuration**. Lets you be sure that an operating system is legitimate before booting to it, making Windows resistant to malicious modification from preboot to full operating system booting, preventing firmware attacks. UEFI and Windows Secure Boot only allow code signed by preapproved digital certificates to run during the firmware and OS boot process. NOTE: An administrator password must be set to activate this setting. Secure Boot must also be enabled. • Secure Boot: Default is disabled. • Secure Boot Key Management: Lets you manage the custom key settings. NOTE: Access to these settings requires Sure Start Secure Boot Keys Protection to be disabled. – Import Custom Secure Boot Keys: Default is disabled. – Clear Secure Boot keys: Lets you delete any previously loaded custom boot keys. Clearing keys will disable secure boot. Default is disabled. – Reset Secure Boot keys to factory defaults: Default is disabled. – Enable MS UEFI CA key: Disabling this setting alters the Secure Boot key list to further restrict the allowed software components. Set this option to disable to support Device Guard. Default is enabled. – Ready BIOS for Device Guard Use: Requires BIOS Administrator password to be configured and Secure Boot to be enabled.

Table 6-2 Computer Setup Security (continued)

Option	Description
Security Configuration	**Secure Platform Management (SPM)** • SPM Current State: Displays the current state. Also lets you change the state. • Unprovision SPM: Deprovisions SPM, which causes HP Sure Run to revert to the inactive state and return HP Sure Recover to default settings. • HP Sure Run Current State: Displays the current state. Also lets you change the state. Deactivate HP Sure Run: Deactivates HP Sure Run without deprovisioning SPM. • Smart Health Enable • EBAM Current State: Displays the current state. Also lets you change the state. Disable EBAM: Disables Enhanced BIOS Authentication Mode (EBAM). • Deactivate HP Sure Run: Requires BIOS Administrator password to be configured. • Local Access Key: Indicates is the key is present. Also lets you clear the keys and reboot. Clear EBAM Local Access Key(s) and Reboot: Deletes all currently established local access keys created for Enhanced BIOS Authentication Mode (EBAM). **Physical Presence Interface**: When set to enabled, the user is notified at system power up when changes are made to system security policy. The user must manually agree to those changes before the change is confirmed. Default is enabled. **Smart Cover**: The Smart Cover Lock (select products only) is a software-controllable solenoid lock that restricts unauthorized access to the system's internal components. • Cover Lock: Default is unlock. • Cover Removal Sensor: Lets you disable the cover sensor or configure what action is taken if the computer cover is removed. Default is disabled. NOTE: **Notify user** alerts the user with a POST error on the first boot after the sensor detects removal of the cover. If the password is set, **Administrator Password** requires that the password be entered to boot the computer if the sensor detects that the cover has been removed. **Trusted Execution Technology (TXT)** Enables Trusted Execution Technology on select Intel-based systems. Default is disabled. NOTE: Enabling this feature disables OS management of the Trusted Platform Module (TPM), prevents a reset of the TPM, and constrains the configuration of VTx, VTd, and TPM. **Intel Software Guard Extensions (SGX)** Intel SGX is a set of processor code instructions that allows user-level code to allocate private regions of memory. Unlike normal process memory, SGX protects these private memory regions from processes running at higher privilege levels. • Software control • Disable • Enable **Full encryption of main memory (DRAM)** (select products only) When selected, the computer stores all data to DRAM in an encrypted format.

Table 6-2 Computer Setup Security (continued)

Option	Description
Utilities	**Hard Drive Utilities** • **Save/Restore GPT of System Hard Drive** Enabling this feature saves the GUID Partition Table (GPT) of the system hard drive. If the GPT is subsequently changed, the user is prompted to choose whether to restore GPT. Default is disabled. • **Boot Sector (GPT) Recovery Policy** Allows selection of the default action when a GPT event occurs. • **DriveLock/Automatic DriveLock** Allows you to assign or modify a master or user password for hard drives. When this feature is enabled, the user is prompted to provide one of the DriveLock passwords during POST. If neither is successfully entered, the hard drive remains inaccessible until one of the passwords is successfully provided during a subsequent cold-boot sequence. NOTE: This selection appears only when at least one drive that supports the DriveLock feature is attached to the system. IMPORTANT: Be aware that these settings take place immediately. It is not necessary to save. IMPORTANT: Be sure to document the DriveLock password. Losing a DriveLock password will render a drive permanently locked. NOTE: Disable DriveLock on NVMe drives before using applications for hardware-based encryption. After you select a drive, the following options are available: – Set DriveLock Master Password. Sets the drive's master password but does not enable DriveLock. – Enable DriveLock. Sets the drive's user password and enables DriveLock. • **Secure Erase** Lets you select a hard drive to completely erase. After you erase a hard drive with a program that uses Secure Erase firmware commands, no file recovery program, partition recovery program, or other data recovery method can extract data from the drive. • **Allow OPAL Hard Drive SID Authentication** BIOS supports drive encryption using the DriveLock feature by creating the storage device's ownership key. If BIOS creates the key, any third-party applications (including other encryption software) are not allowed to perform certain drive operations such as establishing their own key using SID. Encryption software applications may or may not be limited by SID authentication lockout depending on how they are designed. Default is disabled.
Absolute Persistence Module Current State	Shows the current state of the Absolute Persistence module. Yes: Disabled No: Available
System Management Command	Allows authorized personnel to reset security settings during a service event. Default is enabled.
Restore Security Settings to Factory Default	This action resets security devices, clears BIOS passwords (not including DriveLock), and restores settings in the **Security menu** to factory defaults.

Computer Setup Advanced

This table provides information about the Computer Setup Advanced menu.

NOTE: Support for specific Computer Setup options can vary, depending on the hardware configuration.

Table 6-3 Computer Setup Advanced (for advanced users)

Option	Heading
Display Language	Lets you select the language of the menus in F10 Setup and the keyboard layout.
Scheduled Power-On	This feature wakes the system when it is off at a specified date and time.

Boot Options	Select the devices that the computer can boot from, as well as other options, including:
	• Startup Delay (sec): Enabling this feature adds a user-specified delay to the POST process. One purpose for the delay is to provide additional time to activate hotkeys such as esc for the Startup Menu or f10 for Computer Setup.
	• Fast Boot: Default is enabled.
	• CD-ROM Boot (select products only): Default is enabled.
	• USB Storage Boot: Default is enabled.
	• Network (PXE) Boot: Default is enabled.
	• After Power Loss: Default is Power Off.
	  ▪ Power off: Causes the computer to remain off when power is restored.
	  ▪ Power on: Causes the computer to turn on automatically as soon as power is restored.
	  ▪ Previous state: Causes the computer to turn on automatically as soon as power is restored, if it was on when power was lost.
	NOTE: If the system is configured to Power On from Keyboard Ports (see Power Management Options), this setting is forced to Power On.
	• Prompt on Memory Size Change: Default is enabled.
	• Prompt on Fixed Storage Change: Default is disabled.
	• Audio Alerts During Boot: Default is enabled. When disabled, most audible beeps from errors, warnings, and password prompts during boot up are suppressed.
	• Numlock on at boot: Default is disabled.
	• UEFI Boot Order: Specify the order in which UEFI boot sources are checked for a bootable operating system image. The default boot order is:
	  1. USB
	  2. SATA DVD
	  3. SATA hard drives
	  4. M.2 devices
	  5. Network boot

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Boot Options	NOTE: Use the UP and DOWN arrows to highlight an item. Press enter to select. Use the UP and DOWN arrows to move a selected item. Press f5 to enable or disable. Press esc to exit. NOTE: MS-DOS drive lettering assignments might not apply after a non-MS-DOS operating system has started. **Shortcut to Temporarily Override Boot Order** To boot **one time** from a device other than the default device specified in Boot Order, restart the computer and press esc (to access the Startup menu) and then f9 (Boot Menu), or only f9 (skipping the Startup menu) when the power button light turns white. After POST is completed, a list of bootable devices is displayed. Use the arrow keys to select the preferred bootable device and press enter. The computer then boots from the selected non-default device for this one time.
HP Sure Recover	**HP Sure Recover** If enabled and HP Sure Recover is launched, the system firmware honors local and remote requests to reinstall the operating system. If it is disabled, all requests to reinstall the operating system are ignored. Default is enabled. **Recover from Network** Allows system firmware to retrieve the recovery agent from the network. If disabled, system firmware retrieves the recovery agent from a local drive. Default is enabled. **Recover after Boot Failure** If enabled and no bootable UEFI operating system is found, system firmware launches HP Sure Recover. Default is disabled. **Recover before Boot Failure Recovery** If enabled and HP Sure Recover is launched because of a boot failure, the user is notified of the boot failure and asked to choose whether to start or cancel HP Sure Recover. This setting is displayed only if **Recover after Boot Failure** is selected. **Recovery Agent** Displays recovery agent information. This information is displayed only if **Recover from Network** is selected. **Recovery Image** Displays recovery image information. This information is displayed only if **Recover from Network** is selected. **OS Recovery Image Version**. Display the version of the recovery image stored in the embedded secure storage device. This information is displayed only if an embedded secure storage device is installed. **OS Recovery Driver Version** Display the version of the recovery driver stored in the embedded secure storage device. This information is displayed only if an embedded secure storage device is installed.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
System Options	**Configure storage controller for Intel Optane** (Intel products only) Enables the Intel Optane™ memory module. **Configure storage controller for RAID** Enables RAID. Default is enabled. **Limit PCIe Speed** (workstation models only) Lets you restrict the maximum speed of the PCI Express devices to previous generations. The following settings are possible: - Auto - Gen 1 (2.5 Gbps) - Gen 2 (5 Gbps) - Gen 3 (8 Gbps) **Turbo-boost** (Intel products only) Allows Intel Turbo Boost Technology to improve performance when operation conditions allow. Default is enabled. **Hyperthreading** (Intel products only) Lets you control processor capability. Default is enabled. **Virtualization Technology (VTx)** (Intel only) Controls the virtualization features of the processor. Changing this setting requires turning the computer off and then back on. Default is disabled. **Virtualization Technology for Directed I/O (VTd)** (Intel only) Controls virtualization DMA remapping features of the chipset. Changing this setting requires turning the computer off and then back on. Default is disabled. **SVM CPU Virtualization** (AMD® products only) Enables AMD-V and AMD-Vi virtualization features on AMD-based systems **Enhanced Hello Sign-in** (systems with supporting hardware for biometric identification only) Allows for secure logon using the Windows Hello feature. **DMA Protection** Enables DMA redirection using IOMMU for enhanced security. Default is enabled. NOTE: Requires that VTd is enabled. **Pre-boot DMA protection** Secures memory access through DMA to allowed regions prior to operating system startup. **Full encryption of main memory (DRAM)** (select products only) Stores all data to DRAM in an encrypted format. Default is enabled. **PCI slots** (vary by product) Lets you enable or display PCI slots. Default is enabled.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
System Options	**M.2 slots** (vary by product) Lets you enable or display M.2 slots. Default is enabled. **Power Button Override** (disable/4 sec/15 sec/30 sec) Lets you enable and select the number of seconds you have to hold down the power button for it to force the system to turn off. Default is 4 sec. **USB Type-C Connector System Software Interface (UCSI)** (select products only) Allows UCSI to be exposed to the operating system (ACPI table). **HP Application Driver** Provides ACPI structure to enable HP common software application framework. The driver is provided in the latest HP support software that you can download from the web. NOTE: Device Manager shows an alert if this setting is enabled without the HP application driver installed. **AMD DASH** Lets you enable AMD Remote system management capability. Default is disabled. **Hardware enabled Spectre Variant 2 Mitigation** Enables Single Thread Indirect Branch Predictor (STIBP) functionality in AMD processors. Default is disabled.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Built-In Device Options	**Embedded LAN Controller** (select products only) Select to show the device in the operating system. Default is enabled. **Wake On LAN** Lets you either disable the Wake On LAN feature or configure where the computer boots, including the network or hard drive. Default is boot to network. **LAN Controller Option (1)(2)** (select products only) Enables the integrated network controller in the designated rear option slot. **Dust Filter** (select products only) Default is disabled. **Dust Filter Reminder (Days)** (select products only) Default is 60. **Allow No Panel configuration** (All-in-One 1000 series models only) Allows operation of the base unit without a boot warning when the panel is not installed. **Integrated Video** (models with discrete graphics) Disables the integrated video device. When not using integrated video, disabling the integrated video will free some system memory. **VGA Boot Device** (models with discrete graphics) Selects the graphics controller to use as the primary VGA device during boot-up when there are multiple graphics devices. The firmware can use only one graphics device when booting up. **Video Memory Size** Lets you manage graphics memory allocation. The value you choose is allocated permanently to graphics and is unavailable to the operating system. **Integrated Camera** Lets you disable the integrated camera. Default is enabled. **Audio Device** Select to show audio devices in the operating system, including integrated microphone, internal speakers, and headphone out. When selected, operating system visibility of each audio device is controlled independently. When this setting is cleared, all audio devices are hidden from the operating system. Individual audio device settings are also disabled. Default is enabled. **Microphone** Clear to disable the integrated microphone. This does not affect devices plugged into audio jacks. The disable and lock setting prevents other audio ports from being remapped to the microphone function in the operating system. Default is enabled. **Internal Speakers** (does not affect external speakers) Clear to disable the chassis speaker or speakers. This function is applicable to normal audio playback in the operating system and does not affect the error or warning beeps during POST. Default is enabled. **Headphone Output** Clear to disable the headphone jack. Default is enabled.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Built-In Device Options	**Collaboration Buttons** (select products only) Clear to disable the collaboration buttons. Default is enabled. **Button Sensitivity** (select products only) Controls touch sensitivity of collaboration buttons. Select from low, medium, or high. **LAN/WLAN auto switching** Select to enable auto switching between a wired and wireless connection. Default is disabled. **Wake on WLAN** Select to enable wake on WLAN. Default is disabled. **M.2 USB/Bluetooth®** Select to enable the M.2 controller. Default is enabled. **Increase Idle Fan Speed (%)** Increases the minimum fan speeds over the normal settings while still enabling normal control using the internal thermal sensors. **Force enable HP Sure View** Enables the HP Sure View privacy panel by changing the screen brightness.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Port Options	**USB ports** (varies by model) Lets you enable specific USB ports. Default is enabled. **USB Legacy Port Charging** Lets you enable USB charging port capability when the computer is in hibernate or shutdown mode. Default is enabled. **USB Type-C Downstream Charging** Lets you enable USB charging port capability when the computer is in hibernate, on, or off. Default is enabled. **Media Card Reader/SD_RDR USB** Enables the media card reader connector (labeled SD_RDR) on a desktop. Default is enabled. **SATA** (varies by model) Lets you hide SATA ports from the operating system. Default is enabled (not hidden). **Serial Port** (varies by model) Lets you enable specific serial ports. Default is enabled. **Serial Port Voltage** (Retail Point-of-Sale models only; ports vary by model) Lets you configure powered serial port voltage selection on RPOS units that include this feature. Default is 0 Volts. • 0 Volts • 5 Volts • 12 Volts **Cash Drawer Port** (Retail Point-of-Sale models only) Controls whether the cash drawer port can be activated. Default is enabled. **Restrict USB Devices** Specify the following categories of USB devices to enable: • Allow all USB devices (default) • Allow only keyboard and mouse • Allow all but storage devices and hubs When some devices are restricted, the system will disable USB ports that do not meet the allowed criteria. This feature is usually combined with similar policies within the operating system because USB devices can be moved to different ports. The ports disabled by the BIOS remain disabled until the system is restarted.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Power Management Options	**Runtime Power Management** Allows certain operating systems to reduce processor voltage and frequency when the current software load does not require the full capabilities of the processor. Default is enabled. **Extended Idle Power States** Allows certain operating systems to decrease the processors power consumption when the processor is idle. Default is enabled. **S5 Maximum Power Savings** Enabling this feature reduces the power of the system as much as possible in the S5 state. Power is removed from the wake up circuitry, the expansion slots, and any management features while in S5. Default is disabled. **SATA Power Management** Enables or disables SATA bus, device power management, or both. Default is enabled. **PCI Express Power Management** Enabling this option permits the PCI Express links to use Active Power State Management (ASPM) to enter lower power states while not in use. Default is enabled. **Power On from Keyboard Ports** When enabled, this feature allows a key press to turn on the system when it is off (S5 state). If using a USB keyboard, you must plug it into one of the rear ports labeled with the keyboard icon. Default is disabled. **Unique Sleep State Blink Rates** This feature is designed to provide a visual indication of what Sleep state the system is in. Each Sleep state has a unique blink pattern. Default is disabled. NOTE: A normal shutdown goes to the S4 state for Windows 8 or later. S0 (On) = solid white light. S3 (Stand By) = 3 blinks at 1 Hz (50% duty cycle) followed by a pause of 2 seconds (white light), repeated cycles of 3 blinks and a pause. S4 (Hibernation) = 4 blinks at 1 Hz (50% duty cycle) followed by a pause of 2 seconds (white light), repeated cycles of 4 blinks and a pause. S5 (Soft Off) = Light is off.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Remote Management Options (Intel only)	**Active Management Technology (AMT)** Allows you to discover, repair, and protect networked computing devices. Default is enabled. **USB Key Provisioning Support** Enables AMT provisioning using a USB storage device. Default is disabled. **USB Redirection Support** USB redirection allows USB devices plugged into a client computer to be transparently redirected to the guest operating system. Default is enabled. **Unconfigure AMT on next boot**. Resets AMT configuration options on next boot. Default is Do Not Apply. **SOL Terminal Emulation Mode** SOL (serial-over-LAN) terminal emulation mode is only activated during remote AMT (Active Management Technology) redirection operations. The emulation options allow administrators to select which mode works best with their console. Default is ANSI. **Show Unconfigure ME Confirmation Prompt** Requires user confirmation when unconfiguring the Intel Management Engine. Default is enabled. **Verbose Boot Messages** Verbose boot shows additional logging information during startup, which is mainly for debugging if something goes wrong during bootup. Default is enabled. **Watchdog Timer** Allows you to set the amount of time for an operating system and BIOS watchdog alert to be sent if the timers are not deactivated. BIOS watchdog is deactivated by BIOS and would indicate that a halt occurred during execution if the alert is sent to the management console. An operating system alert is deactivated by the operating system image and would indicate that a hang occurred during its initialization. Default is enabled. • OS Watchdog Timer (min.). Default is 5 min. • BIOS Watchdog Timer (min.). Default is 5 min. **CIRA Timeout (min.)** CIRA is Customer Initiated Remote Assistance, an Intel service to help users employing Active Management Technology (AMT). Default is 1.

Table 6-3 Computer Setup Advanced (for advanced users) (continued)

Option	Heading
Thunderbolt Options (select products only)	**Thunderbolt Mode** Enables Thunderbolt™ connections on the Type-C port. When cleared, disables Thunderbolt connections on the Type-C port and disables PCIe tunneling on USB4 connections. **Require BIOS PW to change Thunderbolt Security Level** When selected, **Thunderbolt Security Level** cannot be changed unless a BIOS administrator password has been created. This setting cannot be disabled if DMA Protection (System Options) is enabled. **Thunderbolt Security Level** • PCIe and DisplayPort – No Security: Any Thunderbolt device detected that requests a PCI-express connection is connected to the system PCI-express bus without approval by the local user. • PCIe and DisplayPort – User Authorization (default): Each Thunderbolt peripheral includes a unique identifier used to determine if the device has been previously connected. If the user previously selected **Always Connect** for a device, it is automatically connected to the PCI-Express bus when attached. • PCIe and DisplayPort – Secure Connect: Offers enhanced protection for authenticating a previously connected Thunderbolt device beyond relying on its identifier. The device is provisioned with a key when initially connected, and on subsequent connections a challenge-response is implemented to verify the device before it is connected to the PCI-express bus. • DisplayPort™ only: Permits only USB and DisplayPort functionality to be available via the Type-C Thunderbolt port. PCI-Express will not be connected from the Thunderbolt device to the internal PCI-express interface, thus any Thunderbolt device that requires PCI-Express will not function correctly. **Native PCIe Hot Plug** Enables hot plug support to the system PCI-Express bus.
Remote HP PC Hardware Diagnostics	**Settings** Sets the configuration for Remote HP PC Hardware Diagnostics, including the URLs used for download and upload and scheduled execution frequency. **Execute Remote HP PC Hardware Diagnostics** Select to immediately execute Remote HP PC Hardware Diagnostics based on the how settings are configured. Any unsaved BIOS settings will be lost.

7 POST error messages

This section lists the error codes, error messages, and the various indicator light and audible sequences that you may encounter during Power-On Self-Test (POST) or computer restart, the probable source of the problem, and steps you can take to resolve the error condition.

POST Message Disabled suppresses most system messages during POST, such as memory count and non-error text messages. If a POST error occurs, the screen will display the error message. To manually switch to the POST Messages Enabled mode during POST, press any key except f10, f11, or f12. The default mode is POST Message Disabled.

The POST mode selection determines the speed at which the computer loads the operating system and the extent to which it is tested.

Quick Boot is a fast startup process that does not run all of the system level tests, such as the memory test. Full Boot runs all of the ROM-based system tests and takes longer to complete.

You can enable Full Boot to run every 1 to 30 days on a regularly scheduled basis. To establish the schedule, reconfigure the computer to the Full Boot Every x Days mode, using Computer Setup.

NOTE: For more information about Computer Setup, see Computer Setup (F10) Utility on page 54.

POST numeric codes and text messages

This section identifies those POST errors that have numeric codes associated with them. The section also includes some text messages that you might encounter during POST.

NOTE: The computer beeps once after a POST text message is displayed on the screen.

Table 7-1 POST numeric codes and text messages

Control panel message	Description	Recommended action
002-Option ROM Checksum Error	System ROM or expansion board option ROM checksum.	1. Verify the correct ROM. 2. Flash the ROM if needed. 3. If an expansion board was recently added, remove it to see if the problem remains. 4. Clear CMOS. 5. If the message disappears, there might be a problem with the expansion card. 6. Replace the system board.
003-System Board Failure	DMA or timers.	1. Clear CMOS. 2. Replace the system board.

Table 7-1 POST numeric codes and text messages (continued)

Control panel message	Description	Recommended action
005-Real-Time Clock Power Loss	Invalid time or date in configuration memory. RTC (real-time clock) battery might need to be replaced.	Reset the date and time under Control Panel (Computer Setup can also be used). If the problem persists, replace the RTC battery. See Removal and replacement procedures on page 31 for instructions about installing a new battery.
008-Microcode Patch Error	Processor is not supported by the BIOS.	1. Upgrade BIOS to proper version. 2. Change the processor.
009-PMM Allocation Error during MEBx Download	Memory error during POST execution of the Management Engine (ME) BIOS Extensions option ROM.	1. Reboot the computer. 2. Unplug the power cord, reseat the memory modules, and reboot the computer. 3. If the memory configuration was recently changed, unplug the power cord, restore the original memory configuration, and reboot the computer. 4. If the error persists, replace the system board.
00A-Product Information Not Valid	The product information programmed into the system board is missing or invalid.	Use Computer Setup (F10) Utility on page 54 to update this information.
00B-MEBx Module did not checksum correctly	Memory error during POST execution of the Management Engine (ME) BIOS Extensions option ROM.	1. Reboot the computer. 2. Unplug the power cord, reseat the memory modules, and reboot the computer. 3. If the memory configuration was recently changed, unplug the power cord, restore the original memory configuration, and reboot the computer. 4. If the error persists, replace the system board.
00C-PMM Deallocation Error during MEBx Cleanup	Memory error during POST execution of the Management Engine (ME) BIOS Extensions option ROM.	1. Reboot the computer. 2. Unplug the power cord, reseat the memory modules, and reboot the computer. 3. If the memory configuration was recently changed, unplug the power cord, restore the original memory configuration, and reboot the computer. 4. If the error persists, replace the system board.

Table 7-1 POST numeric codes and text messages (continued)

Control panel message	Description	Recommended action
00D-Setup Error during MEBx Execution	MEBx selection or exit resulted in a setup failure.	1. Reboot the computer. 2. Unplug the power cord, reseat the memory modules, and reboot the computer. 3. If the memory configuration was recently changed, unplug the power cord, restore the original memory configuration, and reboot the computer. 4. If the error persists, replace the system board.
00E-Inventory Error during MEBx Execution	BIOS information passed to the MEBx resulted in a failure.	1. Reboot the computer. 2. If the error persists, update to the latest BIOS version. 3. If the error still persists, replace the system board.
00F-Interface Error during MEBx Execution	MEBx operation experienced a hardware error during communication with the ME.	1. Reboot the computer. 2. If the error persists, update to the latest BIOS version. 3. If the error still persists, replace the system board.
100-Front Audio Not Connected	Front audio cable has been detached or unseated from system board.	Reconnect or replace front audio cable.
2E1-MemorySize Error	Memory amount has changed since the last boot (memory added or removed).	The system memory size is different from the last startup. The most common reason is the removal of memory from the system board. Press the f1 key to save the memory changes.
2E2-Memory Error	Memory module configuration failed during boot-up.	1. Be sure that memory modules are correctly installed. 2. Verify proper memory module type. 3. Remove and replace the identified faulty memory modules. 4. If the error persists after replacing memory modules, replace the system board.
2E3-Incompatible Memory Module in Memory Socket(s) X, X, ...	A memory module in memory socket identified in the error message is missing critical SPD information, or is incompatible with the chipset.	1. Verify proper memory module type. 2. Try another memory socket. 3. Replace with a supported module.
2E4-DIMM Configuration Warning	Populated DIMM Configuration is not optimized.	Rearrange the DIMMs so that each channel has the same amount of memory.

Table 7-1 **POST numeric codes and text messages (continued)**

Control panel message	Description	Recommended action
2E5-ECC Memory Module Detected on Unsupported Platform	Recently added memory modules support ECC memory error correction.	1. If additional memory was recently added, remove it to see if the problem remains. 2. Check product documentation for memory support information.
2E6-Memory Not Configured Correctly for Proper MEBx Execution	DIMM1 is not installed.	Be sure that a memory module is in the DIMM1 socket and that it is properly seated.
300-Configuration Change Warning	A change in storage configuration has been detected (see the **Boot Options** menu in BIOS Setup to enable this feature). Either the installed hardware has changed, storage or firmware mode might have been changed, or a storage device might have failed to respond.	If no changes were made before this warning, check that the drives are connected properly to power cables and system board. User Diagnostics (f2 during boot-up) might help identify any problem with specific devices.
301-Hard Disk 1: SMART Hard Drive Detects Imminent Failure	Hard drive will soon fail. (Some hard drives have a hard drive firmware patch that will fix an erroneous error message.)	1. Determine whether hard drive is giving correct error message. Run the Drive Protection System test under using F2 Diagnostics when booting the computer. 2. Apply hard drive firmware patch if applicable. (Available at http://www.hp.com/support.) 3. Back up contents and replace hard drive.
302-Hard Disk 2: SMART Hard Drive Detects Imminent Failure	Hard drive will soon fail. (Some hard drives have a hard drive firmware patch that will fix an erroneous error message.)	1. Determine whether hard drive is giving correct error message. Run the Drive Protection System test under using F2 Diagnostics when booting the computer. 2. Apply hard drive firmware patch if applicable. (Available at http://www.hp.com/support.) 3. Back up contents and replace hard drive.
309 - 30C: Hard Disk 3-6: SMART Hard Drive Detects Imminent Failure	Hard drive will soon fail. (Some hard drives have a hard drive firmware patch that will fix an erroneous error message.)	1. Determine whether hard drive is giving correct error message. Run the Drive Protection System test under using F2 Diagnostics when booting the computer. 2. Apply hard drive firmware patch if applicable. (Available at http://www.hp.com/support.) 3. Back up contents and replace hard drive.
3F0-Boot Device Not Found	Boot device not found.	Insert boot device or load operating system.

Table 7-1 POST numeric codes and text messages (continued)

Control panel message	Description	Recommended action
3F1–Hard Disk 1 Error	Hard disk 1 error.	1. Check and/or replace cables. 2. Clear CMOS. 3. Replace the hard disk drive.
3F2–Hard Disk 2 Error	Hard disk 2 error.	1. Check and/or replace cables. 2. Clear CMOS. 3. Replace the hard disk drive.
400-Serial Port A Address Conflict Detected	Both external and internal serial ports are assigned to the same resources.	1. Remove any serial port expansion cards. 2. Clear CMOS. 3. Reconfigure card resources and/or run Computer Setup or Windows utilities.
401-Serial Port B Address Conflict Detected	Both external and internal serial ports are assigned to the same resources.	1. Remove any serial port expansion cards. 2. Clear CMOS. 3. Reconfigure card resources and/or run Computer Setup or Windows utilities.
402-Serial Port C Address Conflict Detected	Both external and internal serial ports are assigned to the same resources.	1. Remove any serial port expansion cards. 2. Clear CMOS. 3. Reconfigure card resources and/or run Computer Setup or Windows utilities.
403-Serial Port D Address Conflict Detected	Both external and internal serial ports are assigned to the same resources.	1. Remove any serial port expansion cards. 2. Clear CMOS. 3. Reconfigure card resources and/or run Computer Setup or Windows utilities.
419-Out of Memory Space for Option ROMs	Recently added PCI expansion card contains an option ROM too large to download during POST.	If a PCI expansion card was recently added, remove it to see if the problem remains.
41A-Front USB1/USB2 Not Connected	Front USB cable has been detached or unseated from system board.	Reconnect or replace front USB cable.
41B-Device in PCI Express Slot Failed To Initialize	There is an incompatibility or problem with a PCIe device and the system or PCIe link could not be configured to a valid bus width or speed.	Try rebooting the system. If the error reoccurs, the device might not work with this system
43A-USB Type-C I2C Not Connected	Cable is required between I2C on card and USB-C® on the system board.	Install cable between I2C on card and USB-C on the system board.
43B-More Than One USB type-C Cards Are Installed	More than one USB Type-C card is installed.	Remove USB Type-C card so only one is installed.

Table 7-1 POST numeric codes and text messages (continued)

Control panel message	Description	Recommended action
500–BIOS Recovery	A system BIOS recovery has occurred.	Not applicable.
70x-Wireless Mode Not Supported	The system has detected a wireless module installed in the system that is not supported and has been disabled.	Replace with a supported module.
800-Keyboard Error	Keyboard failure.	1. Reconnect keyboard with computer turned off. 2. Check connector for bent or missing pins. 3. Be sure that none of the keys are pressed. 4. Replace keyboard.
801-Keyboard or System Unit Error	Keyboard failure.	1. Reconnect the keyboard with computer turned off. 2. Be sure that none of the keys are pressed. 3. Replace the keyboard. 4. Replace the system board.
900-CPU Fan Not Detected	CPU fan is not connected or might have malfunctioned.	1. Reseat fan. 2. Reseat fan cable. 3. Replace fan.
901-Chassis, Rear Chassis, Front Chassis, or PCIe blower Fan not Detected	Fan is not connected or might have malfunctioned.	1. Reseat fan. 2. Reseat fan cable. 3. Replace fan.
904-SATA Cabling Error	One or more SATA devices are improperly attached. For optimal performance, the SATA0, SATA1, and SATA2 ports should be used for hard drives before other ports.	Be sure that SATA connectors are used in ascending order. For one device, use SATA0. For two devices, use SATA0 and SATA1. For three devices, use SATA0, SATA1, and SATA2.
90B-Fan Failure	The system has detected that a cooling fan is not operating correctly.	1. Reseat fan. 2. Reseat fan cable. 3. Replace fan.
90D-System Temperature	Thermal shutdown occurred. The system BIOS has detected that your machine was previously shut down to avoid overheating. Overheating might occur if the cooling vents are blocked or the operating temperature exceeds the system specifications. The machine should return to normal operation once the situation is resolved.	Be sure system has proper airflow.
90E-Power Supply Fan Not detected	Power supply fan is not connected or might have malfunctioned.	1. Reseat power supply fan. 2. Reseat fan cable. 3. Replace power supply fan.

Table 7-1 POST numeric codes and text messages (continued)

Control panel message	Description	Recommended action
910–Filter Warning	Airflow filter is dirty.	Replace the airflow filter.
911–Graphics Module Fan Not Detected	Graphics card fan is not connected or might have malfunctioned.	1. Reseat graphics card fan. 2. Reseat fan cable. 3. Replace graphics card fan.
912–Incorrect CPU cooler installed for this configuration	The processor cooler/heat sink does not match processor power requirement.	Replace the cooler/heat sink to match the processor power requirement.

Interpreting POST diagnostic front panel lights and audible codes

This section identifies the front panel light codes as well as the audible codes that can occur before or during POST that might not have an error code or text message associated with them.

⚠ CAUTION: When the computer is plugged into an AC power source, voltage is always applied to the system board. To reduce the risk of personal injury from electrical shock and/or hot surfaces, be sure to disconnect the power cord from the AC outlet and allow the internal system components to cool before touching.

During the system validation phase that occurs at system startup, the BIOS validates the functionality of the following subsystems and conditions:

- AC adapter
- System board power
- Processor failure
- BIOS corruption
- Memory failure
- Graphics failure
- System board failure
- BIOS authentication failure

If an error is detected, specific patterns of long and short blinks, accompanied by long and short beeps (where applicable) are used to identify the error. These patterns make up a two-part code:

- Major: The category of the error
- Minor: The specific error within the category

NOTE: Single beep and blink codes are not used.

Table 7-2 Beep pattern error identification

Number of long beeps/blinks	Error category
1	Not used
2	BIOS
3	Hardware
4	Thermal
5	System board

Patterns of blink/beep codes are determined by using the following parameters:

- 1 second pause occurs after the last major blink.
- 2 second pause occurs after the last minor blink.
- Beep error code sequences occur for the first five iterations of the pattern and then stop.
- Blink error code sequences continue until the computer is unplugged or the power button is pressed.

NOTE: Not all diagnostic lights and audible codes are available on all models.

The red LED blinks to represent the major error category (long blinks). The white LED blinks to represent the minor error category (short blinks). For example, '3.5' indicates 3 long red blinks and 5 short white blinks to communicate the processor is not detected.

Table 7-3 Interpreting POST diagnostic front panel lights and audible codes

Category	Major/minor code	Description
BIOS	2.2	The main area (DXE) of BIOS has become corrupted, and there is no recovery binary image available.
	2.3	The embedded controller policy requires the user to enter a key sequence.
	2.4	The embedded controller is checking or recovering the boot block.
Hardware	3.2	The embedded controller has timed out waiting for BIOS to return from memory initialization.
	3.3	The embedded controller has timed out waiting for BIOS to return from graphics initialization.
	3.4	The system board displays a power failure (crowbar).*
	3.5	The processor is not detected.*
	3.6	The processor does not support an enabled feature.
	3.7	The access panel/top cover has been opened since the last computer start.
Thermal	4.2	A processor over temperature condition has been detected.*
	4.3	An ambient temperature over temperature condition has been detected.
	4.4	An MXM over temperature condition has been detected.

Table 7-3 Interpreting POST diagnostic front panel lights and audible codes (continued)

Category	Major/minor code	Description
System board	5.2	The embedded controller cannot find valid firmware.
	5.3	The embedded controller has timed out waiting for the BIOS.
	5.4	The embedded controller has timed out waiting for BIOS to return from system board initialization.
	5.5	The embedded controller rebooted the system after a possible lockup condition had been detected through the use of a System Health Timer, Automated System Recovery Timer, or other mechanism.

* Indicates a hardware-triggered event; BIOS controls all other events.

8 Password security and resetting CMOS

This computer supports two security password features that you can establish through the Computer Setup Utilities menu: administrator password and power-on password.

When you establish only an administrator password, any user can access all the information on the computer except Computer Setup. When you establish only a power-on password, the power-on password is required to access Computer Setup and any other information on the computer. When you establish both passwords, only the administrator password will give you access to Computer Setup.

When both passwords are set, you can use the administrator password in place of the power-on password as an override to log in to the computer. This feature is useful for a network administrator.

IMPORTANT: Back up the BIOS settings or save them as custom defaults in case you need them later. You can back up in Computer Setup or with the BiosConfigUtility tool available from www.hp.com. See Computer Setup (F10) Utility on page 54 for information about backing up the BIOS settings.

Changing a setup or power-on password

Use this procedure to change a password.

To change the power-on or setup password, complete the following steps:

1. Turn on or restart the computer.

   To change the setup password, go to step 2.

   To change the power-on password, go to step 3.

2. To change the setup password, as soon as the computer turns on:

   - Press esc while the “Press the ESC key for Startup Menu” message is displayed.

   - Press f10 to enter Computer Setup.

3. When the key icon appears, type your current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:

   current password/new password/new password

   NOTE: Type the new password carefully because the characters do not appear on the screen.

4. Press enter.

The new password will take effect the next time the computer is restarted.

Deleting a setup or power-on password

Use this procedure to delete a password.

To delete the power-on or setup password, complete the following steps:

1. Turn on or restart the computer.

   To delete the Setup password, go to step 2.

   To delete the Power-on password, go to step 3.

2. To delete the Setup password, as soon as the computer turns on:

   - Press esc while the “Press the ESC key for Startup Menu” message is displayed.

   - Press f10 to enter Computer Setup.

3. When the key icon appears, type your current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:

   current password/new password/new password

4. Press enter.

9 Backing up, restoring, and recovering

You can use Windows tools or HP software to back up your information, create a restore point, reset your computer, create recovery media, or restore your computer to its factory state. Performing these standard procedures can return your computer to a working state faster.

IMPORTANT: If you are performing recovery procedures on a tablet, the tablet battery must be at least 70% charged before you start the recovery process.

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning any recovery process.

Backing up information and creating recovery media

These methods of creating recovery media and backups are available on select products only.

Using Windows tools for backing up

HP recommends that you back up your information immediately after initial setup. You can do this task either using Windows Backup locally with an external USB drive or using online tools.

IMPORTANT: Windows is the only option that allows you to back up your personal information. Schedule regular backups to avoid information loss.

NOTE: If computer storage is 32 GB or less, Microsoft® System Restore is disabled by default.

Using the HP Cloud Recovery Download Tool to create recovery media (select products only)

You can use the HP Cloud Recovery Download Tool to create HP Recovery media on a bootable USB flash drive.

For details:

- Go to http://www.hp.com, search for HP Cloud Recovery, and then select the result that matches the type of computer that you have.

NOTE: If you cannot create recovery media yourself, contact support to obtain recovery discs. Go to http://www.hp.com/support, select your country or region, and then follow the on-screen instructions.

IMPORTANT: HP recommends that you follow the Restoring and recovery methods on page 87 to restore your computer before you obtain and use the HP recovery discs. Using a recent backup can return your machine to a working state sooner than using the HP recovery discs. After the system is restored, reinstalling all the operating system software released since your initial purchase can be a lengthy process.

Restoring and recovering your system

You have several tools available to recover your system both within and outside of Windows if the desktop cannot load.

HP recommends that you attempt to restore your system using the Restoring and recovery methods on page 87.

Creating a system restore

System Restore is available in Windows. The System Restore software can automatically or manually create restore points, or snapshots, of the system files and settings on the computer at a particular point.

When you use System Restore, it returns your computer to its state at the time you made the restore point. Your personal files and documents should not be affected.

Restoring and recovery methods

After you run the first method, test to see whether the issue still exists before you proceed to the next method, which might now be unnecessary.

1. Run a Microsoft System Restore.
2. Run Reset this PC.

   NOTE: The options **Remove everything** and then **Fully clean the drive** can take several hours to complete and leave no information on your computer. It is the safest way to reset your computer before you recycle it.

3. Recover using HP Recovery media. For more information, see Recovering using HP Recovery media on page 87.

For more information about the first two methods, see the Get Help app:

Select the **Start** button, select the **Get Help** app, and then enter the task you want to perform.

NOTE: You must be connected to the internet to access the Get Help app.

Recovering using HP Recovery media

You can use HP Recovery media to recover the original operating system and software programs that were installed at the factory. On select products, it can be created on a bootable USB flash drive using the HP Cloud Recovery Download Tool.

For details, see Using the HP Cloud Recovery Download Tool to create recovery media (select products only) on page 86.

NOTE: If you cannot create recovery media yourself, contact support to obtain recovery discs. Go to http://www.hp.com/support, select your country or region, and then follow the on-screen instructions.

To recover your system:

- Insert the HP Recovery media, and then restart the computer.

NOTE: HP recommends that you follow the Restoring and recovery methods on page 87 to restore your computer before you obtain and use the HP recovery discs. Using a recent backup can return your

machine to a working state sooner than using the HP recovery discs. After the system is restored, reinstalling all the operating system software released since your initial purchase can be a lengthy process.

Changing the computer boot order

If your computer does not restart using the HP Recovery media, you can change the computer boot order, which is the order of devices listed in BIOS for startup information. You can select an optical drive or a USB flash drive, depending on the location of your HP Recovery media.

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning these steps.

To change the boot order:

1. Insert the HP Recovery media.
2. Access the system **Startup** menu.
   - For computers or tablets with keyboards attached, turn on or restart the computer or tablet, quickly press esc, and then press f9 for boot options.
   - For tablets without keyboards, turn on or restart the tablet, quickly press and hold the volume up button, and then select **f9**.

     – or –

     Turn on or restart the tablet, quickly press and hold the volume down button, and then select **f9**.
3. Select the optical drive or USB flash drive from which you want to boot, and then follow the on-screen instructions.

Using HP Sure Recover (select products only)

Select computer models are configured with HP Sure Recover, a PC operating system (OS) recovery solution built into the hardware and software. HP Sure Recover can fully restore the HP OS image without installed recovery software.

Using HP Sure Recover, an administrator or user can restore the system and install:

- Latest version of the operating system
- Platform-specific device drivers
- Software applications, in the case of a custom image

To access the latest documentation for HP Sure Recover, go to http://www.hp.com/support. Follow the on-screen instructions to find your product and locate your documentation.

10 Using HP PC Hardware Diagnostics

You can use the HP PC Hardware Diagnostics utility to determine whether your computer hardware is running properly. The three versions are HP PC Hardware Diagnostics Windows, HP PC Hardware Diagnostics UEFI (Unified Extensible Firmware Interface), and (for select products only) Remote HP PC Hardware Diagnostics UEFI, a firmware feature.

Using HP PC Hardware Diagnostics Windows (select products only)

HP PC Hardware Diagnostics Windows is a Windows-based utility that allows you to run diagnostic tests to determine whether the computer hardware is functioning properly. The tool runs within the Windows operating system to diagnose hardware failures.

If HP PC Hardware Diagnostics Windows is not installed on your computer, you must download and install it. To download HP PC Hardware Diagnostics Windows, see Downloading HP PC Hardware Diagnostics Windows on page 90.

Using an HP PC Hardware Diagnostics Windows hardware failure ID code

When HP PC Hardware Diagnostics Windows detects a failure that requires hardware replacement, a 24-digit failure ID code is generated for select component tests. For interactive tests, such as keyboard, mouse, or audio and video palette, you must perform troubleshooting steps before you can receive a failure ID.

- You have several options after you receive a failure ID:
  - Select **Next** to open the Event Automation Service (EAS) page, where you can log the case.
  - Scan the QR code with your mobile device, which takes you to the EAS page, where you can log the case.
  - Select the box next to the 24-digit failure ID to copy your failure code and send it to support.

Accessing HP PC Hardware Diagnostics Windows

After HP PC Hardware Diagnostics Windows is installed, you can access it from HP Support Assistant or the Start menu.

Accessing HP PC Hardware Diagnostics Windows from HP Help and Support (select products only)

After HP PC Hardware Diagnostics Windows is installed, follow these steps to access it from HP Help and Support.

1. Select the **Start** button, and then select **HP Help and Support**.
2. Select **HP PC Hardware Diagnostics Windows**.
3. When the tool opens, select the type of diagnostic test that you want to run, and then follow the on-screen instructions.

NOTE: To stop a diagnostic test, select **Cancel**.

Accessing HP PC Hardware Diagnostics Windows from Support Assistant

After HP PC Hardware Diagnostics Windows is installed, follow these steps to access it from HP Support Assistant.

1. Type `support` in the taskbar search box, and then select the **HP Support Assistant** app.

   – or –

   Select the question mark icon in the taskbar.

2. Select **Troubleshooting and fixes**.
3. Select **Diagnostics**, and then select **HP PC Hardware Diagnostics Windows**.
4. When the tool opens, select the type of diagnostic test that you want to run, and then follow the on-screen instructions.

NOTE: To stop a diagnostic test, select **Cancel**.

Accessing HP PC Hardware Diagnostics Windows from the Start menu (select products only)

After HP PC Hardware Diagnostics Windows is installed, follow these steps to access it from the Start menu.

1. Select the **Start** button.
2. Right-click **HP PC Hardware Diagnostics for Windows**, select **More**, and then select **Run as administrator**.
3. When the tool opens, select the type of diagnostic test that you want to run, and then follow the on-screen instructions.

NOTE: To stop a diagnostic test, select **Cancel**.

Downloading HP PC Hardware Diagnostics Windows

The HP PC Hardware Diagnostics Windows downloading instructions are provided in English only. You must use a Windows computer to download this tool because only .exe files are provided.

Downloading the latest HP PC Hardware Diagnostics Windows version from HP

To download HP PC Hardware Diagnostics Windows from HP, follow these steps:

1. Go to http://www.hp.com/go/techcenter/pcdiags. The HP PC Diagnostics home page is displayed.
2. Select **Download HP Diagnostics Windows**, and then select the specific Windows diagnostics version to download to your computer or a USB flash drive.

The tool downloads to the selected location.

Downloading the HP PC Hardware Diagnostics Windows from the Microsoft Store

You can download the HP PC Hardware Diagnostics Windows from the Microsoft Store.

1. Select the Microsoft Store app on your desktop or enter `Microsoft Store` in the taskbar search box.
2. Enter `HP PC Hardware Diagnostics Windows` in the **Microsoft Store** search box.
3. Follow the on-screen directions.

The tool downloads to the selected location.

Downloading HP Hardware Diagnostics Windows by product name or number (select products only)

You can download HP PC Hardware Diagnostics Windows by product name or number.

NOTE: For some products, you might have to download the software to a USB flash drive by using the product name or number.

1. Go to http://www.hp.com/support.
2. Select **Software and Drivers**, select your type of product, and then enter the product name or number in the search box that is displayed.
3. In the **Diagnostics** section, select **Download**, and then follow the on-screen instructions to select the specific Windows diagnostics version to be downloaded to your computer or USB flash drive.

The tool downloads to the selected location.

Installing HP PC Hardware Diagnostics Windows

To install HP PC Hardware Diagnostics Windows, navigate to the folder on your computer or the USB flash drive where the .exe file downloaded, double-click the .exe file, and then follow the on-screen instructions.

Using HP PC Hardware Diagnostics UEFI

HP PC Hardware Diagnostics UEFI (Unified Extensible Firmware Interface) allows you to run diagnostic tests to determine whether the computer hardware is functioning properly. The tool runs outside the operating system so that it can isolate hardware failures from issues that are caused by the operating system or other software components.

NOTE: For Windows 10 S computers, you must use a Windows computer and a USB flash drive to download and create the HP UEFI support environment because only .exe files are provided. For more information, see Downloading HP PC Hardware Diagnostics UEFI to a USB flash drive on page 92.

If your PC does not start in Windows, you can use HP PC Hardware Diagnostics UEFI to diagnose hardware issues.

Using an HP PC Hardware Diagnostics UEFI hardware failure ID code

When HP PC Hardware Diagnostics UEFI detects a failure that requires hardware replacement, a 24-digit failure ID code is generated.

For assistance in solving the problem:

- Select **Contact HP**, accept the HP privacy disclaimer, and then use a mobile device to scan the failure ID code that appears on the next screen. The HP Customer Support - Service Center page appears with your failure ID and product number automatically filled in. Follow the on-screen instructions.

  – or –

  Contact support, and provide the failure ID code.

NOTE: To start diagnostics on a convertible computer, your computer must be in notebook mode, and you must use the attached keyboard.

NOTE: If you need to stop a diagnostic test, press esc.

Starting HP PC Hardware Diagnostics UEFI

To start HP PC Hardware Diagnostics UEFI, follow this procedure.

1. Turn on or restart the computer, and quickly press esc.
2. Press f2.

   The BIOS searches three places for the diagnostic tools, in the following order:

   a. Connected USB flash drive

   NOTE: To download the HP PC Hardware Diagnostics UEFI tool to a USB flash drive, see Downloading the latest HP PC Hardware Diagnostics UEFI version on page 92.

   b. Hard drive

   c. BIOS
3. When the diagnostic tool opens, select a language, select the type of diagnostic test you want to run, and then follow the on-screen instructions.

Downloading HP PC Hardware Diagnostics UEFI to a USB flash drive

Downloading HP PC Hardware Diagnostics UEFI to a USB flash drive can be useful in some situations.

- HP PC Hardware Diagnostics UEFI is not included in the preinstallation image.
- HP PC Hardware Diagnostics UEFI is not included in the HP Tool partition.
- The hard drive is damaged.

NOTE: The HP PC Hardware Diagnostics UEFI downloading instructions are provided in English only, and you must use a Windows computer to download and create the HP UEFI support environment because only .exe files are provided.

Downloading the latest HP PC Hardware Diagnostics UEFI version

To download the latest HP PC Hardware Diagnostics UEFI version to a USB flash drive, follow this procedure:

1. Go to http://www.hp.com/go/techcenter/pcdiags. The HP PC Diagnostics home page is displayed.
2. Select **Download HP Diagnostics UEFI**, and then select **Run**.

Downloading HP PC Hardware Diagnostics UEFI by product name or number (select products only)

You can download HP PC Hardware Diagnostics UEFI by product name or number (select products only) to a USB flash drive.

NOTE: For some products, you might have to download the software to a USB flash drive by using the product name or number.

1. Go to http://www.hp.com/support.
2. Enter the product name or number, select your computer, and then select your operating system.
3. In the **Diagnostics** section, follow the on-screen instructions to select and download the specific UEFI Diagnostics version for your computer.

Using Remote HP PC Hardware Diagnostics UEFI settings (select products only)

Remote HP PC Hardware Diagnostics UEFI is a firmware (BIOS) feature that downloads HP PC Hardware Diagnostics UEFI to your computer. It can then run the diagnostics on your computer, and it might upload results to a preconfigured server.

For more information about Remote HP PC Hardware Diagnostics UEFI, go to http://www.hp.com/go/techcenter/pcdiags, and then select **Find out more**.

Downloading Remote HP PC Hardware Diagnostics UEFI

HP Remote PC Hardware Diagnostics UEFI is also available as a SoftPaq that you can download to a server.

Downloading the latest Remote HP PC Hardware Diagnostics UEFI version

You can download the latest HP PC Hardware Diagnostics UEFI version to a USB flash drive.

1. Go to http://www.hp.com/go/techcenter/pcdiags. The HP PC Diagnostics home page is displayed.
2. Select **Download Remote Diagnostics**, and then select **Run**.

Downloading Remote HP PC Hardware Diagnostics UEFI by product name or number

You can download HP Remote PC Hardware Diagnostics UEFI by product name or number.

NOTE: For some products, you might have to download the software by using the product name or number.

1. Go to http://www.hp.com/support.
2. Select **Software and Drivers**, select your type of product, enter the product name or number in the search box that is displayed, select your computer, and then select your operating system.
3. In the **Diagnostics** section, follow the on-screen instructions to select and download the **Remote UEFI** version for the product.

Customizing Remote HP PC Hardware Diagnostics UEFI settings

Using the Remote HP PC Hardware Diagnostics setting in Computer Setup (BIOS), you can perform several customizations.

- Set a schedule for running diagnostics unattended. You can also start diagnostics immediately in interactive mode by selecting **Execute Remote HP PC Hardware Diagnostics**.
- Set the location for downloading the diagnostic tools. This feature provides access to the tools from the HP website or from a server that has been preconfigured for use. Your computer does not require the traditional local storage (such as a hard drive or USB flash drive) to run remote diagnostics.
- Set a location for storing the test results. You can also set the user name and password that you use for uploads.
- Display status information about the diagnostics run previously.

To customize Remote HP PC Hardware Diagnostics UEFI settings, follow these steps:

1. Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
2. Select **Advanced**, and then select **Settings**.
3. Make your customization selections.
4. Select **Main**, and then **Save Changes and Exit** to save your settings.

Your changes take effect when the computer restarts.

11 Statement of memory volatility

For general information regarding nonvolatile memory in HP business computers, and to restore nonvolatile memory that can contain personal data after the system has been turned off and the hard drive has been removed, use these instructions.

HP business computer products that use Intel®-based or AMD®-based system boards contain volatile DDR memory. The amount of nonvolatile memory present in the system depends upon the system configuration. Intel-based and AMD-based system boards contain nonvolatile memory subcomponents as originally shipped from HP, with the following assumptions:

- No subsequent modifications were made to the system.
- No applications, features, or functionality were added to or installed on the system.

Following system shutdown and removal of all power sources from an HP business computer system, personal data can remain on volatile system memory (DIMMs) for a finite period of time and also remains in nonvolatile memory. Use the following steps to remove personal data from the computer, including the nonvolatile memory found in Intel-based and AMD-based system boards.

NOTE: If your tablet has a keyboard base, connect to the keyboard base before beginning steps in this chapter.

Current BIOS steps

Use these instructions to restore nonvolatile memory.

1. Follow these steps to restore the nonvolatile memory that can contain personal data. Restoring or reprogramming nonvolatile memory that does not store personal data is neither necessary nor recommended.

   a. Turn on or restart the computer, and then quickly press esc.

   NOTE: If the system has a BIOS administrator password, type the password at the prompt.

   b. Select **Main**, select **Apply Factory Defaults and Exit**, and then select **Yes** to load defaults. The computer restarts.

   c. During the restart, press esc while the "Press the ESC key for Startup Menu" message is displayed at the bottom of the screen.

   NOTE: If the system has a BIOS administrator password, type the password at the prompt.

   d. Select the **Security** menu, select **Restore Security Settings to Factory Defaults**, and then select **Yes** to restore security level defaults. The computer reboots.

   e. During the reboot, press esc while the "Press the ESC key for Startup Menu" message is displayed at the bottom of the screen.

   NOTE: If the system has a BIOS administrator password, type the password at the prompt.

f. If an asset or ownership tag is set, select the **Security** menu and scroll down to the **Utilities** menu. Select **System IDs**, and then select **Asset Tracking Number**. Clear the tag, and then make the selection to return to the prior menu.

g. If a DriveLock password is set, select the **Security** menu, and scroll down to **Hard Drive Utilities** under the **Utilities** menu. Select **Hard Drive Utilities**, select **DriveLock**, and then clear the check box for **DriveLock password on restart**. Select **OK** to proceed.

h. Select the **Main** menu, and then select **Reset BIOS Security to factory default**. Select **Yes** at the warning message. The computer reboots.

i. During the reboot, press esc while the "Press the ESC key for Startup Menu" message is displayed at the bottom of the screen.

NOTE: If the system has a BIOS administrator password, type the password at the prompt.

j. Select the **Main** menu, select **Apply Factory Defaults and Exit**, select **Yes** to save changes and exit, and then select **Shutdown**.

k. Reboot the system. If the system has a Trusted Platform Module (TPM), fingerprint reader, or both, one or two prompts will appear—one to clear the TPM and the other to Reset Fingerprint Sensor. Press or tap f1 to accept or f2 to reject.

l. Remove all power and system batteries for at least 24 hours.

2. Complete one of the following:

- Remove and retain the storage drive.

  – or –

- Clear the drive contents by using a third-party utility designed to erase data from an SSD.

  – or –

- Clear the contents of the drive by using the following BIOS Setup Secure Erase command option steps:

NOTE: If you clear data using Secure Erase, you cannot recover it.

a. Turn on or restart the computer, and then quickly press esc.

b. Select the **Security** menu and scroll down to the esc menu.

c. Select **Hard Drive Utilities**.

d. Under **Utilities**, select **Secure Erase**, select the hard drive storing the data you want to clear, and then follow the on-screen instructions to continue.

   – or –

   Clear the contents of the drive using the following Disk Sanitizer commands steps:

   i. Turn on or restart the computer, and then quickly press esc.

   ii. Select the **Security** menu and scroll down to the **Utilities** menu.

   iii. Select **Hard Drive Utilities**.

iv. Under **Utilities**, select **Disk Sanitizer**, select the hard drive with the data that you want to clear, and then follow the on-screen instructions to continue.

NOTE: The amount of time it takes for Disk Sanitizer to run can take several hours. Plug the computer into an AC outlet before starting.

Nonvolatile memory usage

Use this table to troubleshoot nonvolatile memory usage.

Table 11-1 Troubleshooting steps for nonvolatile memory usage

Nonvolatile memory type	Amount (Size)	Does this memory store customer data?	Does this memory retain data when power is removed?	What is the purpose of this memory?	How is data entered into this memory?	How is this memory write-protected?
HP Sure Start flash (select models only)	8 MB	No	Yes	Provides protected backup of critical System BIOS code, EC firmware, and critical computer configuration data for select platforms that support HP Sure Start. For more information, see Using HP Sure Start (select products only) on page 101.	Data cannot be written to this device via the host processor. The content is managed solely by the HP Sure Start Embedded Controller.	This memory is protected by the HP Sure Start Embedded Controller.
Real Time Clock (RTC) battery backed-up CMOS configuration memory	256 bytes	No	Yes	Stores system date and time and noncritical data.	RTC battery backed-up CMOS is programmed using Computer Setup (BIOS), or by changing the Windows date & time.	This memory is not write-protected.
Controller (NIC) EEPROM	64 KB (not customer accessible)	No	Yes	Stores NIC configuration and NIC firmware.	NIC EEPROM is programmed using a utility from the NIC vendor that can be run from DOS.	A utility must be used to write data to this memory and is available from the NIC vendor. Writing data to this ROM in an inappropriate manner will render the NIC nonfunctional.

Table 11-1 Troubleshooting steps for nonvolatile memory usage (continued)

Nonvolatile memory type	Amount (Size)	Does this memory store customer data?	Does this memory retain data when power is removed?	What is the purpose of this memory?	How is data entered into this memory?	How is this memory write-protected?
DIMM Serial Presence Detect (SPD) configuration data	256 bytes per memory module, 128 bytes programmable (not customer accessible)	No	Yes	Stores memory module information.	DIMM SPD is programmed by the memory vendor.	Data cannot be written to this memory when the module is installed in a computer. The specific write-protection method varies by memory vendor.
System BIOS	9 MB	Yes	Yes	Stores system BIOS code and computer configuration data.	System BIOS code is programmed at the factory. Code is updated when the system BIOS is updated. Configuration data and settings are entered using the Computer Setup (BIOS) or a custom utility.	NOTE: Writing data to this ROM in an inappropriate manner can render the computer nonfunctional. A utility must be used for writing data to this memory and is available on the HP website; go to http://www.hp.com/support. Select **Find your product**, and then follow the on-screen instructions.
Intel Management Engine Firmware (present only in select Elite or Z models. For more information, go to http://www.hp.com/support. Select **Identify your product for manuals and specific product information**, and then follow the on-screen instructions.)	1.5 MB or 7 MB	Yes	Yes	Stores Management Engine Code, Settings, Provisioning Data and iAMT third-party data store.	Management Engine Code is programmed at the factory. Code is updated via Intel secure firmware update utility. Unique Provisioning Data can be entered at the factory or by an administrator using the Management Engine (MEBx) setup utility. The third-party data store contents can be populated by a remote management console or local applications that have been registered by an administrator to have access to the space.	The Intel chipset is configured to enforce hardware protection to block all direct read-write access to this area. An Intel utility must be used for updating the firmware. Only firmware updates digitally signed by Intel can be applied using this utility.
Bluetooth flash (select products only)	2 megabits	No	Yes	Stores Bluetooth configuration and firmware.	Bluetooth flash is programmed at the factory. Tools for writing data to this memory are not publicly available but can be obtained from the silicon vendor.	A utility must be used for writing data to this memory and is made available through newer versions of the driver whenever the flash requires an upgrade.

Table 11-1 Troubleshooting steps for nonvolatile memory usage (continued)

Nonvolatile memory type	Amount (Size)	Does this memory store customer data?	Does this memory retain data when power is removed?	What is the purpose of this memory?	How is data entered into this memory?	How is this memory write-protected?
802.11 WLAN EEPROM	4 kilobits to 8 kilobits	No	Yes	Stores configuration and calibration data.	802.11 WLAN EEPROM is programmed at the factory. Tools for writing data to this memory are not made public.	A utility must be used for writing data to this memory and is typically not made available to the public unless a firmware upgrade is necessary to address a unique issue.
Camera (select products only)	64 kilobits	No	Yes	Stores camera configuration and firmware.	Camera memory is programmed using a utility from the device manufacturer that can be run from Windows.	A utility must be used for writing data to this memory and is typically not made available to the public unless a firmware upgrade is necessary to address a unique issue.
Fingerprint reader (select products only)	512 KB flash	Yes	Yes	Stores fingerprint templates.	Fingerprint reader memory is programmed by user enrollment in HP ProtectTools Security Manager.	Only a digitally signed application can make the call to write to the flash.

Questions and answers

Use this section to answer your questions about nonvolatile memory.

1. **How can the BIOS settings be restored (returned to factory settings)?**

IMPORTANT: The restore defaults feature does not securely erase any information on your hard drive. See question and answer 6 for steps to securely erase information.

The restore defaults feature does not reset the Custom Secure Boot keys. See question and answer 7 for information about resetting the keys.

a. Turn on or restart the computer, and then quickly press esc.

b. Select **Main**, and then select **Apply Factory Defaults and Exit**.

c. Follow the on-screen instructions.

d. Select **Main**, select **Save Changes and Exit**, and then follow the on-screen instructions.

2. **What is a UEFI BIOS, and how is it different from a legacy BIOS?**

The Unified Extensible Firmware Interface (UEFI) BIOS is an industry-standard software interface between the platform firmware and an operating system (OS). It replaces the older BIOS architecture but supports much of the legacy BIOS functionality.

Like the legacy BIOS, the UEFI BIOS provides an interface to display the system information and configuration settings and to change the configuration of your computer before an OS is loaded. BIOS provides a secure runtime environment that supports a Graphic User Interface (GUI). In this environment, you can use either a pointing device (touch screen, touchpad, pointing stick, or USB mouse) or the keyboard to navigate and make menu and configuration selections. The UEFI BIOS also contains basic system diagnostics.

The UEFI BIOS provides functionality beyond that of the legacy BIOS. In addition, the UEFI BIOS works to initialize the computer's hardware before loading and executing the OS; the runtime environment allows the loading and execution of software programs from storage devices to provide more functionality, such as advanced hardware diagnostics (with the ability to display more detailed system information) and advanced firmware management and recovery software.

HP has provided options in Computer Setup (BIOS) to allow you to run in legacy BIOS, if required by the operating system. Examples of this requirement would be if you upgrade or downgrade the OS.

3. **Where is the UEFI BIOS located?**

   The UEFI BIOS is located on a flash memory chip. You must use a utility to write to the chip.

4. **What kind of configuration data is stored on the DIMM Serial Presence Detect (SPD) memory module? How would this data be written?**

   The DIMM SPD memory contains information about the memory module, such as size, serial number, data width, speed and timing, voltage, and thermal information. This information is written by the module manufacturer and stored on an EEPROM. You cannot write to this EEPROM when the memory module is installed in a computer. Third-party tools do exist that can write to the EEPROM when the memory module is not installed in a computer. Various third-party tools are available to read SPD memory.

5. **What is meant by "Restore the nonvolatile memory found in Intel-based system boards"?**

   This message relates to clearing the Real Time Clock (RTC) CMOS memory that contains computer configuration data.

6. **How can the BIOS security be reset to factory defaults and erase the data?**

   IMPORTANT: Resetting results in the loss of information.

   These steps do not reset Custom Secure Boot Keys. See question and answer 7 for information about resetting the keys.

   a. Turn on or restart the computer, and then quickly press esc.

   b. Select **Main**, and then select **Reset Security to Factory Defaults**.

   c. Follow the on-screen instructions.

   d. Select **Main**, select **Save Changes and Exit**, and then follow the on-screen instructions.

7. **How can the Custom Secure Boot Keys be reset?**

   Secure Boot is a feature to ensure that only authenticated code can start on a platform. If you enabled Secure Boot and created Custom Secure Boot Keys, disabling Secure Boot does not clear the keys. You must also select to clear the Custom Secure Boot Keys. Use the same Secure Boot access procedure that you used to create the Custom Secure Boot Keys, but select to clear or delete all Secure Boot Keys.

   a. Turn on or restart the computer, and then quickly press esc.

b. Select the **Security** menu, select **Secure Boot Configuration**, and then follow the on-screen instructions.

c. At the **Secure Boot Configuration** window, select **Secure Boot**, select **Clear Secure Boot Keys**, and then follow the on-screen instructions to continue.

Using HP Sure Start (select products only)

Select computer models are configured with HP Sure Start, a technology that continuously monitors your computer's BIOS for attacks or corruption.

If the BIOS becomes corrupted or is attacked, HP Sure Start restores the BIOS to its previously safe state, without user intervention. Those select computer models ship with HP Sure Start configured and enabled. HP Sure Start is configured and already enabled so that most users can use the HP Sure Start default configuration. Advanced users can customize the default configuration.

To access the latest documentation on HP Sure Start, go to http://www.hp.com/support.

12 Power cord set requirements

The power supplies on some computers have external power switches.

The voltage select switch feature on the computer permits it to operate from any line voltage of 100 V ac to 120 V ac or 220 V ac to 240 V ac. Power supplies on those computers that do not have external power switches are equipped with internal switches that sense the incoming voltage and automatically switch to the proper voltage.

The power cord set received with the computer meets the requirements for use in the country where you purchased the equipment.

Power cord sets for use in other countries must meet the requirements of the country where you use the computer.

General requirements

These requirements are applicable to all countries.

1. The power cord must be approved by an acceptable accredited agency responsible for evaluation in the country where the power cord set will be installed.
2. The power cord set must have a minimum current capacity of 10A (7A Japan only) and a nominal voltage rating of 125 V ac or 250 V ac, as required by each country's power system.
3. The diameter of the wire must be a minimum of 0.75 mm^2 or 18AWG, and the length of the cord must be between 1.8 m (6 ft) and 3.6 m (12 ft).

The power cord should be routed so that it is not likely to be walked on or pinched by items placed upon it or against it. Particular attention should be paid to the plug, electrical outlet, and the point where the cord exits from the product.

⚠ **WARNING!** Do not operate this product with a damaged power cord set. If the power cord set is damaged in any manner, replace it immediately.

Japanese power cord requirements

For use in Japan, use only the power cord received with this product.

IMPORTANT: Do not use the power cord received with this product on any other products.

Country-specific requirements

This information provides additional requirements specific to a country.

Table 12-1 **Power cord country-specific requirements**

Country	Accrediting Agency	Country	Accrediting Agency
Australia (1)	EANSW	Italy (1)	IMQ
Austria (1)	OVE	Japan (3)	METI
Belgium (1)	CEBC	Norway (1)	NEMKO
Canada (2)	CSA	Sweden (1)	SEMKO
Denmark (1)	DEMKO	Switzerland (1)	SEV
Finland (1)	SETI	United Kingdom (1)	BSI
France (1)	UTE	United States (2)	UL
Germany (1)	VDE		

1. The flexible cord must be Type HO5VV-F, 3-conductor, 0.75mm^2 conductor size. Power cord set fittings (appliance coupler and plug) must bear the certification mark of the agency responsible for evaluation in the country where it will be used.
2. The flexible cord must be Type SVT or equivalent, No. 18 AWG, 3 conductor. The plug must be a 2-pole grounding type with a NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
3. Appliance coupler, flexible cord, and plug must bear a T mark and registration number in accordance with the Japanese Dentori Law. Flexible cord must be Type VCT or VCTF, 3-conductor, 0.75 mm^2 conductor size. Plug must be a 2-pole grounding type with a Japanese Industrial Standard C8303 (7 A, 125 V) configuration.

13 Specifications

This section provides specifications for your computer.

Table 13-1 Specifications

	Metric	U.S.
Dimensions		
Height	10 mm	0.39 in
Width	240 mm	9.45 in
Depth	176 mm	6.93 in
Approximate weight	725.8 g	1.6 lb
Temperature range		
Operating	10°C to 35°C	50°F to 95°F
Nonoperating	-30°C to 60°C	-22°F to 140°F
NOTE: Operating temperature is derated 1.0°C per 300 m (1000 ft) to 3000 m (10,000 ft) above sea level; no direct sustained sunlight. Maximum rate of change is 10°C/Hr. The upper limit might be limited by the type and number of options installed.		
Maximum altitude (unpressurized)		
Operating	3,048 m	10,000 ft
Nonoperating	9,144 m	30,000 ft
Relative humidity (noncondensing)		
Operating	10% to 90%	
Nonoperating (38.7°C max wet bulb)	5% to 95%	
Power supply		
Operating voltage range	90 V ac to 264 V ac	
Rated voltage range[1]	100 V ac to 240 V ac	
Rated line frequency	50 Hz to 60 Hz	
Operating line frequency	47 Hz to 63 Hz	

[1] This system uses an active power factor-corrected power supply. This allows the system to pass the CE mark requirements for use in the countries of the European Union. The active power factor-corrected power supply also has the added benefit of not requiring an input-voltage range select switch.

Index

U

V

W