

# XPS 13 9315 / XPS 9315

## Service Manual



## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

<b>Chapter 1: Working inside your computer</b> .....	<b>5</b>
Safety instructions.....	5
Before working inside your computer.....	5
Safety precautions.....	6
Electrostatic discharge—ESD protection.....	6
ESD field service kit .....	7
Transporting sensitive components.....	8
After working inside your computer.....	8
<b>Chapter 2: Removing and installing components</b> .....	<b>9</b>
Recommended tools.....	9
Screw list.....	9
Major components of XPS 13 9315.....	10
Base cover.....	12
Removing the base cover.....	12
Installing the base cover.....	14
Battery.....	16
Lithium-ion battery precautions.....	16
Removing the battery.....	16
Installing the battery.....	17
Fan.....	18
Removing the fan.....	18
Installing the fan.....	19
Heat sink.....	21
Removing the heat sink.....	21
Installing the heat sink.....	21
Display assembly.....	22
Removing the display assembly.....	22
Installing the display assembly.....	25
I/O daughter-board.....	28
Removing the I/O daughter-board.....	28
Installing the I/O daughter-board.....	30
System board.....	31
Removing the system board.....	31
Installing the system board.....	33
Palm-rest and keyboard assembly.....	36
Removing the palm-rest and keyboard assembly.....	36
Installing the palm-rest and keyboard assembly.....	36
<b>Chapter 3: Drivers and downloads</b> .....	<b>38</b>
<b>Chapter 4: System setup</b> .....	<b>39</b>
Entering BIOS setup program.....	39
Navigation keys.....	39











Boot Sequence.....	39
One time boot menu.....	40
System setup options.....	40
System and setup password.....	56
Assigning a system setup password.....	56
Deleting or changing an existing system setup password.....	57
Clearing BIOS (System Setup) and System passwords.....	57
Updating the BIOS.....	57
Updating the BIOS in Windows.....	57
Updating the BIOS using the USB drive in Windows.....	58
Updating the BIOS in Linux and Ubuntu.....	58
Updating the BIOS from the F12 One-Time boot menu.....	58
<b>Chapter 5: Troubleshooting.....</b>	<b>60</b>
Handling swollen Lithium-ion batteries.....	60
<b>Locate the Service Tag or Express Service Code of your Dell computer .....</b>	<b>60</b>
System diagnostic lights.....	61
SupportAssist diagnostics.....	61
Built-in self-test (BIST).....	62
M-BIST.....	62
LCD Built-in Self Test (BIST).....	62
Recovering the operating system.....	63
WiFi power cycle.....	63
Drain residual flea power (perform hard reset).....	63
Backup media and recovery options.....	64
Real Time Clock—RTC reset.....	64
<b>Chapter 6: Getting help and contacting Dell.....</b>	<b>65</b>



# Working inside your computer



## Safety instructions

Use the following safety guidelines to protect your computer from potential damage and to ensure your personal safety. Unless otherwise noted, each procedure included in this document assumes that you have read the safety information that shipped with your computer.

-  **WARNING:** Before working inside your computer, read the safety information that is shipped with your computer. For more safety best practices, see the Regulatory Compliance home page at [www.dell.com/regulatory\\_compliance](http://www.dell.com/regulatory_compliance).
-  **WARNING:** Disconnect your computer from all power sources before opening the computer cover or panels. After you finish working inside the computer, replace all covers, panels, and screws before connecting your computer to an electrical outlet.
-  **CAUTION:** To avoid damaging the computer, ensure that the work surface is flat, dry, and clean.
-  **CAUTION:** To avoid damaging the components and cards, handle them by their edges, and avoid touching the pins and the contacts.
-  **CAUTION:** You should only perform troubleshooting and repairs as authorized or directed by the Dell technical assistance team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. See the safety instructions that is shipped with the product or at [www.dell.com/regulatory\\_compliance](http://www.dell.com/regulatory_compliance).
-  **CAUTION:** Before touching anything inside your computer, ground yourself by touching an unpainted metal surface, such as the metal at the back of the computer. While you work, periodically touch an unpainted metal surface to dissipate static electricity which could harm internal components.
-  **CAUTION:** When you disconnect a cable, pull it by its connector or its pull tab, not the cable itself. Some cables have connectors with locking tabs or thumbscrews that you must disengage before disconnecting the cable. When disconnecting cables, keep them evenly aligned to avoid bending the connector pins. When connecting cables, ensure that the ports and the connectors are correctly oriented and aligned.
-  **CAUTION:** Press and eject any installed card from the media-card reader.
-  **CAUTION:** Exercise caution when handling Lithium-ion batteries in laptops. Swollen batteries should not be used and should be replaced and disposed properly.
-  **NOTE:** The color of your computer and certain components may appear differently than shown in this document.

## Before working inside your computer

### Steps

1. Save and close all open files and exit all open applications.
2. Shut down your computer. For Windows operating system, click **Start** >  **Power** > **Shut down**.
  -  **NOTE:** If you are using a different operating system, see the documentation of your operating system for shut-down instructions.
3. Disconnect your computer and all attached devices from their electrical outlets.
4. Disconnect all attached network devices and peripherals, such as keyboard, mouse, and monitor from your computer.

5. Remove any media card and optical disk from your computer, if applicable.
6. Enter the service mode, if you are able to power on your computer.

### Service Mode

Service Mode is used to cut-off power, without disconnecting battery cable from system board prior conducting repairs in the computer.

**CAUTION:** If you are unable to turn on the computer to put it into Service Mode or the computer does not support Service Mode then proceed to disconnect the battery cable. To disconnect the battery cable, follow the steps in [Removing the battery](#).

**NOTE:** Ensure that your computer is shut down and the AC adapter is disconnected.

- a. Hold **<B>** key on the keyboard and press the power button for 3 seconds or until the Dell logo appears on the screen.
- b. Press any key to continue.
- c. If the AC adapter is not disconnected, a message prompting you to remove the AC adapter appears on the screen. Remove the AC adapter and then press any key to continue the **Service Mode** procedure. The **Service Mode** procedure automatically skips the following step if the **Owner Tag** of the computer is not set up in advance by the user.
- d. When the ready-to-proceed message appears on the screen, press any key to proceed. The computer emits three short beeps and shuts down immediately.
- e. Once the computer shuts down, it has successfully entered Service Mode.

**NOTE:** If you are unable to power on your computer or unable to enter service mode skip this process.

## Safety precautions

The safety precautions chapter details the primary steps to be taken before performing any disassembly instructions.

Observe the following safety precautions before you perform any installation or break/fix procedures involving disassembly or reassembly:

- Turn off the system and all attached peripherals.
- Disconnect the system and all attached peripherals from AC power.
- Disconnect all network cables, telephone, and telecommunications lines from the system.
- Use an ESD field service kit when working inside any to avoid electrostatic discharge (ESD) damage.
- After removing any system component, carefully place the removed component on an anti-static mat.
- Wear shoes with non-conductive rubber soles to reduce the chance of getting electrocuted.

## Standby power

Dell products with standby power must be unplugged before you open the case. Systems that incorporate standby power are essentially powered while turned off. The internal power enables the system to be remotely turned on (wake on LAN) and suspended into a sleep mode and has other advanced power management features.

Unplugging, pressing and holding the power button for 15 seconds should discharge residual power in the system board.

## Bonding

Bonding is a method for connecting two or more grounding conductors to the same electrical potential. This is done through the use of a field service electrostatic discharge (ESD) kit. When connecting a bonding wire, ensure that it is connected to bare metal and never to a painted or non-metal surface. The wrist strap should be secure and in full contact with your skin, and ensure that you remove all jewelry such as watches, bracelets, or rings prior to bonding yourself and the equipment.

## Electrostatic discharge—ESD protection

ESD is a major concern when you handle electronic components, especially sensitive components such as expansion cards, processors, memory DIMMs, and system boards. Very slight charges can damage circuits in ways that may not be obvious, such as intermittent problems or a shortened product life span. As the industry pushes for lower power requirements and increased density, ESD protection is an increasing concern.

Due to the increased density of semiconductors used in recent Dell products, the sensitivity to static damage is now higher than in previous Dell products. For this reason, some previously approved methods of handling parts are no longer applicable.

Two recognized types of ESD damage are catastrophic and intermittent failures.

- **Catastrophic** – Catastrophic failures represent approximately 20 percent of ESD-related failures. The damage causes an immediate and complete loss of device functionality. An example of catastrophic failure is a memory DIMM that has received a static shock and immediately generates a "No POST/No Video" symptom with a beep code emitted for missing or nonfunctional memory.
- **Intermittent** – Intermittent failures represent approximately 80 percent of ESD-related failures. The high rate of intermittent failures means that most of the time when damage occurs, it is not immediately recognizable. The DIMM receives a static shock, but the tracing is merely weakened and does not immediately produce outward symptoms related to the damage. The weakened trace may take weeks or months to melt, and in the meantime may cause degradation of memory integrity, intermittent memory errors, etc.

The more difficult type of damage to recognize and troubleshoot is the intermittent (also called latent or "walking wounded") failure.

Perform the following steps to prevent ESD damage:

- Use a wired ESD wrist strap that is properly grounded. The use of wireless anti-static straps is no longer allowed; they do not provide adequate protection. Touching the chassis before handling parts does not ensure adequate ESD protection on parts with increased sensitivity to ESD damage.
- Handle all static-sensitive components in a static-safe area. If possible, use anti-static floor pads and workbench pads.
- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the anti-static packing material until you are ready to install the component. Before unwrapping the anti-static packaging, ensure that you discharge static electricity from your body.
- Before transporting a static-sensitive component, place it in an anti-static container or packaging.

## ESD field service kit

The unmonitored Field Service kit is the most commonly used service kit. Each Field Service kit includes three main components: anti-static mat, wrist strap, and bonding wire.

### Components of an ESD field service kit

The components of an ESD field service kit are:

- **Anti-Static Mat** – The anti-static mat is dissipative and parts can be placed on it during service procedures. When using an anti-static mat, your wrist strap should be snug and the bonding wire should be connected to the mat and to any bare metal on the system being worked on. Once deployed properly, service parts can be removed from the ESD bag and placed directly on the mat. ESD-sensitive items are safe in your hand, on the ESD mat, in the system, or inside a bag.
- **Wrist Strap and Bonding Wire** – The wrist strap and bonding wire can be either directly connected between your wrist and bare metal on the hardware if the ESD mat is not required, or connected to the anti-static mat to protect hardware that is temporarily placed on the mat. The physical connection of the wrist strap and bonding wire between your skin, the ESD mat, and the hardware is known as bonding. Use only Field Service kits with a wrist strap, mat, and bonding wire. Never use wireless wrist straps. Always be aware that the internal wires of a wrist strap are prone to damage from normal wear and tear, and must be checked regularly with a wrist strap tester in order to avoid accidental ESD hardware damage. It is recommended to test the wrist strap and bonding wire at least once per week.
- **ESD Wrist Strap Tester** – The wires inside of an ESD strap are prone to damage over time. When using an unmonitored kit, it is a best practice to regularly test the strap prior to each service call, and at a minimum, test once per week. A wrist strap tester is the best method for doing this test. If you do not have your own wrist strap tester, check with your regional office to find out if they have one. To perform the test, plug the wrist-strap's bonding-wire into the tester while it is strapped to your wrist and push the button to test. A green LED is lit if the test is successful; a red LED is lit and an alarm sounds if the test fails.
- **Insulator Elements** – It is critical to keep ESD sensitive devices, such as plastic heat sink casings, away from internal parts that are insulators and often highly charged.
- **Working Environment** – Before deploying the ESD Field Service kit, assess the situation at the customer location. For example, deploying the kit for a server environment is different than for a desktop or portable environment. Servers are typically installed in a rack within a data center; desktops or portables are typically placed on office desks or cubicles. Always look for a large open flat work area that is free of clutter and large enough to deploy the ESD kit with additional space to accommodate the type of system that is being repaired. The workspace should also be free of insulators that can cause an ESD event. On the work area, insulators such as Styrofoam and other plastics should always be moved at least 12 inches or 30 centimeters away from sensitive parts before physically handling any hardware components

- **ESD Packaging** – All ESD-sensitive devices must be shipped and received in static-safe packaging. Metal, static-shielded bags are preferred. However, you should always return the damaged part using the same ESD bag and packaging that the new part arrived in. The ESD bag should be folded over and taped shut and all the same foam packing material should be used in the original box that the new part arrived in. ESD-sensitive devices should be removed from packaging only at an ESD-protected work surface, and parts should never be placed on top of the ESD bag because only the inside of the bag is shielded. Always place parts in your hand, on the ESD mat, in the system, or inside an anti-static bag.
- **Transporting Sensitive Components** – When transporting ESD sensitive components such as replacement parts or parts to be returned to Dell, it is critical to place these parts in anti-static bags for safe transport.

## ESD protection summary

It is recommended that all field service technicians use the traditional wired ESD grounding wrist strap and protective anti-static mat at all times when servicing Dell products. In addition, it is critical that technicians keep sensitive parts separate from all insulator parts while performing service and that they use anti-static bags for transporting sensitive components.

## Transporting sensitive components

When transporting ESD sensitive components such as replacement parts or parts to be returned to Dell, it is critical to place these parts in anti-static bags for safe transport.

## After working inside your computer

### About this task

 **CAUTION:** Leaving stray or loose screws inside your computer may severely damage your computer.

### Steps

1. Replace all screws and ensure that no stray screws remain inside your computer.
2. Connect any external devices, peripherals, or cables you removed before working on your computer.
3. Replace any media cards, discs, or any other parts that you removed before working on your computer.
4. Connect your computer and all attached devices to their electrical outlets.
  - ① **NOTE:** To exit service mode, ensure to connect the AC adapter to the power-adaptor port on your computer.
5. Press the power button to turn on the computer. Your computer will automatically return to normal functioning mode.

# Removing and installing components

**NOTE:** The images in this document may differ from your computer depending on the configuration you ordered.

## Recommended tools

The procedures in this document may require the following tools:

- Phillips screwdriver #0
- Phillips screwdriver #1
- Torx #5 (T5) screwdriver









## Screw list

**NOTE:** When removing screws from a component, it is recommended to note the screw type, the quantity of screws, and then place them in a screw storage box. This is to ensure that the correct number of screws and correct screw type is restored when the component is replaced.






**NOTE:** Some computers have magnetic surfaces. Ensure that the screws are not left attached to such surfaces when replacing a component.

**NOTE:** Screw color may vary with the configuration ordered.

**Table 1. Screw list**

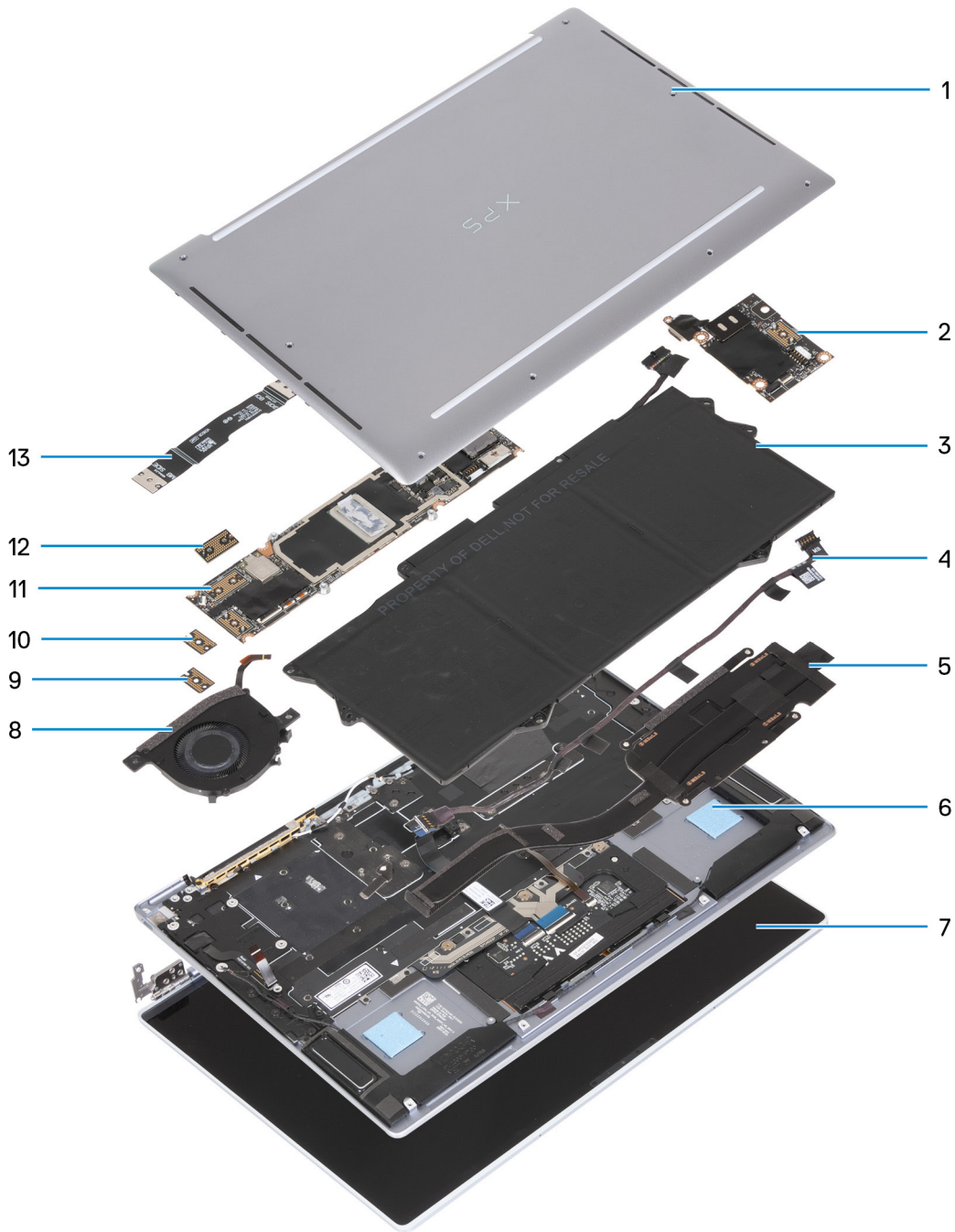
Component	Secured to	Screw type	Quantity	Screw image
Base cover	Palm-rest and keyboard assembly	M2x3, Torx 5	8	
Battery	Palm-rest and keyboard assembly	M2x3	8	
Fan	System board	M1.6x2.5	2	
Heat sink	System board	M2x3	4	
Display-assembly cable brackets	System board	M1.6x2.3	4	
Camera and display-assembly cable	System board	M1.6x3.5	2	
Display-assembly hinges	Palm-rest and keyboard assembly	M2.5x4.3	6	
Display-assembly hinges	Palm-rest and keyboard assembly	M1.6x3	2	

**Table 1. Screw list (continued)**

<b>Component</b>	<b>Secured to</b>	<b>Screw type</b>	<b>Quantity</b>	<b>Screw image</b>
Display-assembly hinges	Palm-rest and keyboard assembly	M1.6x2.5	2	
Wireless-card bracket	System board	M1.6x2.3	1	
System board	Palm-rest and keyboard assembly	M1.6x2.8	1	
System board	Palm-rest and keyboard assembly	M1.6x1.5	5	
System board	Palm-rest and keyboard assembly	M1.6x2.3	1	

## Major components of XPS 13 9315

The following image shows the major components of XPS 13 9315.



1. Base cover
2. I/O daughter-board
3. Battery
4. I/O daughter-board power cable
5. Heat sink
6. Palm-rest and keyboard assembly
7. Display assembly
8. Fan
9. I/O daughter-board interposer board
10. System-board interposer board
11. System board
12. Display-assembly interposer board
13. I/O daughter-board cable



**NOTE:** Dell provides a list of components and their part numbers for the original system configuration purchased. These parts are available according to warranty coverages purchased by the customer. Contact your Dell sales representative for purchase options.

## Base cover

### Removing the base cover

#### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).

**NOTE:** Ensure that your computer is in Service Mode. For more information, see Step 6 in [Before working inside your computer](#).

#### About this task

The following image(s) indicate the location of the base cover and provides a visual representation of the removal procedure.



**8x**  
M2x3, Torx 5







## Steps

1. Remove the eight screws (M2x3, Torx 5) that secure the base cover to the palm-rest and keyboard assembly.

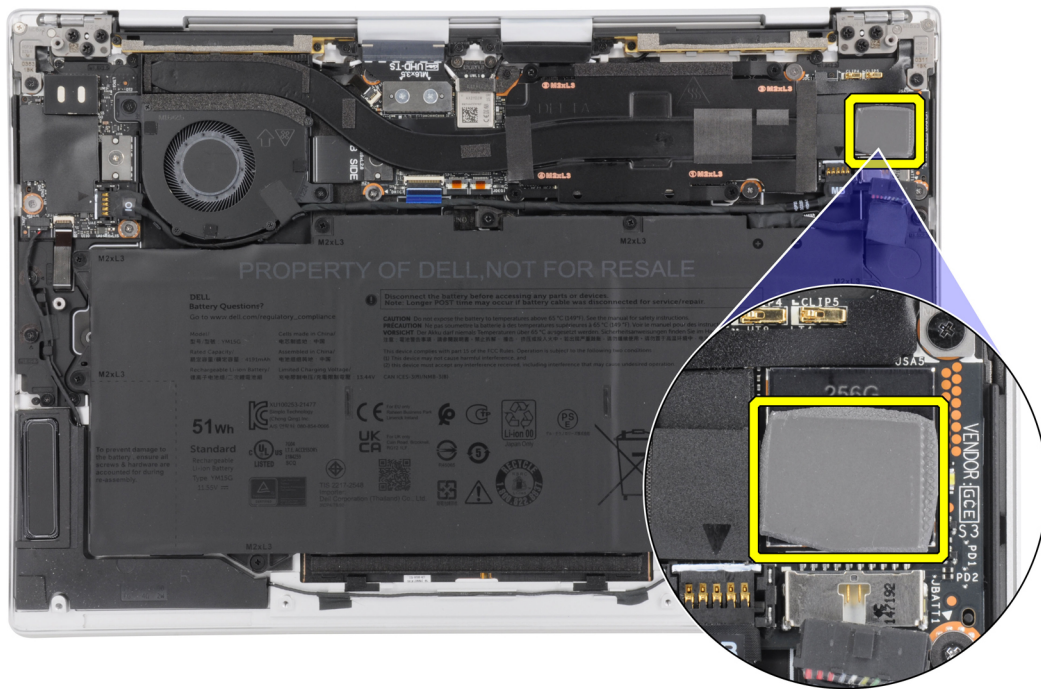
**(i) NOTE:** A Torx #5 (T5) screwdriver is necessary to remove the six screws (M2x3, Torx 5).

2. Place your thumbs and fingers into the recess at the top edge of the base cover.
3. Hold the top side of the base cover and push the base cover slightly to the rear of the computer.

**(i) NOTE:** This action releases the base cover from the hooks that are on the palm-rest and keyboard assembly.

**(i) NOTE:** Do not pull on or pry the base cover from where the display assembly hinges are, doing so may damage the base cover.

4. Lift the base cover off the palm-rest and keyboard assembly.
5. If the thermal pad that covers the BGA solid-state drive is dislodged after the base cover is removed, replace the thermal pad to its original position.



## Installing the base cover

### Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

### About this task

The following image(s) indicate the location of the base cover and provides a visual representation of the installation procedure.



**8x**  
M2x3, Torx 5



## Steps

1. Place and snap the base cover into place on the palm-rest and keyboard assembly.  
**i** **NOTE:** Align the screw holes on the base cover with the screw holes on the palm-rest and keyboard assembly before applying slight pressure to the base cover.
2. Replace the eight screws (M2x3, Torx 5) that secure the base cover to the palm-rest and keyboard assembly.  
**i** **NOTE:** A Torx #5 (T5) screwdriver is necessary to install the six screws (M2x3, Torx 5).

## Next steps

1. Follow the procedure in [After working inside your computer](#).

# Battery

## Lithium-ion battery precautions

### CAUTION:

- Exercise caution when handling Lithium-ion batteries.
- Discharge the battery completely before removing it. Disconnect the AC power adapter from the system and operate the computer solely on battery power—the battery is fully discharged when the computer no longer turns on when the power button is pressed.
- Do not crush, drop, mutilate, or penetrate the battery with foreign objects.
- Do not expose the battery to high temperatures, or disassemble battery packs and cells.
- Do not apply pressure to the surface of the battery.
- Do not bend the battery.
- Do not use tools of any kind to pry on or against the battery.
- Ensure any screws during the servicing of this product are not lost or misplaced, to prevent accidental puncture or damage to the battery and other system components.
- If the battery gets stuck inside your computer as a result of swelling, do not try to release it as puncturing, bending, or crushing a lithium-ion battery can be dangerous. In such an instance, contact Dell technical support for assistance. See [www.dell.com/contactdell](http://www.dell.com/contactdell).
- Always purchase genuine batteries from [www.dell.com](http://www.dell.com) or authorized Dell partners and resellers.
- Swollen batteries should not be used and should be replaced and disposed properly. For guidelines on how to handle and replace swollen Lithium-ion batteries, see [Handling swollen Lithium-ion batteries](#).

## Removing the battery

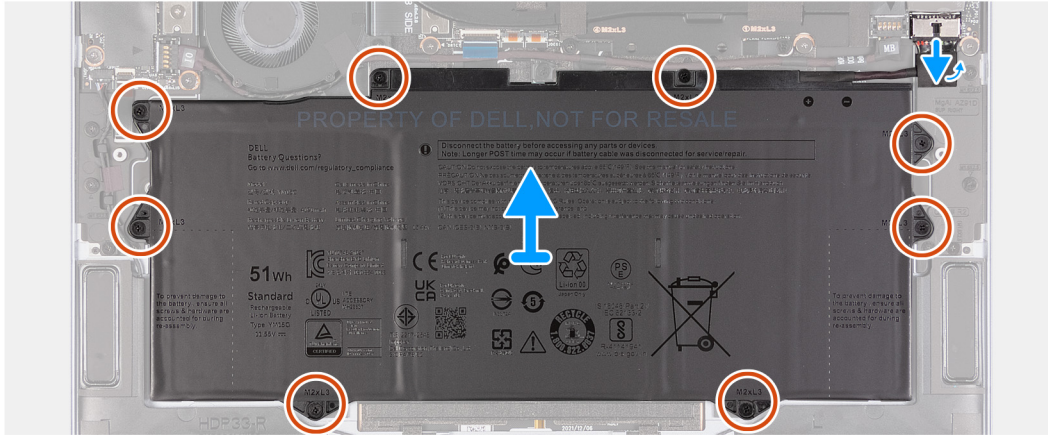
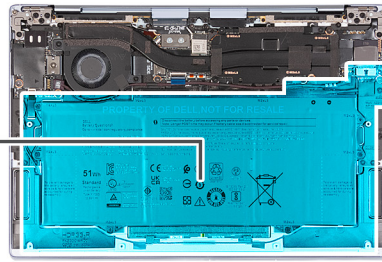
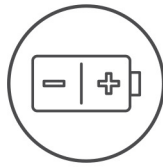
### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).

### About this task

The following image indicates the location of the battery and provides a visual representation of the removal procedure.





### Steps

1. Use the pull tab on the battery power cable to disconnect the battery cable from the battery connector.
2. Remove the eight screws (M1.6x2.5) that secure the battery to the palm-rest and keyboard assembly.
3. Lift the battery off the palm-rest and keyboard assembly.

## Installing the battery

### Prerequisites

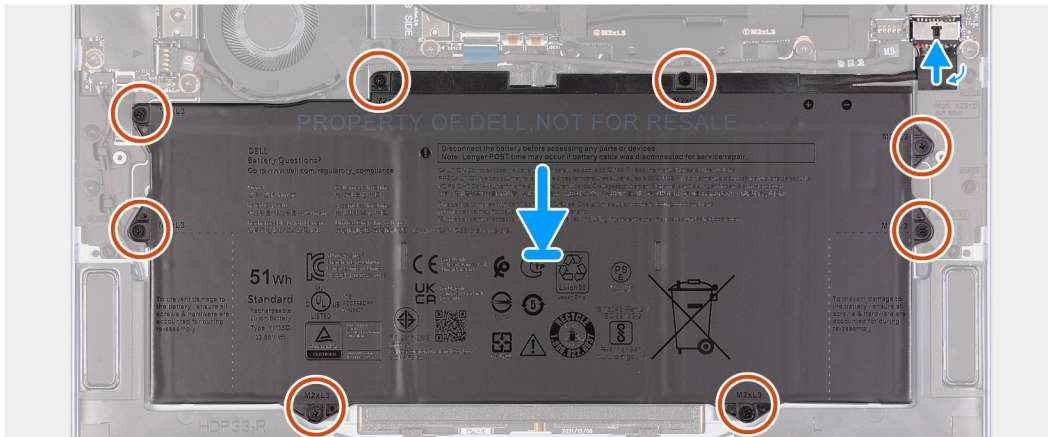
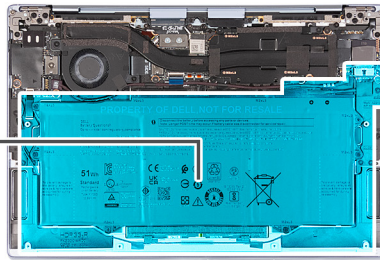
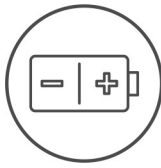
If you are replacing a component, remove the existing component before performing the installation process.

### About this task

The following image indicates the location of the battery and provides a visual representation of the installation procedure.



8x  
M2x3



### Steps

1. Align the screw holes of the battery with the screw holes on the palm-rest and keyboard assembly.
2. Place the battery on the palm-rest and keyboard assembly.
3. Replace the eight screws (M1.6x2.5) that secure the battery to the palm-rest and keyboard assembly.
4. Connect the battery cable to the system board.

### Next steps

1. Install the [base cover](#).
2. Follow the procedure in [After working inside your computer](#).

## Fan

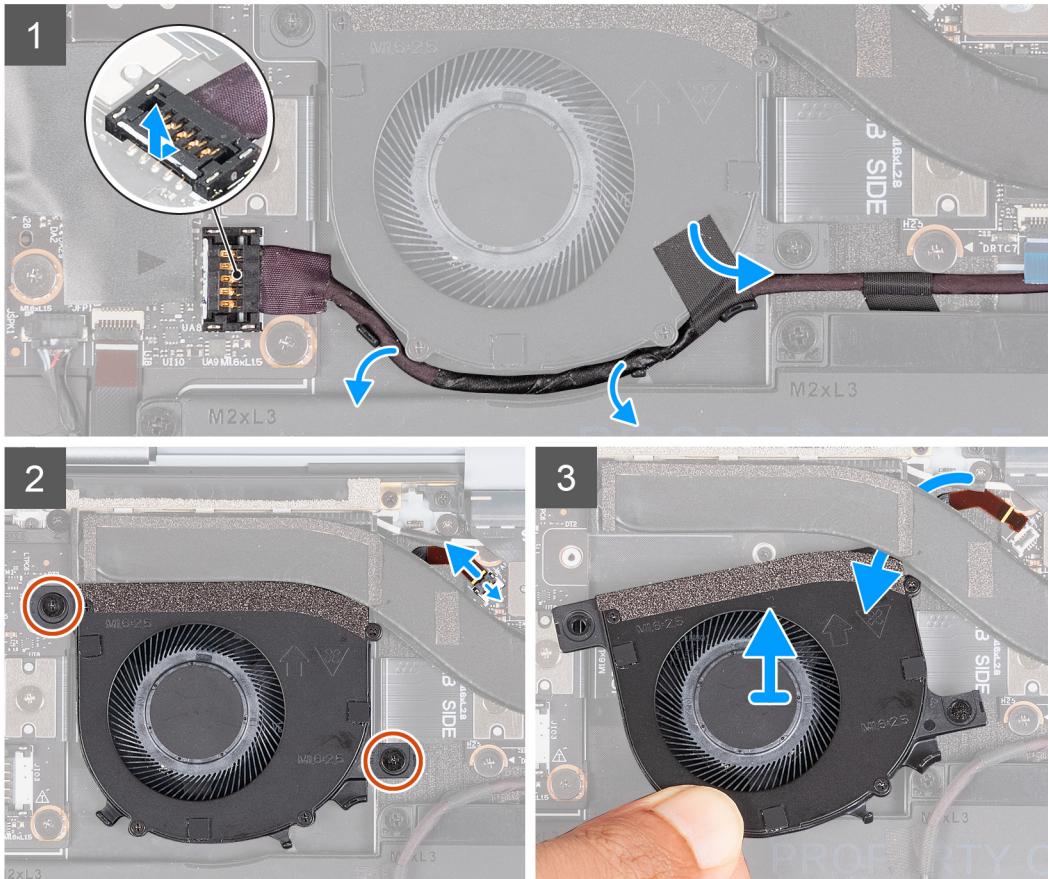
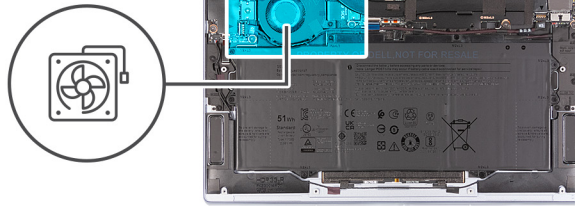
### Removing the fan

#### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).

#### About this task

The following image(s) indicate the location of the fan and provides a visual representation of the removal procedure.



### Steps

1. Pry up the I/O daughter-board power cable connector from the edge that is marked white.
2. Slide the I/O daughter-board power cable connector out to disconnect the I/O daughter-board power cable from the I/O daughter board.
3. Remove the I/O daughter-board power cable from the two routing guide below the fan, and peel off the tape from the fan.
4. Lift the latch of fan cable connector, use the pull tab of the fan cable to disconnect it from the system board.
5. Remove the two screws (M1.6x2.5) that secure the fan to the I/O daughter-board and the system board.
6. Slide the fan, together with the cable, towards the front of the computer.
7. Lift the fan off the I/O daughter-board and the system board carefully, and ensure the fan cable slides out from the bottom of the heat sink.

## Installing the fan

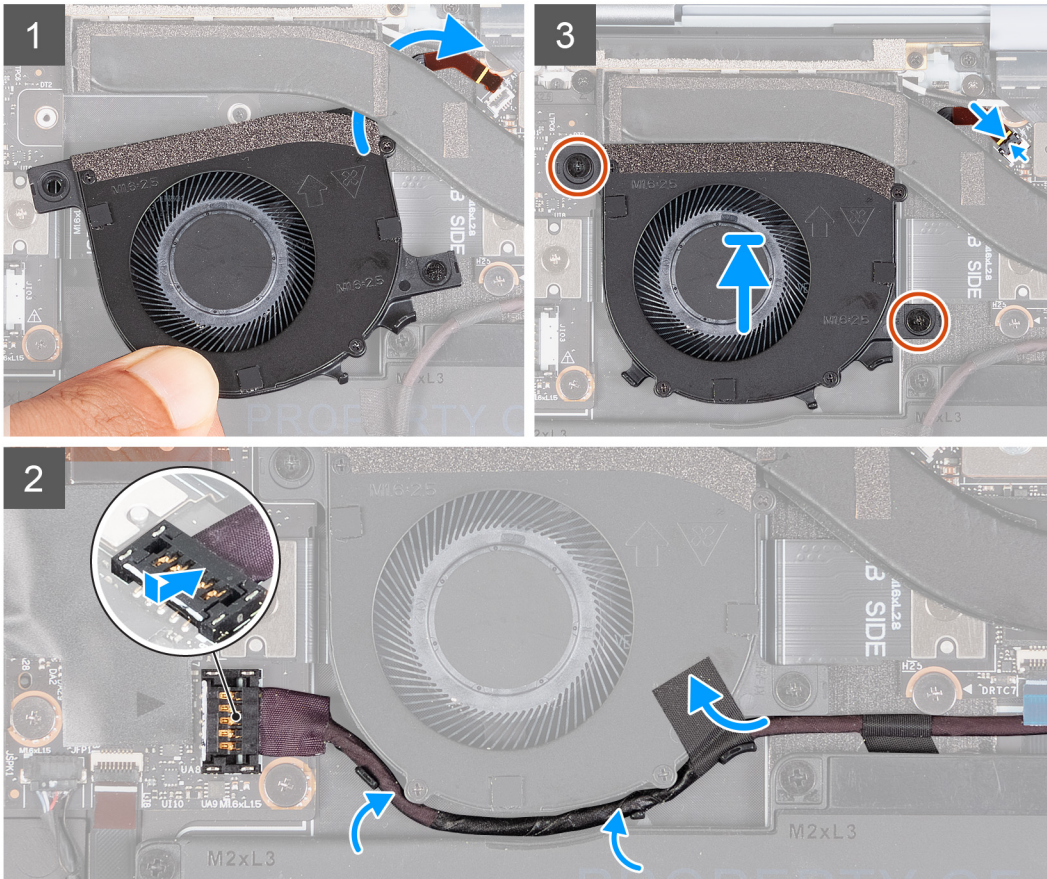
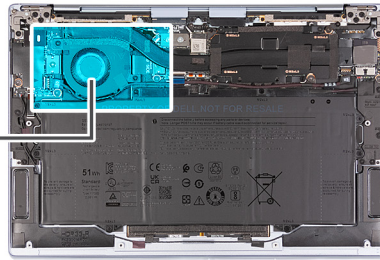
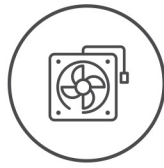
### Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

### About this task

The following image(s) indicate the location of the fan and provides a visual representation of the installation procedure.





### Steps

1. Slide the fan cable under the heat sink.
2. Align the screw holes of the fan with the screw hole of the I/O daughter-board and the screw hole of the system board.
3. Slide the fan into its place between the I/O daughter-board and the system board.
4. Replace the two screws (M1.6x2.5) that secure the fan to the I/O daughter-board and the system board.
5. Replace the tape that secures the I/O daughter-board power cable to the fan.
6. Place the I/O daughter-board power cable back to the two routing guides below the fan.
7. Connect the I/O daughter-board power cable to the I/O daughter-board.

### Next steps

1. Install the [base cover](#).
2. Follow the procedure in [After working inside your computer](#).



# Heat sink

## Removing the heat sink

### Prerequisites

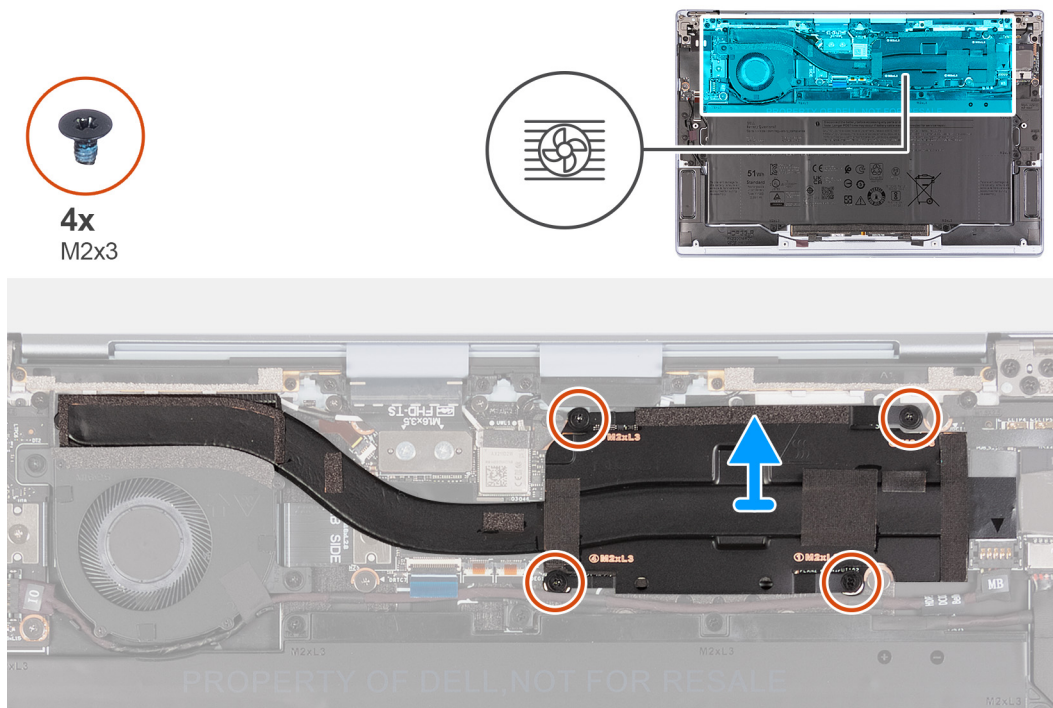
1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).

### About this task

**CAUTION:** The heat sink may become hot during normal operation. Allow sufficient time for the heat sink to cool before you touch it.

**NOTE:** For maximum cooling of the processor, do not touch the heat transfer areas on the heat sink. The oils in your skin can reduce the heat transfer capability of the thermal grease.

The following image(s) indicate the location of the heat sink and provides a visual representation of the removal procedure.



### Steps

1. In reverse sequential order (4>3>2>1), loosen the four screws (M2x3) that secure the heat sink to the system board.
2. Lift the heat sink off the system board.

## Installing the heat sink

### Prerequisites

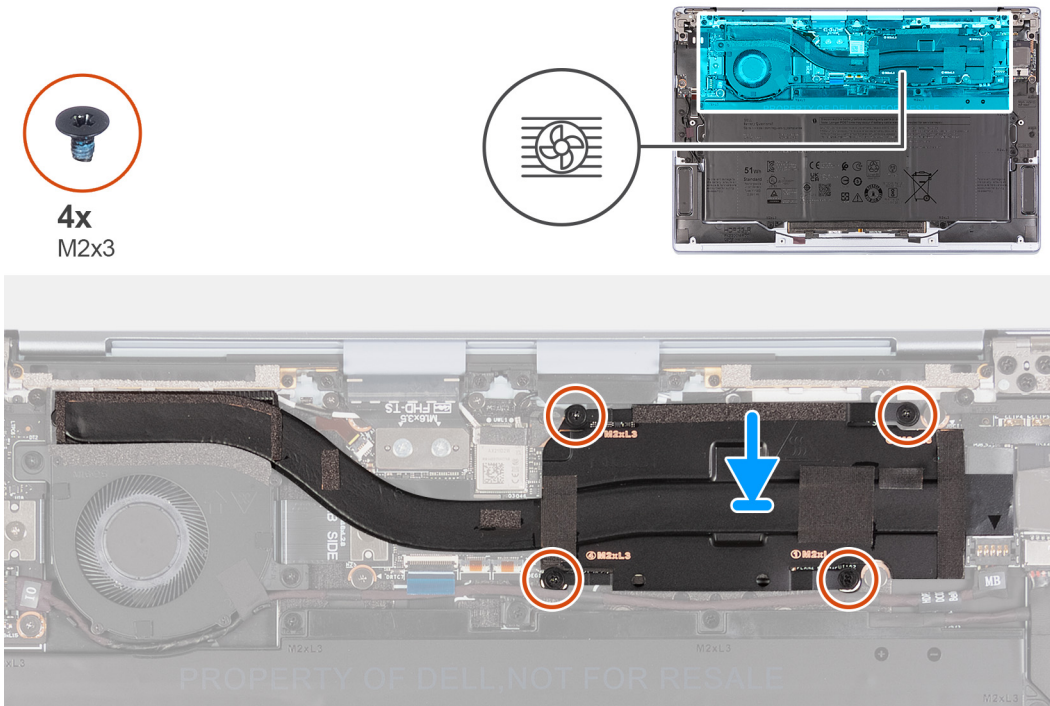
If you are replacing a component, remove the existing component before performing the installation process.

### About this task

**NOTE:** Incorrect alignment of the heat sink can damage the system board and processor.

**NOTE:** If either the system board or the heat sink is replaced, use the thermal grease that is provided in the kit to ensure that thermal conductivity is achieved.

The following image(s) indicate the location of the heat sink and provides a visual representation of the installation procedure.



### Steps

1. Align the screw holes of the heat sink with the screw holes of the system board.
2. In sequential order (1>2>3>4), tighten the four screws (M2x3) that secure the heat sink to the system board.

### Next steps

1. Install the [base cover](#).
2. Follow the procedure in [After working inside your computer](#).

## Display assembly

### Removing the display assembly

#### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).

#### About this task

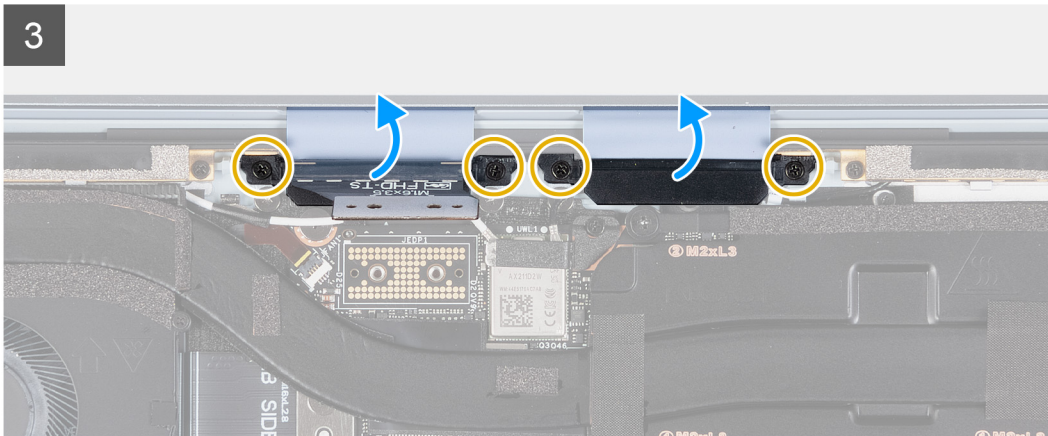
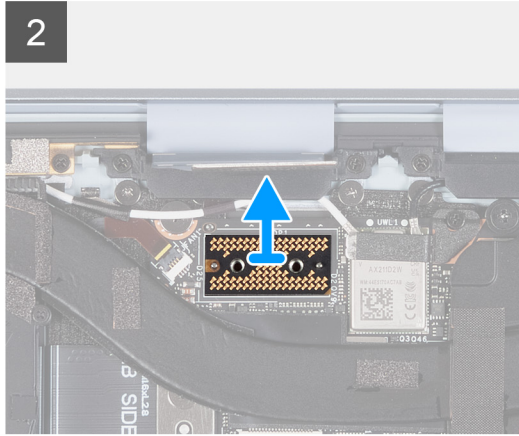
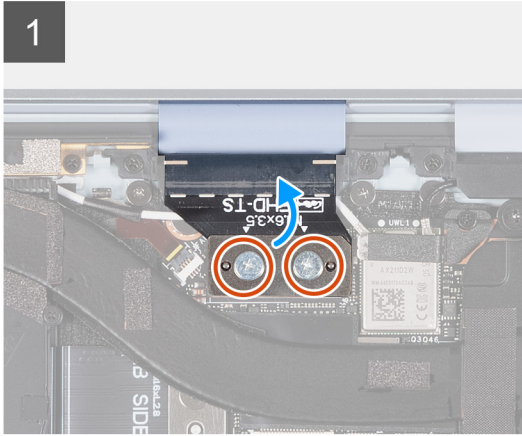
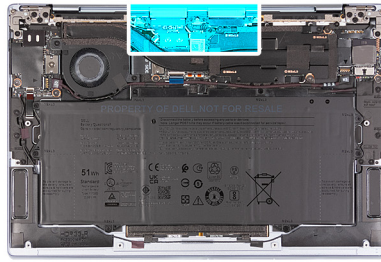
The following image(s) indicate the location of the display assembly and provides a visual representation of the removal procedure.



2x  
M1.6x3.5



4x  
M1.6x2.3





6x  
M2.5x4.3



2x  
M1.6x3




2x  
M1.6x2.5

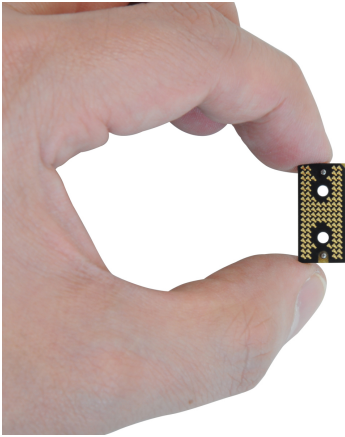


### Steps

1. Open the display assembly to a 90-degree angle and place the computer on the edge of a flat surface.
2. Remove the two screws (M1.6x3.5) that secure the camera and display-assembly cable to the display-assembly interposer board on the system board.
3. Lift the camera and display-assembly cable off and remove the display-assembly interposer board from the system board.

 **CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.





4. Remove the four screws (M1.6x2.3) that secure the two display-assembly cable brackets to the palm-rest and keyboard assembly.
5. Lift the display-assembly cable brackets off the system board.
6. Remove the six screws (M2.5x4.3) that secure the hinges of the display assembly to the palm-rest and keyboard assembly.
7. Remove the screw (M1.6x3) and the screw (M1.6x2.5) that secure the left hinge of display assembly to the system board and the palm-rest and keyboard assembly.
8. Remove the screw (M1.6x3) and the screw (M1.6x2.5) that secure the right hinge of display assembly to the I/O daughter-board and the palm-rest and keyboard assembly.
9. Lift the display assembly off the palm-rest and keyboard assembly.
10. After performing all the above steps, you are left with display assembly.

## Results



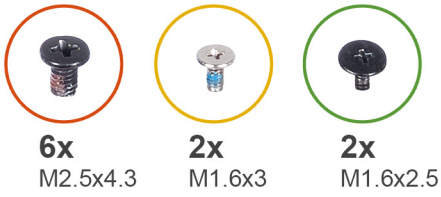
## Installing the display assembly

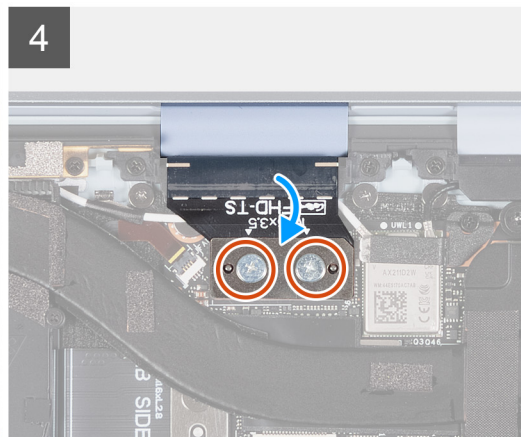
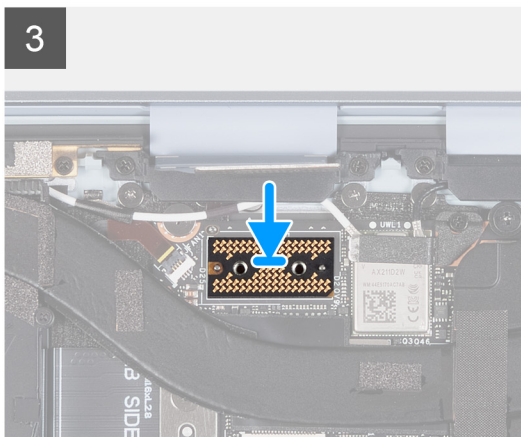
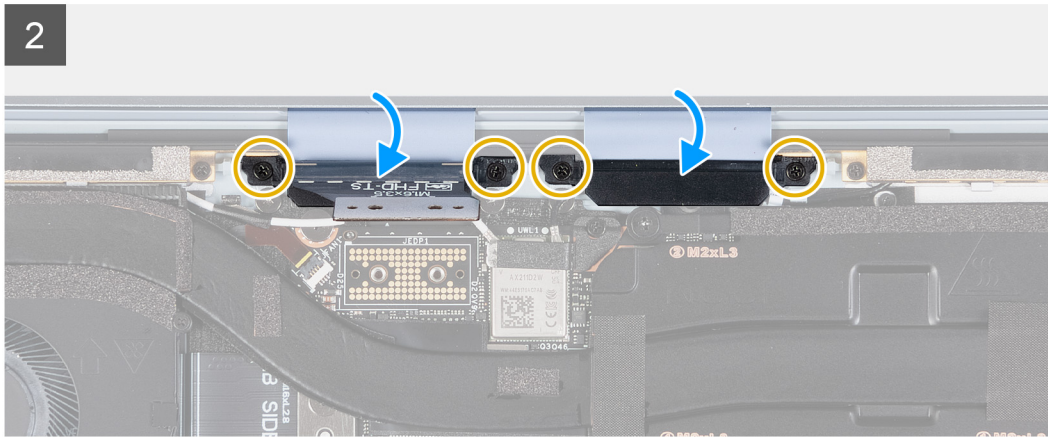
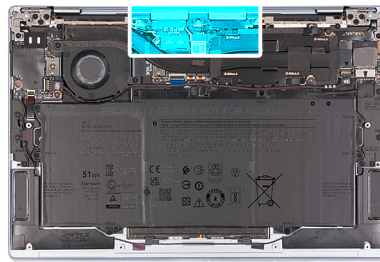
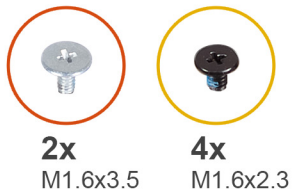
### Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

**About this task**

The following image(s) indicate the location of the display assembly and provides a visual representation of the installation procedure.



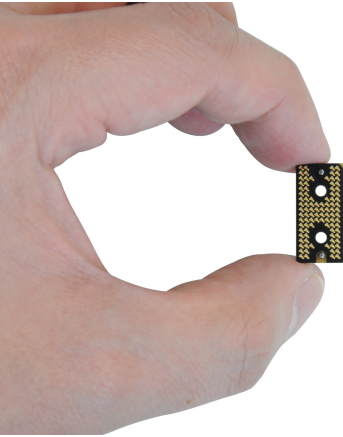


## Steps

1. Place the palm-rest and keyboard assembly at the edge of a flat table.
2. Open the hinges of the display assembly to a 90-degree angle.
3. Align the screw holes of the palm-rest and keyboard assembly to the screws holes on the hinges of the display assembly.
4. Replace the six screws (M2.5x4.3) that secure the hinges of the display assembly to the palm-rest and keyboard assembly.
5. Replace the screw (M1.6x3) and the screw (M1.6x2.5) that secure the left hinge of display assembly to the system board and the palm-rest and keyboard assembly.
6. Replace the screw (M1.6x3) and the screw (M1.6x2.5) that secure the right hinge of display assembly to the I/O daughter-board and the palm-rest and keyboard assembly.
7. Replace the four screws (M1.6x2.3) that secure the two display-assembly cable brackets to the palm-rest and keyboard assembly.
8. Replace the display-assembly interposer board on the system board.

**NOTE:** Ensure the cutouts of display-assembly interposer board are aligned with the stubs on the system board.

**CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.



9. Replace the two screws (M1.6x3.5) that secure the camera and display-assembly cable to the display-assembly interposer board on the system board.

#### **Next steps**

1. Install the [base cover](#).
2. Follow the procedure in [After working inside your computer](#).

## **I/O daughter-board**

### **Removing the I/O daughter-board**

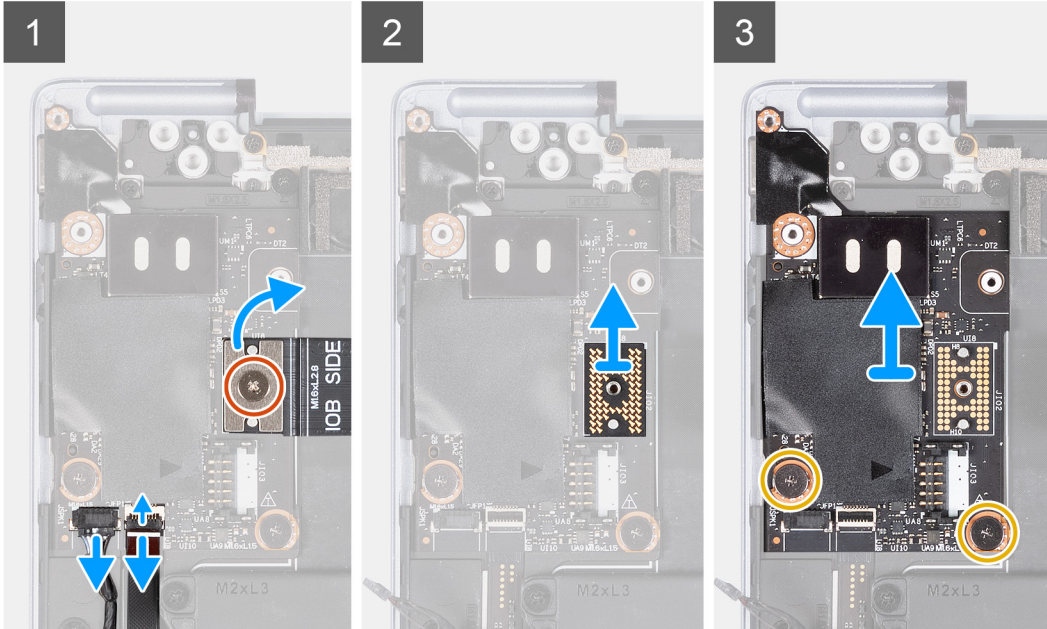
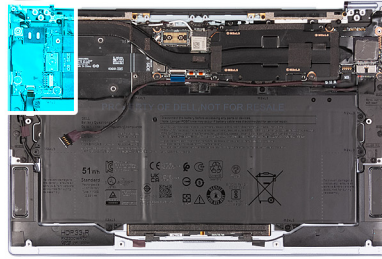
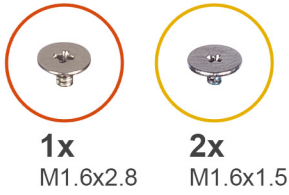
#### **Prerequisites**

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).
3. Remove the [fan](#).

#### **About this task**

The following image(s) indicate the location of the system board and provides a visual representation of the removal procedure.

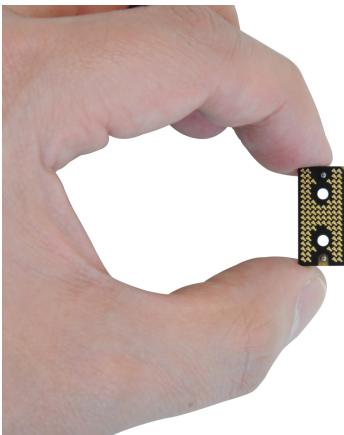




### Steps

1. Remove the screw (M1.6x2.8) that secures the I/O daughter-board cable to the I/O daughter-board interposer board.
2. Remove the I/O daughter-board cable from the I/O daughter-board interposer board.
3. Use the pull tab on the right speaker cable to disconnect the right speaker cable from the I/O daughter-board.
4. Lift the latch of the fingerprint-reader cable connector on the I/O daughter-board.
5. Use the pull tab on the fingerprint-reader cable connector to disconnect the fingerprint-reader cable from the I/O daughter-board.
6. Remove the I/O daughter-board interposer board from the I/O daughter-board.

**CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.



7. Remove the two screws (M1.6x1.5) that secure the I/O daughter-board to the palm-rest and keyboard assembly.
8. Lift the I/O daughter-board at an angle, and remove the I/O daughter-board from the palm-rest and keyboard assembly.

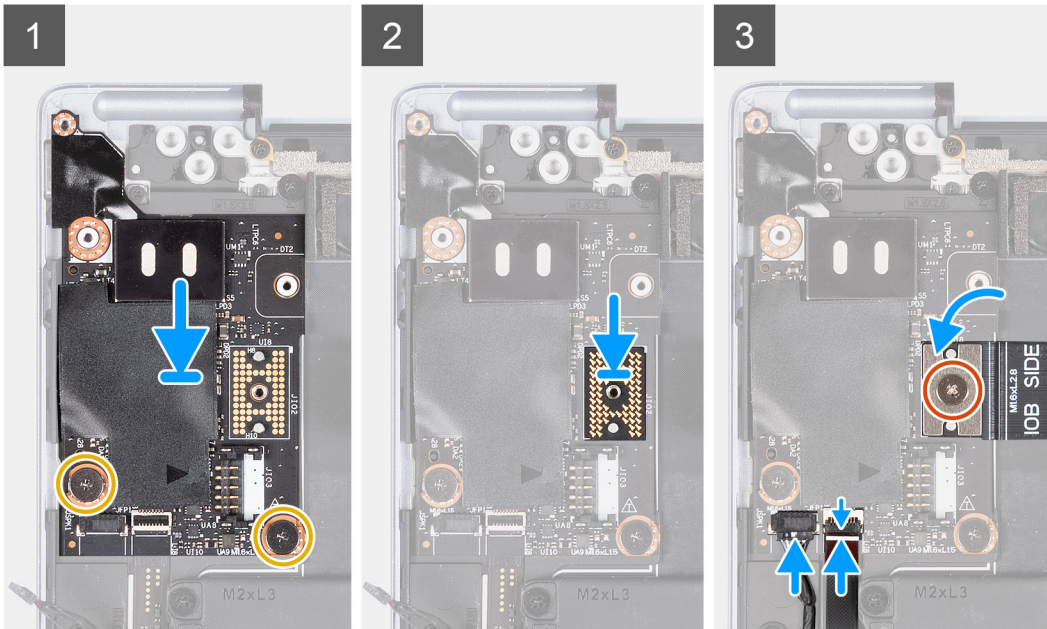
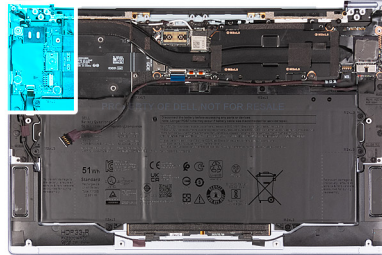
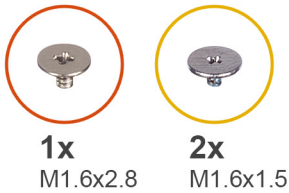
# Installing the I/O daughter-board

## Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

## About this task

The following image(s) indicate the location of the I/O daughter-board and provides a visual representation of the installation procedure.



## Steps

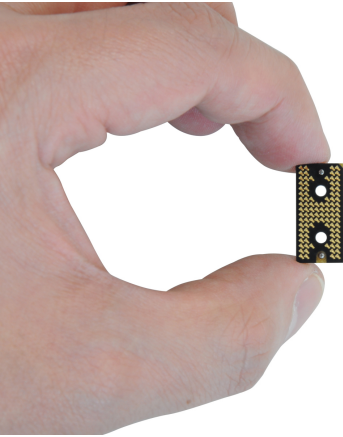
1. Align the screw holes of the I/O daughter-board with the screw holes of the palm-rest and keyboard assembly.
2. Place the I/O daughter-board on the palm-rest and keyboard assembly.

**i** **NOTE:** Ensure the right Thunderbolt 4 port of the I/O daughter-board is aligned with the right port hole of the palm-rest and keyboard assembly.

3. Replace the two screws (M1.6x1.5) that secure the I/O daughter-board to the palm-rest and keyboard assembly.
4. Place the I/O daughter-board interposer board on the I/O daughter-board.

**i** **NOTE:** Ensure the cutouts of I/O daughter-board interposer board are aligned with the stubs on the I/O daughter-board.

**⚠ CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.



5. Connect the I/O daughter-board cable to the I/O daughter-board interposer board.
6. Replace the screw (M1.6x2.8) that secures the I/O daughter-board cable to the I/O daughter-board interposer board.
7. Connect the right speaker cable to the I/O daughter-board.
8. Connect the fingerprint-reader cable and close the latch of the fingerprint-reader cable connector on the I/O daughter-board.

#### Next steps

1. Install the [fan](#).
2. Install the [base cover](#).
3. Follow the procedure in [After working inside your computer](#).

## System board

### Removing the system board

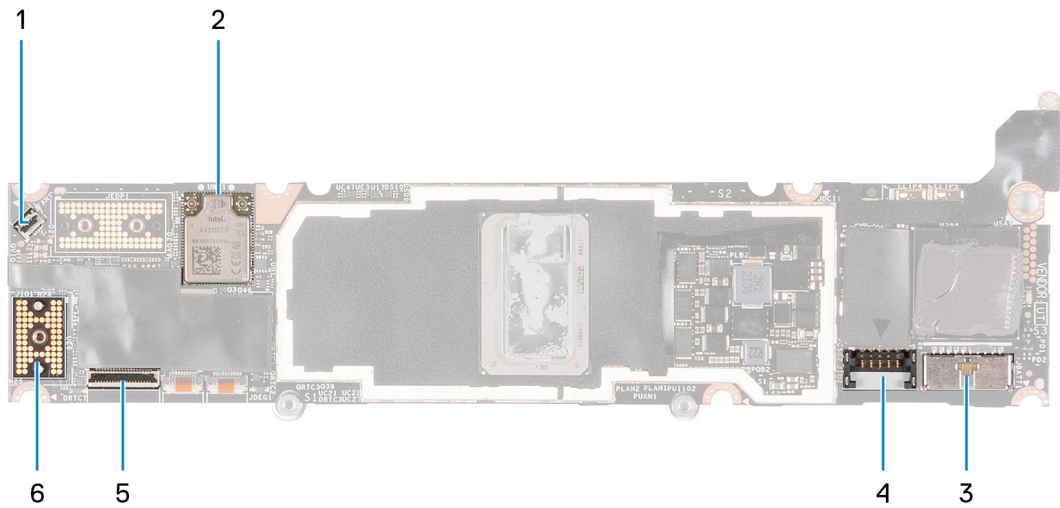
#### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).
3. Remove the [battery](#).
4. Remove the [display assembly](#).
5. Remove the [heat sink](#).

#### About this task

The following image indicates the connectors and component(s) on your system board.

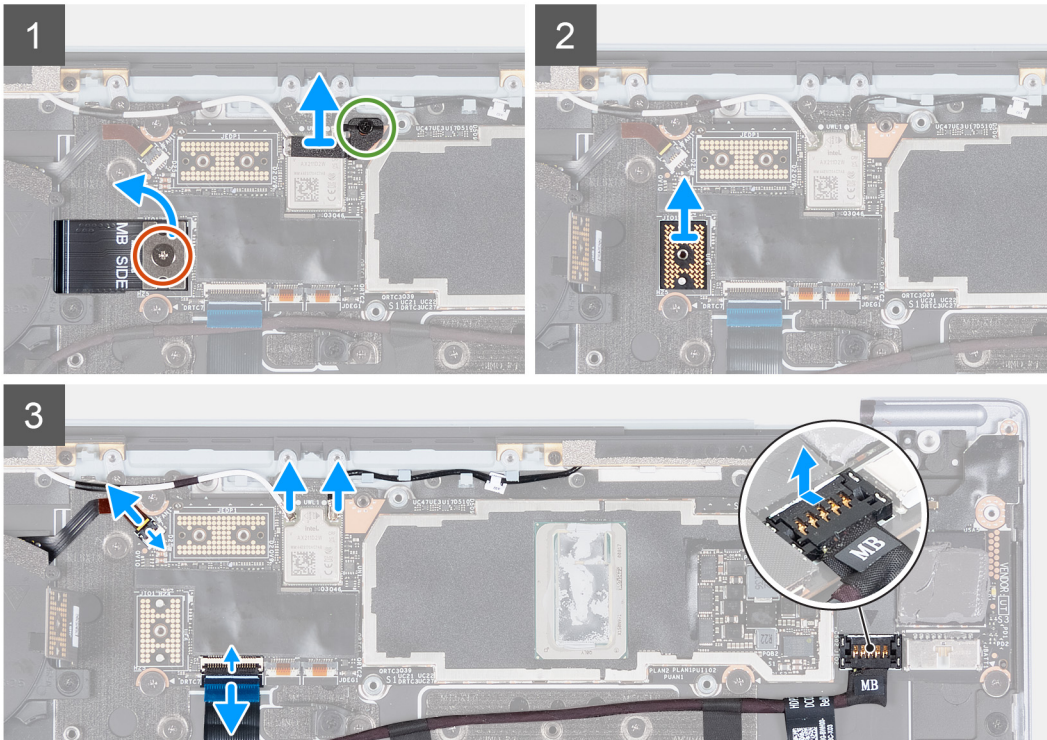


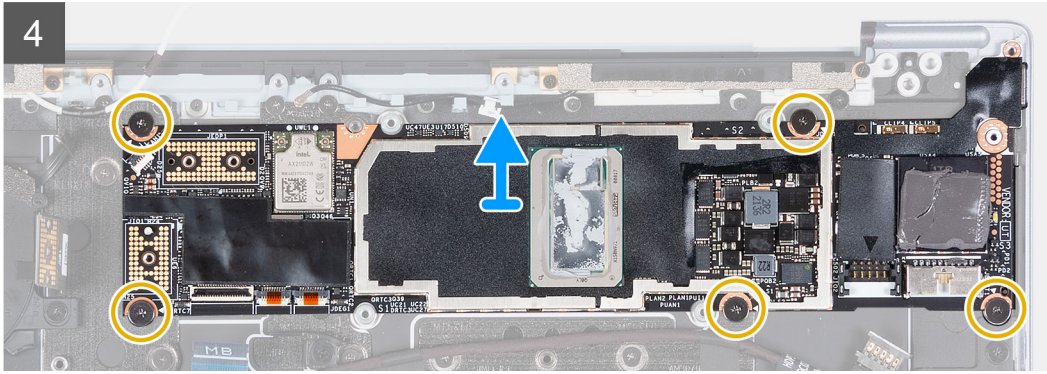


**Figure 1. System-board connectors**

- |                                |   |
|--------------------------------|---|
| 1. Fan cable connector         | 2. Wireless card                            |
| 3. Battery cable connector     | 4. I/O daughter-board power cable connector |
| 5. Touch-panel cable connector | 6. Camera-assembly cable connector          |

The following image(s) indicate the location of the system board and provides a visual representation of the removal procedure.

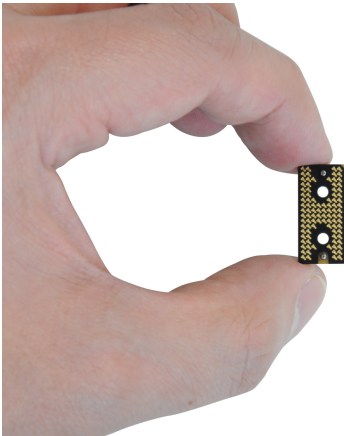




### Steps

1. Remove the screw (M1.6x2.3) that secures the wireless-module bracket to the system board.
2. Lift the wireless-module bracket off the system board.
3. Remove the screw (M1.6x2.8) that secures the I/O daughter-board cable to the system board.
4. Remove the system-board interposer board off the system board.

**CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.



5. Disconnect the wireless-module cables from the wireless module.
6. Lift the latch of fan cable connector, use the pull tab of the fan cable to disconnect it from the system board.
7. Lift the latch of the touch-panel connector and use the pull tab of the cable to disconnect the capacitive touch-panel cable.
8. Pry up the I/O daughter-board power cable connector from the edge that is marked white.
9. Slide the I/O daughter-board power cable connector out to disconnect the I/O daughter-board power cable from the system board.
10. Remove the five screws (M1.6x1.5) that secure the system board to the palm-rest and keyboard assembly.
11. Hold the system board by the long edges and lift the board off the palm-rest and keyboard assembly with care.

## Installing the system board

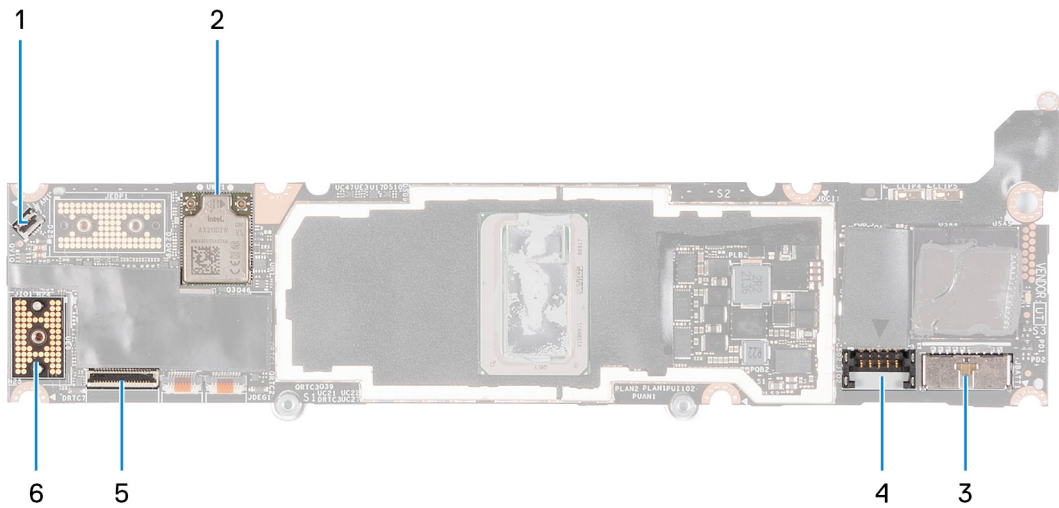
### Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

### About this task

The following image indicates the connectors and component(s) on your system board.

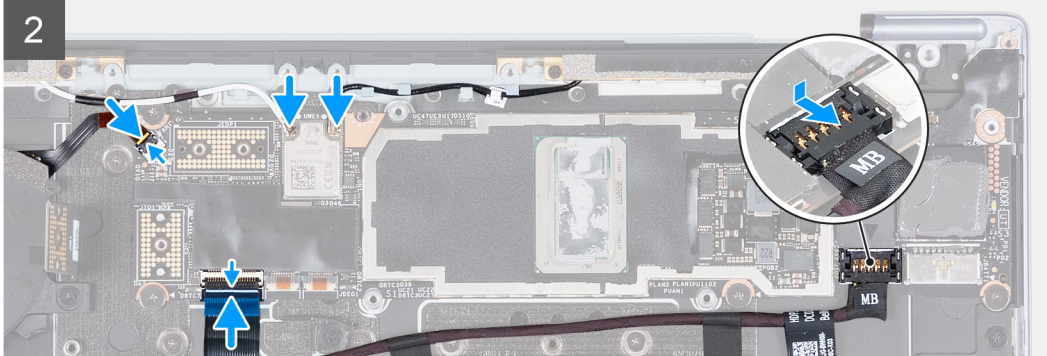
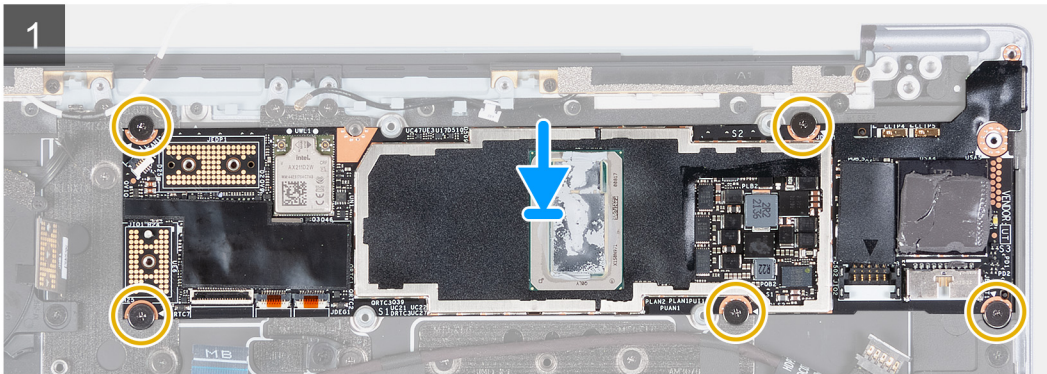
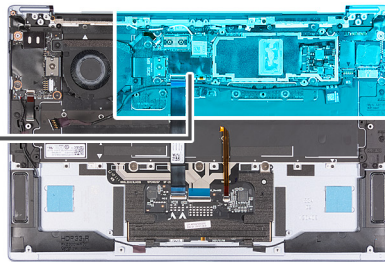
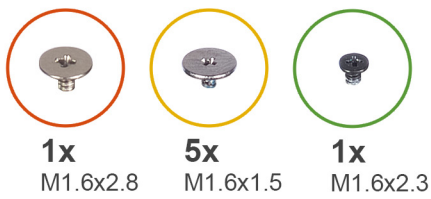


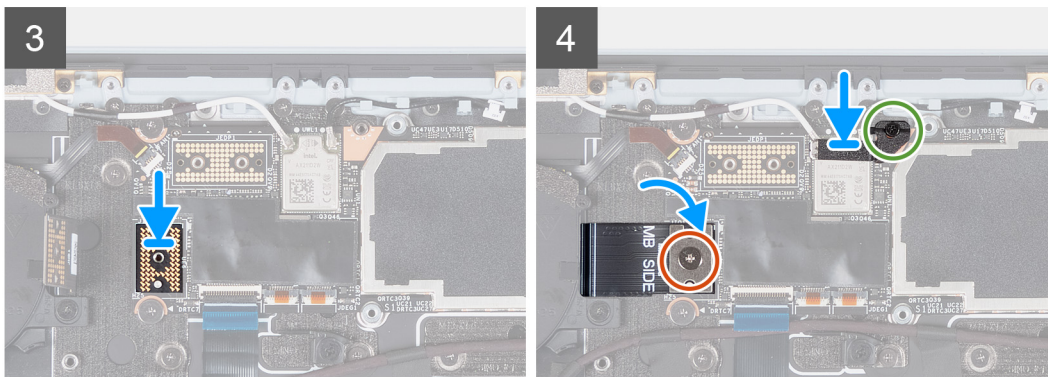


**Figure 2. System-board connectors**

- |                                |   |
|--------------------------------|---|
| 1. Fan cable connector         | 2. Wireless card                            |
| 3. Battery cable connector     | 4. I/O daughter-board power cable connector |
| 5. Touch-panel cable connector | 6. I/O daughter-board cable connector       |

The following image(s) indicate the location of the system board and provides a visual representation of the installation procedure.



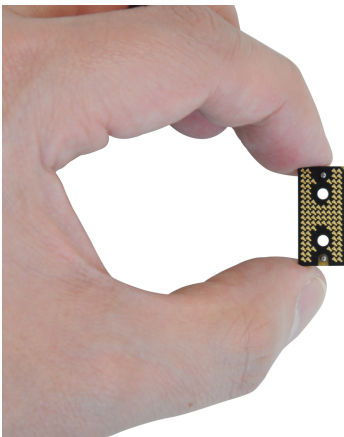


## Steps

1. Align the screw holes on the system board with the screw holes on the palm-rest and keyboard assembly.
2. Hold the system board by the long edges and place the system board on the palm-rest and keyboard assembly. Ensure that the left Thunderbolt 4 port is aligned with the left port hole on the palm-rest and keyboard assembly.
3. Replace the five screws (M1.6x1.5) that secure the system board to the palm-rest and keyboard assembly.
4. Connect the I/O daughter-board power cable to the system board.
5. Connect the touchpad cable and close the latch of the touchpad connector.
6. Connect the fan cable and close the latch of fan cable connector.
7. Connect the wireless-module cables from the wireless module.
8. Place the system-board interposer board on the system board.

**NOTE:** Ensure the cutouts of I/O daughter-board interposer board are aligned with the stubs on the I/O daughter-board.

**CAUTION:** The pins on the interposer board are fragile. Hold and lift the interposer board from the edges or the sides.



9. Replace the screw (M1.6x2.8) that secures the I/O daughter-board cable to the system board.
10. Align the screw hole of the wireless-module bracket with the screw hole on the system board.
11. Replace the screw (M1.6x2.3) that secures the wireless-module bracket to the system board.

## Next steps

1. Install the [heat sink](#).
2. Install the [display assembly](#).
3. Install the [battery](#).
4. Install the [base cover](#).
5. Follow the procedure in [After working inside your computer](#).



# Palm-rest and keyboard assembly

## Removing the palm-rest and keyboard assembly

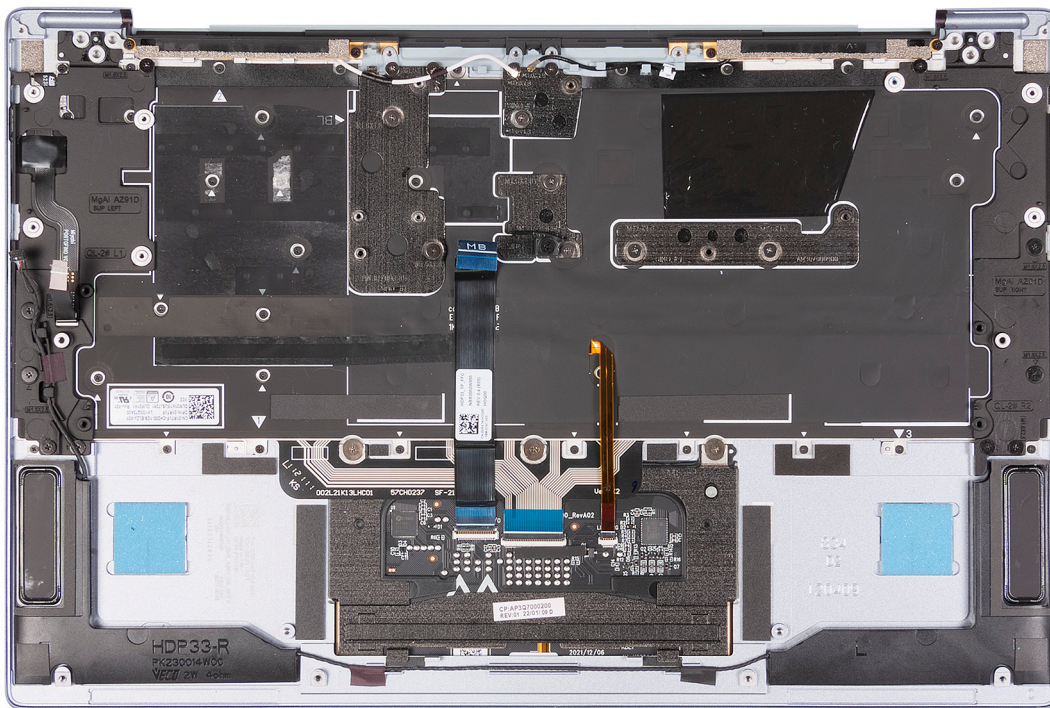
### Prerequisites

1. Follow the procedure in [Before working inside your computer](#).
2. Remove the [base cover](#).
3. Remove the [battery](#).
4. Remove the [fan](#).
5. Remove the [display assembly](#).
6. Remove the [I/O daughter-board](#).
7. Remove the [system board](#).

**i** **NOTE:** The system board can be removed with the attached heat sink.

### About this task

The following image shows the palm-rest and keyboard assembly.



### Steps

After performing the steps in the pre-requisites, you are left with the palm-rest and keyboard assembly.

## Installing the palm-rest and keyboard assembly

### Prerequisites

If you are replacing a component, remove the existing component before performing the installation process.

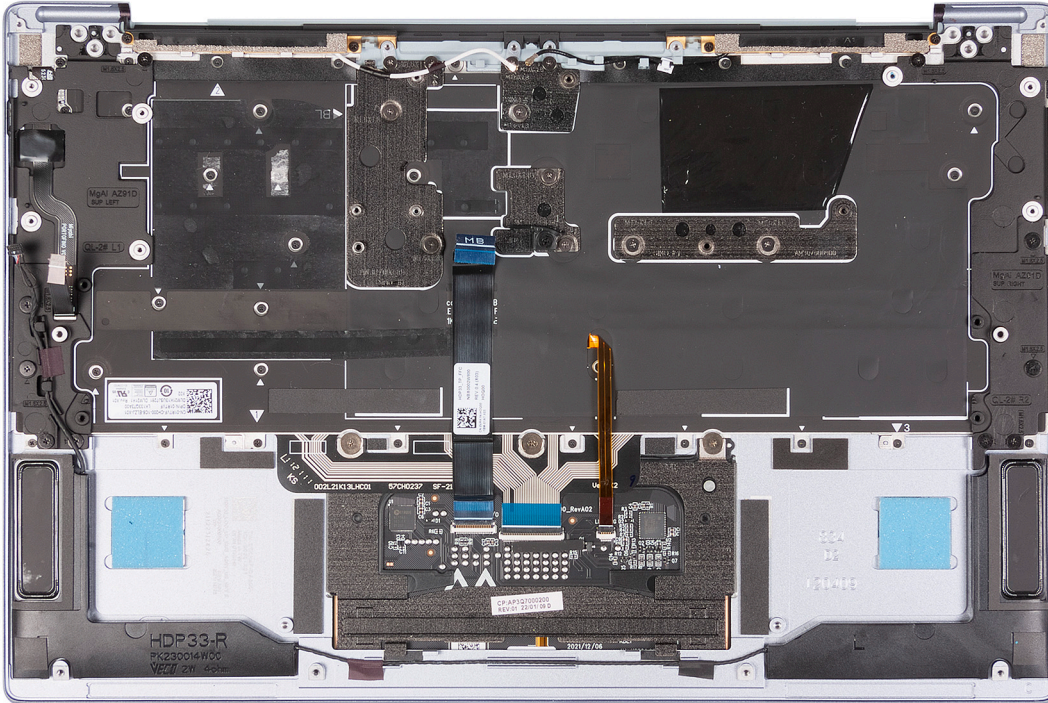
### About this task

- i** **NOTE:** The replacement palm-rest and keyboard assembly comes pre-assembled with the following components:
- palm rest



- keyboard
- speakers
- wireless-antenna modules
- touchpad

The following image shows the palm-rest and keyboard assembly.



### Steps

Place the palm-rest and keyboard assembly on a flat surface.

### Next steps

1. Install the [system board](#).  
**i** **NOTE:** The system board can be installed with the attached heat sink.
2. Install the [I/O daughter-board](#).
3. Install the [display assembly](#).
4. Install the [fan](#).
5. Install the [battery](#).
6. Install the [base cover](#).
7. Follow the procedure in [After working inside your computer](#).

## Drivers and downloads

When troubleshooting, downloading or installing drivers it is recommended that you read the Dell Knowledge Based article, Drivers and Downloads FAQ [000123347](#).

# System setup

**CAUTION:** Unless you are an expert computer user, do not change the settings in the BIOS Setup program. Certain changes can make your computer work incorrectly.

**NOTE:** Depending on the computer and its installed devices, the items listed in this section may or may not be displayed.

**NOTE:** Before you change BIOS Setup program, it is recommended that you write down the BIOS Setup program screen information for future reference.

Use the BIOS Setup program for the following purposes:

- Get information about the hardware installed in your computer, such as the amount of RAM and the size of the hard drive.
- Change the system configuration information.
- Set or change a user-selectable option, such as the user password, type of hard drive installed, and enabling or disabling base devices.

## Entering BIOS setup program

### About this task

Turn on (or restart) your computer and press F2 immediately.

## Navigation keys

**NOTE:** For most of the System Setup options, changes that you make are recorded but do not take effect until you restart the system.

**Table 2. Navigation keys**

Keys	Navigation
Up arrow	Moves to the previous field.
Down arrow	Moves to the next field.
Enter	Selects a value in the selected field (if applicable) or follow the link in the field.
Spacebar	Expands or collapses a drop-down list, if applicable.
Tab	Moves to the next focus area. <b>NOTE:</b> For the standard graphics browser only.
Esc	Moves to the previous page until you view the main screen. Pressing Esc in the main screen displays a message that prompts you to save any unsaved changes and restarts the system.

## Boot Sequence

Boot Sequence allows you to bypass the System Setup–defined boot device order and boot directly to a specific device (for example: USB flash drive, external optical drive, or external storage device). During the Power-on Self Test (POST), when the Dell logo appears, you can:

- Access System Setup by pressing F2 key
- Bring up the one-time boot menu by pressing F12 key


The one-time boot menu displays the devices that you can boot from including the diagnostic option. The boot menu options are:

- Removable Drive (if available)
- Optical Drive (if available)
- Solid-State Drive (if available)
- Diagnostics

The boot sequence screen also displays the option to access the System Setup screen.

## One time boot menu

To enter **one time boot menu**, turn on your computer, and then press F12 immediately.


 **NOTE:** It is recommended to shutdown the computer if it is on.

The one-time boot menu displays the devices that you can boot from including the diagnostic option. The boot menu options are:

- Removable Drive (if available)
- Optical Drive (if available)
- Solid-State Drive (if available)
- Diagnostics

The boot sequence screen also displays the option to access the System Setup screen.

## System setup options

 **NOTE:** Depending on your computer and its installed devices, the items that are listed in this section may or may not be displayed.

**Table 3. System setup options—Overview menu**

Overview	
<b>XPS 13 9315/XPS 9315</b>	
BIOS Version	Displays the BIOS version number.
Service Tag	Displays the Service Tag of the computer.
Asset Tag	Displays the Asset Tag of the computer.
Manufacture Date	Displays the manufacture date of the computer.
Ownership Date	Displays the ownership date of the computer.
Express Service Code	Displays the Express Service Code of the computer.
Ownership Tag	Displays the Ownership Tag of the computer.
Signed Firmware Update	Displays whether the Signed Firmware Update is enabled on your computer. By default, the <b>Signed Firmware Update</b> option is enabled.
<b>Battery Information</b>	
Primary	Displays the primary battery of the computer.
Battery Level	Displays the battery level of the computer.
Battery State	Displays the battery state of the computer.
Health	Displays the battery health of the computer.

**Table 3. System setup options—Overview menu (continued)**

<b>Overview</b>	
AC Adapter	Displays whether an AC adapter is connected. If connected, displays the type of AC adapter that is connected.
<b>Processor Information</b>	
Processor Type	Displays the processor type.
Maximum Clock Speed	Displays the maximum processor clock speed.
Minimum Clock Speed	Displays the minimum processor clock speed.
Current Clock Speed	Displays the current processor clock speed.
Core Count	Displays the number of cores on the processor.
Processor ID	Displays the processor identification code.
Processor L2 Cache	Displays the processor L2 Cache size.
Processor L3 Cache	Displays the processor L3 Cache size.
Microcode Version	Displays the microcode version.
Intel Hyper-Threading Capable	Displays whether the processor is Hyper-Threading (HT) capable.
64-Bit Technology	Displays whether 64-bit technology is used.
<b>Memory Information</b>	
Memory Installed	Displays the total computer memory installed.
Memory Available	Displays the total computer memory available.
Memory Speed	Displays the memory speed.
Memory Channel Mode	Displays single or dual channel mode.
Memory Technology	Displays the technology that is used for the memory.
<b>Devices Information</b>	
Panel Type	Displays the Panel Type of the computer.
Video Controller	Displays the video controller type of the computer.
Video Memory	Displays the video memory information of the computer.
Wi-Fi Device	Displays the wireless device information of the computer.
Native Resolution	Displays the native resolution of the computer.
Video BIOS Version	Displays the video BIOS version of the computer.
Audio Controller	Displays the audio controller information of the computer.
Bluetooth Device	Displays the Bluetooth device information of the computer.
Pass Through MAC Address	Displays the MAC address of the video pass-through.

**Table 4. System setup options—Boot Configuration menu**

<b>Boot Configuration</b>	
<b>Boot Sequence</b>	
Boot Mode: UEFI only	Displays the boot mode of the computer.
Boot Sequence	Displays the boot sequence.
Secure Digital (SD) Card Boot	Enables or disables read-only boot from Secure Digital (SD) card. By default, the <b>Secure Digital (SD) Card Boot</b> option is enabled.

**Table 4. System setup options—Boot Configuration menu (continued)**

<b>Boot Configuration</b>	
<b>Secure Boot</b>	Secure Boot is a method of guaranteeing the integrity of the boot path by performing additional validation of the operating system and PCI add-in cards. The computer stops booting to the operating system when a component is not authenticated during the boot process.
Enable Secure Boot	<p>Enables the computer to boot using only validated boot software.</p> <p>By default, the <b>Enable Secure Boot</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Secure Boot</b> option enabled to ensure that the UEFI firmware validates the operating system during the boot process.</p> <p><b>i</b> <b>NOTE:</b> For Secure Boot to be enabled, the computer is required to be in UEFI boot mode and the Enable Legacy Option ROMs option is required to be turned off.</p>
Secure Boot Mode	<p>Enables or disables the Secure Boot operation mode.</p> <p>By default, the <b>Deployed Mode</b> is selected.</p> <p><b>i</b> <b>NOTE:</b> <b>Deployed Mode</b> should be selected for normal operation of Secure Boot.</p>
Enable Microsoft UEFI CA	<p>When disabled, the UEFI CA is removed from the BIOS UEFI Secure Boot database.</p> <p><b>i</b> <b>NOTE:</b> When disabled, the Microsoft UEFI CA could render your computer unable to boot, system graphics may not function, some devices may not function properly, and the computer could become unrecoverable.</p> <p>By default, the <b>Enable Microsoft UEFI CA</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Microsoft UEFI CA</b> option enabled to ensure the broadest compatibility with devices and operating systems.</p>
<b>Expert Key Management</b>	
Enable Custom Mode	<p>Enables or disables the keys in the PK, KEK, db, and dbx security key databases to be modified.</p> <p>By default, the <b>Enable Custom Mode</b> option is disabled.</p>
Custom Mode Key Management	<p>Selects the custom values for expert key management.</p> <p>By default, the <b>PK</b> option is selected.</p>

**Table 5. System setup options—Integrated Devices menu**

<b>Integrated Devices</b>	
<b>Date/Time</b>	
Date	Sets the computer date in MM/DD/YYYY format. Changes to the date format take effect immediately.
Time	Sets the computer time in HH/MM/SS 24-hour format. You can switch between 12-hour and 24-hour clock. Changes to the time format take effect immediately.
<b>Camera</b>	
Enable Camera	<p>Enables the camera.</p> <p>By default, the <b>Enable Camera</b> option is enabled.</p> <p><b>i</b> <b>NOTE:</b> Depending on the configuration ordered, the camera setup option may not be available.</p>
<b>Audio</b>	

**Table 5. System setup options—Integrated Devices menu (continued)**

<b>Integrated Devices</b>	
Enable Audio	Enables all integrated audio controller. By default, all the options are enabled.
Enable Microphone	Enables the microphone. By default, the <b>Enable Microphone</b> option is enabled. <b>i</b> <b>NOTE:</b> Depending on the configuration ordered, the microphone setup option may not be available.
Enable Internal Speaker	Enables the internal speaker. By default, the <b>Enable Internal Speaker</b> option is enabled.
<b>USB/Thunderbolt Configuration</b>	
Enable USB Boot Support	Enables booting from USB mass storage devices that are connected to external USB ports. By default, the <b>Enable USB Boot Support</b> option is enabled.
Enable External USB Ports	Enables the external USB ports. By default, the <b>Enable External USB Ports</b> option is enabled.
<b>Enable Thunderbolt Technology Support</b>	
Enable Thunderbolt Technology Support	Enables the associated ports and adapters for Thunderbolt Technology support. By default, the <b>Enable Thunderbolt Technology Support</b> option is enabled.
<b>Enable Thunderbolt Boot Support</b>	
Enable Thunderbolt Boot Support	Enables the Thunderbolt adapter-peripheral device and USB devices that are connected to the Thunderbolt adapter to be used during BIOS Pre-boot. By default, the <b>Enable Thunderbolt Boot Support</b> option is disabled.
<b>Enable Thunderbolt (and PCIe behind TBT) pre-boot modules</b>	Enables the PCIe devices that are connected through a Thunderbolt adapter to run the PCIe devices UEFI Option ROM (if present) during pre-boot. By default, the <b>Enable Thunderbolt (and PCIe behind TBT) pre-boot modules</b> option is disabled.
<b>Disable USB4 PCIE Tunneling</b>	Disables the USB4 PCIE Tunneling option. By default, the <b>Disable USB4 PCIE Tunneling</b> option is disabled.
<b>Video/Power only on Type-C Ports</b>	Enables or disables the Type-C port functionality to video or only power. By default, the <b>Video/Power only on Type-C Ports</b> option is disabled.
<b>Type-C Dock</b>	
Type-C Dock Override	Enables or disables to use connected Type-C Dell Dock to provide data stream with external USB ports disabled. When Type-C Dock override is enabled, the Video/Audio/LAN submenu is activated. By default, the <b>Type-C Dock Override</b> option is enabled.
Type-C Dock Audio	Enables or disables the usage of audio inputs and outputs from the connected Type-C Dell docking station. By default, the <b>Type-C Dock Audio</b> option is enabled.
Type-C Dock LAN	Enables or disables the usage of LAN on the external ports of the connected Type-C Dell docking station. By default, the <b>Type-C Dock LAN</b> option is enabled.

**Table 5. System setup options—Integrated Devices menu (continued)**

<b>Integrated Devices</b>	
<b>Miscellaneous Devices</b>	
Enable Fingerprint Reader Device	Enables the Fingerprint Reader Device option. By default, the <b>Enable Fingerprint Reader Device</b> option is enabled.

**Table 6. System setup options—Storage menu**

<b>Storage</b>	
<b>SATA/NVMe Operation</b>	
SATA/NVMe Operation	Sets operating mode of the integrated SATA hard drive controller. By default, the <b>AHCI/NVMe</b> option is selected. Storage device is configured for AHCI/NVMe mode.
<b>Storage Interface</b>	
Port Enablement	Enables or disables the M.2 PCIe SSD option. By default, the <b>M.2 PCIe SSD</b> option is enabled.
<b>Drive Information</b>	
<b>Enable MediaCard</b>	
Secure Digital (SD) Card	Enables or disables the SD card. By default, the <b>Secure Digital (SD) Card</b> option is enabled.
Secure Digital (SD) Card Read-Only Mode	Enables or disables the SD card read-only mode. By default, the <b>Secure Digital (SD) Card Read-Only Mode</b> option is disabled.

**Table 7. System setup options—Display menu**

<b>Display</b>	
<b>Display Brightness</b>	
Brightness on battery power	Enables to set the screen brightness when the computer is running on battery power. By default, the screen brightness is set to 50 when the computer is running on battery power.
Brightness on AC power	Enables to set the screen brightness when the computer is running on AC power. By default, the screen brightness is set to 100 when the computer is running on AC power.
<b>Touchscreen</b>	
<b>Full Screen Logo</b>	
	Enables or disables the computer to display full screen logo, if the image matches screen resolution. By default, the <b>Full Screen Logo</b> option is disabled.

**Table 8. System setup options—Connection menu**

<b>Connection</b>	
<b>Wireless Device Enable</b>	
WLAN	Enables or disables the internal WLAN device. By default, the <b>WLAN</b> option enabled.



**Table 8. System setup options—Connection menu (continued)**

<b>Connection</b>	
Bluetooth	Enables or disables the internal Bluetooth device. By default, the <b>Bluetooth</b> option enabled.
<b>Enable UEFI Network Stack</b>	Enables or disables the UEFI Network Stack and controls the on-board LAN Controller. By default, the <b>Enable UEFI Network Stack</b> option is enabled.
<b>Wireless Radio Control</b>	
Control WLAN Radio	Enables to sense the connection of the computer to a wired network and then disables the selected wireless radios (WLAN and/or WWAN). Upon disconnection from the wired network, the selected wireless radios are re-enabled. By default, the <b>Control WLAN Radio</b> option is disabled.


**Table 9. System setup options—Power menu**

<b>Power</b>	
<b>Battery Configuration</b>	Enables or disables the computer to run on battery during peak power usage hours. Use the table <b>Custom Charge Start</b> and <b>Custom Charge Stop</b> , to prevent AC power usage between certain times of each day. By default, the <b>Adaptive</b> option is selected. Battery settings are adaptively optimized based on your typical battery usage pattern.
<b>Advanced Configuration</b>	
Enable Advanced Battery Charge Configuration	Enables Advanced Battery Charge Configuration from the beginning of the day to a specified work period. When enabled, Advanced Battery Charged maximizes battery health while still supporting heavy use during the work day. By default, the <b>Enable Advanced Battery Charge Configuration</b> option is disabled.
<b>Peak Shift</b>	
Enable Peak Shift	Enables the computer to run on battery during peak power usage hours. By default, the <b>Enable Peak Shift</b> option is disabled.
<b>Thermal Management</b>	Enables or disables cooling of fan and manages processor heat to adjust the system performance, noise, and temperature. By default, the <b>Optimized</b> option is selected. Standard setting for balanced performance, noise, and temperature.
<b>USB Wake Support</b>	
Wake on Dell USB-C Dock	When enabled, connecting a Dell USB-C Dock wakes the computer from Standby, Hibernate, and Power Off. By default, the <b>Wake on Dell USB-C Dock</b> option is enabled.
<b>Block Sleep</b>	Enables or disables the computer from entering Sleep (S3) mode in the operating system. By default, the <b>Block Sleep</b> option is disabled. <b>i</b> <b>NOTE:</b> When enabled, the computer does not go to Sleep, Intel Rapid Start is disabled automatically, and the operating system power option is blank if it was set to Sleep.
<b>Lid Switch</b>	
Enable Lid Switch	Enables or disables the Lid Switch.

**Table 9. System setup options—Power menu (continued)**

<b>Power</b>	
	By default, the <b>Enable Lid Switch</b> option is enabled.
Power On Lid Open	When enabled, allows the computer to power on from the off state whenever the lid is opened.  By default, the <b>Power On Lid Open</b> option is enabled.
<b>Intel Speed Shift Technology</b>	Enables or disables the Intel Speed Shift Technology support. When enabled, the operating system selects the appropriate processor performance automatically.  By default, the <b>Intel Speed Shift Technology</b> option is enabled.

**Table 10. System setup options—Security menu**

<b>Security</b>	
<b>Trusted Platform Module (TPM)</b>	Trusted Platform Module (TPM) is a security device that stores computer-generated keys for encryption and features such as BitLocker, Virtual Secure Mode, remote Attestation.  By default, the <b>Trusted Platform Module (TPM)</b> option is enabled.  For additional security, Dell Technologies recommends keeping Trusted Platform Module (TPM) enabled to allow these security technologies to fully function.
TPM On	Allows you to enable or disable TPM.  By default, the <b>TPM On</b> option is enabled.  For additional security, Dell Technologies recommends keeping TPM enabled to allow these security technologies to fully function.
Physical Presence Interface (PPI) Bypass for Enable Commands	The Physical Presence Interface (PPI) Bypass options can be used to allow the operating system to manage certain aspects of the TPM. If these options are enabled, you are not prompted to confirm certain changes to the TPM configuration.  By default, the <b>PPI Bypass for Enable Commands</b> option is enabled.  For additional security, Dell Technologies recommends keeping the <b>PPI Bypass for Enable Commands</b> option enabled.
Physical Presence Interface (PPI) Bypass for Disable Commands	By default, the <b>PPI Bypass for Disable Commands</b> option is disabled.  For additional security, Dell Technologies recommends keeping the <b>PPI Bypass for Disable Commands</b> option disabled.
Physical Presence Interface (PPI) Bypass for Clear Commands	By default, the <b>PPI Bypass for Clear Commands</b> option is disabled.  For additional security, Dell Technologies recommends keeping the <b>PPI Bypass for Clear Commands</b> option disabled.
Attestation Enable	The <b>Attestation Enable</b> option controls the endorsement hierarchy of TPM. Disabling the <b>Attestation Enable</b> option prevents TPM from being used to digitally-sign certificates.  By default, the <b>Attestation Enable</b> option is enabled.  For additional security, Dell Technologies recommends keeping the <b>Attestation Enable</b> option enabled.   <b>NOTE:</b> When disabled, this feature may cause compatibility issues or loss of functionality in some operating systems.
Key Storage Enable	The <b>Key Storage Enable</b> option controls the storage hierarchy of TPM, which is used to store digital keys. Disabling the <b>Key Storage Enable</b> option restricts the ability of TPM to store owner's data.

**Table 10. System setup options—Security menu (continued)**

<b>Security</b>	
	<p>By default, the <b>Key Storage Enable</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Key Storage Enable</b> option enabled.</p> <p><b>i</b> <b>NOTE:</b> When disabled, this feature may cause compatibility issues or loss of functionality in some operating systems.</p>
SHA-256	<p>Allows you control the usage of SHA-256 by TPM. When enabled, the BIOS and TPM use the SHA-256 hash algorithm to extend measurements into the TPM PCRs during BIOS boot. When disabled, the BIOS and TPM use the SHA-1 hash algorithm to extend measurements into the TPM PCRs during BIOS boot.</p> <p>By default, the <b>SHA-256</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>SHA-256</b> option enabled.</p>
Clear	<p>When enabled, the <b>Clear</b> option clears information stored in the TPM after exiting the system's BIOS. This option returns to disabled state when the system restarts.</p> <p>By default, the <b>Clear</b> option is disabled.</p> <p>Dell Technologies recommends enabling the <b>Clear</b> option only when TPM data is required to be cleared.</p>
TPM State	<p>Enables or disables the Trusted Platform Module (TPM). This is the normal operating state for the Trusted Platform Module (TPM) when you want to use its complete array of capabilities.</p> <p>By default, the <b>TPM State</b> option is enabled.</p>
<b>Intel Platform Trust Technology (PTT)</b>	<p>Intel PTT is a firmware-based Trusted Platform Module (fTPM) device that is part of Intel chipsets. It provides credential storage and key management that can replace the equivalent functionality of a discrete TPM chip.</p>
PTT On	<p>Enables or disables the Intel PTT option.</p> <p>By default, the <b>PTT On</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>PTT On</b> option enabled.</p>
Physical Presence Interface (PPI) Bypass for Clear Commands	<p>The PPI Bypass for Clear Commands option allows the operating system to manage certain aspects of PTT. When enabled, you are not prompted to confirm changes to the PTT configuration.</p> <p>By default, the <b>PPI Bypass for Clear Commands</b> option is disabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>PPI Bypass for Clear Commands</b> option disabled.</p>
Clear	<p>When enabled, the <b>Clear</b> option clears the information stored in the PTT fTPM after exiting the system's BIOS. This option returns to disabled state when the system restarts.</p> <p>By default, the <b>Clear</b> option is disabled.</p> <p>Dell Technologies recommends enabling the <b>Clear</b> option only when PTT fTPM data needs to be cleared.</p>
<b>Chassis intrusion</b>	
Chassis Intrusion Detection	<p>Allows you to control the chassis intrusion feature. This feature notifies the user when the base cover has been removed from the computer.</p> <p>When set to <b>Enabled</b>, a notification is displayed on the next boot and the event is logged in the BIOS Events log.</p>

**Table 10. System setup options—Security menu (continued)**

<b>Security</b>	
	<p>When set to <b>On-Silent</b>, the event is logged in the BIOS Events log, but no notification is displayed.</p> <p>When set to <b>Disabled</b>, no notification is displayed and no event is logged in the BIOS Events log.</p> <p>By default, the <b>Chassis Intrusion Detection</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Chassis Intrusion Detection</b> option enabled.</p>
Block Boot Until Cleared	<p>Enables or disables the Block Boot Until Cleared option.</p> <p>By default, the <b>Block Boot Until Cleared</b> option is enabled.</p> <p><b>i NOTE:</b> When enabled, the computer does not boot until the chassis intrusion is cleared. If the administrator password is set, Setup has to be unlocked before the warning can be cleared.</p>
<b>Legacy Manageability Interface Access</b>	<p>Allows the administrator to control the access to BIOS configuration through the Legacy Manageability Interface option. When enabled, this prevents the BIOS Administrator password-based manageability tools from running, prevents some Dell software applications from reading configuration settings, and/or prevents changes to the BIOS configuration settings.</p> <p>When enabled, this option only supports the Authenticated BIOS Manageability Interface (ABI) for managing the BIOS configuration changes. To support this feature, ABI must be enabled and provisioned.</p> <p>When set to <b>Enabled</b>, the Legacy Manageability Interface can be used to read and change BIOS configuration settings.</p> <p>When set to <b>Read-Only</b>, BIOS configuration settings can be read, but cannot be changed through the Legacy Manageability Interface.</p> <p>When set to <b>Disabled</b>, the Legacy Manageability Interface is disabled. BIOS configuration reads and writes are blocked.</p>
<b>SMM Security Mitigation</b>	<p>Enables or disables additional UEFI SMM Security Mitigation protections. This option uses the Windows SMM Security Mitigations Table (WSMT) to confirm to the operating system that security best practices have been implemented by the UEFI firmware.</p> <p>By default, the <b>SMM Security Mitigation</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>SMM Security Mitigation</b> option enabled unless you have a specific application which is not compatible.</p> <p><b>i NOTE:</b> This feature may cause compatibility issues or loss of functionality with some legacy tools and applications.</p>
<b>Data Wipe on Next Boot</b>	
Start Data Wipe	<p><b>⚠ CAUTION: Secure Data Wipe operation deletes information in a way that it cannot be reconstructed.</b></p> <p>Commands such as delete and format in the operating system may remove files from showing up in the file system, however they can be reconstructed through forensic means as they are still represented on the physical media. Data Wipe prevents this reconstruction and is not recoverable.</p> <p>When enabled, the BIOS will queue up a data wipe cycle for storage devices that are connected to the motherboard on the next reboot.</p> <p>By default, the <b>Start Data Wipe</b> option is disabled.</p>
Absolute	<p>Enables, disables, or permanently disables the BIOS module interface of the optional Absolute Persistence Module service from Absolute software.</p>

**Table 10. System setup options—Security menu (continued)**



Security	
	<p>By default, the <b>Absolute</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Absolute</b> option enabled.</p> <p><b>⚠ WARNING: The 'Permanently Disabled' option can only be selected once. When 'Permanently Disabled' is selected, Absolute Persistence cannot be re-enabled. No further changes to the Enable/Disable states are allowed.</b></p> <p><b>i NOTE:</b> The Enable/Disable options are unavailable while the computer is in the activated state.</p> <p><b>i NOTE:</b> When the Absolute features are activated, the Absolute integration cannot be disabled from the BIOS setup screen.</p>
UEFI Boot Path Security	<p>Enables or disables the computer to prompt the user to enter the Administrator password (if set) when booting to a UEFI boot path device from the F12 boot menu.</p> <p>By default, the <b>Always Except Internal HDD</b> option is enabled.</p>
<b>Firmware Device Tamper Detection</b>	<p>Allows you to control the firmware device tamper detection feature. This feature notifies the user when the firmware device is tampered. When enabled, a screen warning messages are displayed on the computer and a tamper detection event is logged in the BIOS Events log. The computer fails to reboot until the event is cleared.</p> <p>By default, the <b>Firmware Device Tamper Detection</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Firmware Device Tamper Detection</b> option enabled.</p>

**Table 11. System setup options—Passwords menu**

Passwords	
<b>Administrator Password</b>	<p>The Administrator Password prevents unauthorized access to the BIOS Setup options. Once the administrator password is set, the BIOS setup options can only be modified after providing the correct password.</p> <p>The following rules and dependencies apply to the Administrator Password -</p> <ul style="list-style-type: none"> <li>• The administrator password cannot be set if system and/or internal hard drive passwords are previously set.</li> <li>• The administrator password can be used in place of the system and/or internal hard drive passwords.</li> <li>• When set, the administrator password must be provided during a firmware update.</li> <li>• Clearing the administrator password also clears the system password (if set).</li> </ul> <p>Dell Technologies recommends using an administrator password to prevent unauthorized changes to BIOS setup options.</p>
<b>System Password</b>	<p>The System Password prevents the system from booting to an operating system without entering the correct password.</p> <p>The following rules and dependencies apply when the System Password is used -</p> <ul style="list-style-type: none"> <li>• The computer shuts down when idle for approximately 10 minutes at the system password prompt.</li> <li>• The computer shuts down after three incorrect attempts to enter the system password.</li> <li>• The computer shuts down when the <b>Esc</b> key is pressed at the System Password prompt.</li> </ul>



**Table 11. System setup options—Passwords menu (continued)**

<b>Passwords</b>	<ul style="list-style-type: none"> <li>• The system password is not prompted when the computer resumes from standby mode.</li> </ul> <p>Dell Technologies recommends using the system password in situations where it is likely that a system may be lost or stolen.</p>
<b>Hard Drive Password</b>	<p>The Hard Drive Password can be set to prevent unauthorized access of the data stored on the hard drive. The computer prompts for the hard drive password during boot in order to unlock the drive. A password secured hard drive stays locked even when removed from the computer or placed into another computer. It prevents an attacker from accessing data on the drive without authorization.</p> <p>The following rules and dependencies apply when the Hard Drive Password is used -</p> <ul style="list-style-type: none"> <li>• The hard drive password option cannot be accessed when a hard drive is disabled in the BIOS setup.</li> <li>• The computer shuts down when idle for approximately 10 minutes at the hard drive password prompt.</li> <li>• The computer shuts down after three incorrect attempts to enter the hard drive password and treats the hard drive as not available.</li> <li>• The hard drive does not accept password unlock attempts after five incorrect attempts to enter the hard drive password from the BIOS Setup. The hard drive password must be reset for the new password unlock attempts.</li> <li>• The computer treats the hard drive as not available when the <b>Esc</b> key is pressed at the hard drive password prompt.</li> <li>• The hard drive password is not prompted when the computer resumes from standby mode. When the hard drive is unlocked by the user before the computer goes into standby mode, it remains unlocked after the computer resumes from standby mode.</li> <li>• If the system and hard drive passwords are set to the same value, the hard drive unlocks after the correct system password is entered.</li> </ul> <p>Dell Technologies recommends using a hard drive password to protect unauthorized data access.</p>
<b>Owner Password</b>	<p>The Owner Password is typically used when a system is loaned or leased, and the end user sets their own system or hard drive password. The Owner Password can provide override access to unlock the system when it is returned. The Owner Password cannot be set via BIOS Setup. System lessors are given a tool which enables them to configure the Owner Password.</p> <p>The following rules and dependencies apply when the Owner Password is used -</p> <ul style="list-style-type: none"> <li>• The owner password cannot be set when the administrator password is already set.</li> <li>• The owner password can be used in place of the administrator, system, or hard drive passwords.</li> </ul> <p> <b>NOTE:</b> The hard drive password must have been set on the computer with owner password.</p> <p>Dell Technologies recommends that only system lessors use the owner password.</p>
<b>Strong Password</b>	<p>The Strong Password feature enforces stricter rules for administrator, owner, and system passwords.</p> <p>When enabled, the following rules are enforced -</p> <ul style="list-style-type: none"> <li>• The minimum length of the password is set to 8 characters.</li> <li>• The password is required to include at least 1 upper case and 1 lower case character.</li> </ul> <p> <b>NOTE:</b> These requirements do not affect the hard drive password.</p> <p>By default, the <b>Strong Password</b> option is enabled.</p>

**Table 11. System setup options—Passwords menu (continued)**

<b>Passwords</b>	
	For additional security, Dell Technologies recommends keeping the <b>Strong Password</b> option enabled as it requires passwords be more complex.
<b>Password Configuration</b>	<p>The Password configuration page includes several options for changing the requirements of BIOS passwords. You can modify the minimum and maximum length of the passwords as well as require passwords to contain certain character classes (upper case, lower case, digit, special character).</p> <p>Dell Technologies recommends setting the minimum password length to at least 8 characters.</p>
<b>Password Bypass</b>	<p>The <b>Password Bypass</b> option allows the computer to reboot from the operating system without entering the system or hard drive password. If the computer has already booted to the operating system, it is presumed that the user has already entered the correct system or hard drive password.</p> <p><b>NOTE:</b> This option does not remove the requirement to enter the password after shutting down.</p> <p>By default, the <b>Password Bypass</b> option is enabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Password Bypass</b> option enabled.</p>
<b>Password Changes</b>	
Allow Non-Admin Password Changes	<p>The <b>Allow Non-Admin Password Changes</b> option in BIOS setup allows an end user to set or change the system or hard drive passwords without entering the administrator password. This gives an administrator control over the BIOS settings but enables an end user to provide their own password.</p> <p>By default, the <b>Allow Non-Admin Password Changes</b> option is disabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Allow Non-Admin Password Changes</b> option disabled.</p>
Non-Admin Setup Changes	<p>The <b>Non-Admin Setup Changes</b> option allows an end user to configure the wireless devices without requiring the administrator password.</p> <p>By default, the <b>Non-Admin Setup Changes</b> option is disabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Non-Admin Setup Changes</b> option disabled.</p>
<b>Admin Setup Lockout</b>	<p>The <b>Admin Setup Lockout</b> option prevents an end user from even viewing the BIOS setup configuration without first entering the administrator password (if set).</p> <p>By default, the <b>Admin Setup Lockout</b> option is disabled.</p> <p>For additional security, Dell Technologies recommends keeping the <b>Admin Setup Lockout</b> option disabled.</p>
<b>Master Password Lockout</b>	
Enable Master Password Lockout	<p>The Master Password Lockout setting allows you to disable the Recovery Password feature. If the system, administrator, or hard drive password is forgotten, the system becomes unusable.</p> <p><b>NOTE:</b> When the owner password is set, the Master Password Lockout option is not available.</p> <p><b>NOTE:</b> When an internal hard drive password is set, it must first be cleared before Master Password Lockout can be changed.</p> <p>By default, the <b>Enable Master Password Lockout</b> option is disabled.</p> <p>Dell Technologies does not recommend enabling the <b>Master Password Lockout</b> unless you have implemented your own password recovery system.</p>

**Table 12. System setup options—Update, Recovery menu**

<b>Update, Recovery</b>	
<b>UEFI Capsule Firmware Updates</b>	
Enable UEFI Capsule Firmware Updates	<p>Enables or disables BIOS updates through UEFI capsule update packages.</p> <p><b>i</b> <b>NOTE:</b> Disabling this option blocks the BIOS updates from services such as Microsoft Windows Update and Linux Vendor Firmware Service (LVFS).</p> <p>By default, the <b>Enable UEFI Capsule Firmware Updates</b> option is enabled.</p>
<b>BIOS Recovery from Hard Drive</b>	
	<p>Enables or disables the user to recover from certain corrupted BIOS conditions from a recovery file on the user primary hard drive or an external USB key.</p> <p>By default, the <b>BIOS Recovery from Hard Drive</b> option is enabled.</p> <p><b>i</b> <b>NOTE:</b> BIOS Recovery from Hard Drive is not available for self-encrypting drives (SED).</p> <p><b>i</b> <b>NOTE:</b> BIOS recovery is designed to fix the main BIOS block and cannot work if the Boot Block is damaged. In addition, this feature cannot work in the event of EC corruption, ME corruption, or a hardware issue. The recovery image must exist on an unencrypted partition on the drive.</p>
<b>BIOS Downgrade</b>	
Allow BIOS Downgrade	<p>Controls flashing of the system firmware to previous revisions.</p> <p>By default, the <b>Allow BIOS Downgrade</b> option is enabled.</p>
<b>SupportAssist OS Recovery</b>	
	<p>Enables or disables the boot flow for SupportAssist OS Recovery tool in the event of certain system errors.</p> <p>By default, the <b>SupportAssist OS Recovery</b> option is enabled.</p>
<b>BIOSConnect</b>	
	<p>Enables or disables cloud Service operating system recovery if the main operating system fails to boot with the number of failures equal to or greater than the value specified by the Auto operating system Recovery Threshold setup option and local Service operating system does not boot or is not installed.</p> <p>By default, the <b>BIOSConnect</b> option is enabled.</p>
<b>Dell Auto OS Recovery Threshold</b>	
	<p>Allows you to control the automatic boot flow for SupportAssist System Resolution Console and for Dell operating system Recovery Tool.</p> <p>By default, the <b>Dell Auto OS Recovery Threshold</b> value is set to 2.</p>

**Table 13. System setup options—System Management menu**

<b>System Management</b>	
<b>Service Tag</b>	Displays the Service Tag of the computer.
<b>Asset Tag</b>	<p>Creates a computer Asset Tag that can be used by an IT administrator to uniquely identify a particular computer.</p> <p><b>i</b> <b>NOTE:</b> Once set in BIOS, the Asset Tag cannot be changed.</p>
<b>AC Behavior</b>	
Wake on AC	<p>Enables or disables the computer to turn on and go to boot when AC power is supplied to the computer.</p> <p>By default, the <b>Wake on AC</b> option is disabled.</p>
<b>Wake on LAN</b>	<p>Enables or disables the computer to turn on by a special LAN signal.</p> <p>By default, the <b>Wake on LAN</b> option is disabled.</p>
<b>Auto On Time</b>	<p>Enable to set the system to turn on automatically every day or on a preselected date and time. This option can be configured only if the Auto On Time is set to Everyday, Weekdays, or Selected Days.</p>

**Table 13. System setup options—System Management menu (continued)**

<b>System Management</b>	
	By default, the <b>Auto On Time</b> option is disabled.

**Table 14. System setup options—Keyboard menu**

<b>Keyboard</b>	
<b>Fn Lock Options</b>	Enables or disables the Fn Lock option. By default, the <b>Fn Lock</b> option is enabled.
<b>Lock Mode</b>	By default, the <b>Lock Mode Secondary</b> option is enabled. With this option, the F1-F12 keys scan the code for their secondary functions.
<b>Keyboard Illumination</b>	Configures the operating mode of the keyboard illumination feature. By default, the <b>Bright</b> option is selected. Enables the keyboard illumination feature at 100% brightness level.
<b>Keyboard Backlight Timeout on AC</b>	Sets the timeout value for the keyboard backlight when an AC adapter is connected to the computer. By default, the <b>10 seconds</b> option is selected.
<b>Keyboard Backlight Timeout on Battery</b>	Sets the timeout value for the keyboard backlight when the computer is running only on the battery power. The keyboard backlight timeout value is only effective when the backlight is enabled. By default, the <b>10 seconds</b> option is selected.
<b>Device Configuration HotKey Access</b>	Allows you to control whether you can access device configuration screens through hotkeys during system startup. By default, the <b>Device Configuration HotKey Access</b> option is enabled. <b>i</b> <b>NOTE:</b> This setting controls only the Intel RAID (CTRL+I), MEBX (CTRL+P), and LSI RAID (CTRL+C) Option ROMs. Other pre-boot Option ROMs, which support entry using a key sequence, are not affected by this setting.



**Table 15. System setup options—Pre-boot Behavior menu**

<b>Pre-boot Behavior</b>	
<b>Adapter Warnings</b>	
Enable Dock Warning Messages	Enables the warning messages during boot when the adapters with less power capacity are detected. By default, the <b>Enable Dock Warning Messages</b> option is enabled.
<b>Warnings and Errors</b>	Enables or disables the action to be taken when a warning or error is encountered. By default, the <b>Prompt on Warnings and Errors</b> option is selected. Stop, prompt, and wait for user input when warnings or errors are detected. <b>i</b> <b>NOTE:</b> Errors deemed critical to the operation of the computer hardware stop the functioning of the computer.
<b>USB-C Warnings</b>	
Enable Dock Warning Messages	Enables the warning messages during boot when the USB-C adapters with less power capacity are detected. By default, the <b>Enable Dock Warning Messages</b> option is enabled.
<b>Fastboot</b>	Allows you to configure the speed of the UEFI boot process. By default, the <b>Thorough</b> option is selected. Performs complete hardware and configuration initialization during boot.

**Table 15. System setup options—Pre-boot Behavior menu (continued)**

<b>Pre-boot Behavior</b>	
<b>Extend BIOS POST Time</b>	Sets the BIOS POST (Power-On Self-Test) load time. By default, the <b>0 seconds</b> option is selected.
<b>MAC Address Pass-Through</b>	Replaces the external NIC MAC address (in a supported dock or dongle) with the selected MAC address from the computer. By default, the <b>System Unique MAC Address</b> option is selected.
<b>Mouse/Touchpad</b>	Defines how the computer handles mouse and touchpad input. By default, the <b>Touchpad and PS/2 Mouse</b> option is selected. Leaves the integrated touchpad enabled when an external PS/2 mouse is present.
<b>Sign of Life</b>	
Early Logo Display	Display Logo Sign of Life. By default, the <b>Early Logo Display</b> option is enabled.
Early Keyboard Backlight	Keyboard Backlight Sign of Life. By default, the <b>Early Keyboard Backlight</b> option is enabled.

**Table 16. System setup options—Virtualization menu**

<b>Virtualization Support</b>	
<b>Intel Virtualization Technology</b>	
Enable Intel Virtualization Technology (VT)	When enabled, the computer can run a Virtual Machine Monitor (VMM). By default, the <b>Enable Intel Virtualization Technology (VT)</b> option is enabled.
<b>VT for Direct I/O</b>	
Enable Intel VT for Direct I/O	When enabled, the system can perform Virtualization Technology for Direct I/O (VT-d). VT-d is an Intel method that provides virtualization for memory map I/O. By default, the <b>Enable Intel VT for Direct I/O</b> option is enabled.
<b>Intel Trusted Execution Technology (TXT)</b>	
	Specifies whether a measured Virtual Machine Monitor (MVMM) can use the additional hardware capabilities provided by Intel Trusted Execution Technology. The following must be enabled in order to enable Intel TXT - <ul style="list-style-type: none"> <li>● Trusted Platform Module (TPM)</li> <li>● Intel Hyper-Threading</li> <li>● All CPU cores (Multi-Core Support)</li> <li>● Intel Virtualization Technology</li> <li>● Intel VT for Direct I/O</li> </ul> By default, the <b>Intel Trusted Execution Technology (TXT)</b> option is disabled.
<b>DMA Protection</b>	
Enable Pre-Boot DMA Support	Allows you to control the Pre-Boot DMA protection for both internal and external ports. This option does not directly enable DMA protection in the operating system.  <b>NOTE:</b> This option is not available when the virtualization setting for IOMMU is disabled (VT-d/AMD Vi). By default, the <b>Enable Pre-Boot DMA Support</b> option is enabled. For additional security, Dell Technologies recommends keeping the <b>Enable Pre-Boot DMA Support</b> option enabled.  <b>NOTE:</b> This option is provided only for compatibility purposes, since some older hardware is not DMA capable.



**Table 16. System setup options—Virtualization menu (continued)**

<b>Virtualization Support</b>	
Enable OS Kernel DMA Support	<p>Allows you to control the Kernel DMA protection for both internal and external ports. This option does not directly enable DMA protection in the operating system. For operating systems that support DMA protection, this setting indicates to the operating system that the BIOS supports the feature.</p> <p><b>i</b> <b>NOTE:</b> This option is not available when the virtualization setting for IOMMU is disabled (VT-d/AMD Vi).</p> <p>By default, the <b>Enable OS Kernel DMA Support</b> option is enabled.</p> <p><b>i</b> <b>NOTE:</b> This option is provided only for compatibility purposes, since some older hardware is not DMA capable.</p>

**Table 17. System setup options—Performance menu**

<b>Performance</b>	
<b>Multi-Core Support</b>	
Multiple Atom Cores	<p>Enables to change the number of Atom cores available to the operating system. The default value is set to the maximum number of cores.</p> <p>By default, the <b>All Cores</b> option is selected.</p>
<b>Intel SpeedStep</b>	
Enable Intel SpeedStep Technology	<p>Enables the computer to dynamically adjust processor voltage and core frequency, decreasing average power consumption and heat production.</p> <p>By default, the <b>Enable Intel SpeedStep Technology</b> option is enabled.</p>
<b>C-State Control</b>	
Enable C-State Control	<p>Enables or disables the ability of the CPU to enter and exit low-power state. When disabled, it disables all C-states. When enabled, it enables all C-states that the chipset or platform allows.</p> <p>By default, the <b>Enable C-State Control</b> option is enabled.</p>
<b>Intel Turbo Boost Technology</b>	
Enable Intel Turbo Boost Technology	<p>Enables the Intel TurboBoost mode of the processor. When enabled, the Intel TurboBoost driver increases the performance of the CPU or graphics processor.</p> <p>By default, the <b>Enable Intel Turbo Boost Technology</b> option is enabled.</p>
<b>Intel Hyper-Threading Technology</b>	
Enable Intel Hyper-Threading Technology	<p>Enables the Intel Hyper-Threading mode of the processor. When enabled, the Intel Hyper-Threading increases the efficiency of the processor resources when multiple threads run on each core.</p> <p>By default, the <b>Intel Hyper-Threading Technology</b> option is enabled.</p>
<b>Dynamic Tuning: Machine Learning</b>	
Enable Dynamic Tuning: Machine Learning	<p>Enables or disables operating system capability to enhance power tuning capabilities depending on the detected workloads.</p> <p><b>i</b> <b>NOTE:</b> This option is available for development only and is not customer visible.</p> <p>By default, the <b>Enable Dynamic Tuning: Machine Learning</b> option is enabled.</p>

**Table 18. System setup options—System Logs menu**

<b>System Logs</b>	
<b>BIOS Event Log</b>	

**Table 18. System setup options—System Logs menu (continued)**

<b>System Logs</b>	
Clear BIOS Event Log	Allows you to select option to keep or clear BIOS events logs. By default, the <b>Keep Log</b> option is selected.
<b>Thermal Event Log</b>	
Clear Thermal Event Log	Allows you to select option to keep or clear Thermal events logs. By default, the <b>Keep Log</b> option is selected.
<b>Power Event Log</b>	
Clear Power Event Log	Allows you to select option to keep or clear Power events logs. By default, the <b>Keep Log</b> option is selected.

## System and setup password


**Table 19. System and setup password**

<b>Password type</b>	<b>Description</b>
System password	Password that you must enter to log in to your system.
Setup password	Password that you must enter to access and make changes to the BIOS settings of your computer.

You can create a system password and a setup password to secure your computer.

 **CAUTION:** The password features provide a basic level of security for the data on your computer.

 **CAUTION:** Anyone can access the data that is stored on your computer if it is not locked and left unattended.

 **NOTE:** System and setup password feature is disabled.

## Assigning a system setup password

### Prerequisites

You can assign a new **System or Admin Password** only when the status is in **Not Set**.

### About this task

To enter the system setup, press F12 immediately after a power-on or reboot.

### Steps

1. In the **System BIOS** or **System Setup** screen, select **Security** and press Enter.  
The **Security** screen is displayed.
2. Select **System/Admin Password** and create a password in the **Enter the new password** field.  
Use the following guidelines to assign the system password:
  - A password can have up to 32 characters.
  - At least one special character: ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | }
  - Numbers 0 through 9.
  - Upper case letters from A to Z.
  - Lower case letters from a to z.
3. Type the system password that you entered earlier in the **Confirm new password** field and click **OK**.
4. Press Esc and save the changes as prompted by the pop-up message.

5. Press Y to save the changes.  
The computer restarts.

## Deleting or changing an existing system setup password


### Prerequisites

Ensure that the **Password Status** is Unlocked (in the System Setup) before attempting to delete or change the existing System and/or Setup password. You cannot delete or change an existing System or Setup password, if the **Password Status** is Locked.

### About this task

To enter the System Setup, press F12 immediately after a power-on or reboot.


### Steps

1. In the **System BIOS** or **System Setup** screen, select **System Security** and press Enter.  
The **System Security** screen is displayed.
2. In the **System Security** screen, verify that **Password Status** is **Unlocked**.
3. Select **System Password**, update, or delete the existing system password, and press Enter or Tab.
4. Select **Setup Password**, update, or delete the existing setup password, and press Enter or Tab.  
 **NOTE:** If you change the System and/or Setup password, reenter the new password when prompted. If you delete the System and/or Setup password, confirm the deletion when prompted.
5. Press Esc and a message prompts you to save the changes.
6. Press Y to save the changes and exit from System Setup.  
The computer restarts.

## Clearing BIOS (System Setup) and System passwords

### About this task


To clear the system or BIOS passwords, contact Dell technical support as described at [www.dell.com/contactdell](http://www.dell.com/contactdell).

-  **NOTE:** For information on how to reset Windows or application passwords, refer to the documentation accompanying Windows or your application.

## Updating the BIOS

### Updating the BIOS in Windows

#### Steps

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. Click **Product support**. In the **Search support** box, enter the Service Tag of your computer, and then click **Search**.  
 **NOTE:** If you do not have the Service Tag, use the SupportAssist feature to automatically identify your computer. You can also use the product ID or manually browse for your computer model.
3. Click **Drivers & Downloads**. Expand **Find drivers**.
4. Select the operating system installed on your computer.
5. In the **Category** drop-down list, select **BIOS**.
6. Select the latest version of BIOS, and click **Download** to download the BIOS file for your computer.
7. After the download is complete, browse the folder where you saved the BIOS update file.
8. Double-click the BIOS update file icon and follow the on-screen instructions.  
For more information, see knowledge base article [000124211](https://www.dell.com/support/000124211) at [www.dell.com/support](http://www.dell.com/support).

# Updating the BIOS using the USB drive in Windows

## Steps

1. Follow the procedure from step 1 to step 6 in [Updating the BIOS in Windows](#) to download the latest BIOS setup program file.
2. Create a bootable USB drive. For more information, see the knowledge base article [000145519](#) at [www.dell.com/support](http://www.dell.com/support).
3. Copy the BIOS setup program file to the bootable USB drive.
4. Connect the bootable USB drive to the computer that needs the BIOS update.
5. Restart the computer and press **F12**.
6. Select the USB drive from the **One Time Boot Menu**.
7. Type the BIOS setup program filename and press **Enter**.  
The **BIOS Update Utility** appears.
8. Follow the on-screen instructions to complete the BIOS update.

# Updating the BIOS in Linux and Ubuntu

To update the system BIOS on a computer that is installed with Linux or Ubuntu, see the knowledge base article [000131486](#) at [www.dell.com/support](http://www.dell.com/support).

# Updating the BIOS from the F12 One-Time boot menu


Update your computer BIOS using the BIOS update.exe file that is copied to a FAT32 USB drive and booting from the F12 One-Time boot menu.

## About this task

### BIOS Update

You can run the BIOS update file from Windows using a bootable USB drive or you can also update the BIOS from the F12 One-Time boot menu on the computer.

Most of the Dell computers built after 2012 have this capability, and you can confirm by booting your computer to the F12 One-Time Boot Menu to see if BIOS FLASH UPDATE is listed as a boot option for your computer. If the option is listed, then the BIOS supports this BIOS update option.

 **NOTE:** Only computers with BIOS Flash Update option in the F12 One-Time boot menu can use this function.

### Updating from the One-Time boot menu

To update your BIOS from the F12 One-Time boot menu, you need the following:

- USB drive formatted to the FAT32 file system (key does not have to be bootable)
- BIOS executable file that you downloaded from the Dell Support website and copied to the root of the USB drive
- AC power adapter that is connected to the computer
- Functional computer battery to flash the BIOS

Perform the following steps to perform the BIOS update flash process from the F12 menu:

 **CAUTION:** Do not turn off the computer during the BIOS update process. The computer may not boot if you turn off your computer.

## Steps

1. From a turn off state, insert the USB drive where you copied the flash into a USB port of the computer.
2. Turn on the computer and press F12 to access the One-Time Boot Menu, select BIOS Update using the mouse or arrow keys then press Enter.  
The flash BIOS menu is displayed.
3. Click **Flash from file**.
4. Select external USB device.
5. Select the file and double-click the flash target file, and then click **Submit**.
6. Click **Update BIOS**. The computer restarts to flash the BIOS.



7. The computer will restart after the BIOS update is completed.

# Troubleshooting

## Handling swollen Lithium-ion batteries

Like most laptops, Dell laptops use lithium-ion batteries. One type of lithium-ion battery is the lithium-ion polymer battery. Lithium-ion polymer batteries have increased in popularity in recent years and have become standard in the electronics industry due to customer preferences for a slim form factor (especially with newer ultra-thin laptops) and long battery life. Inherent to lithium-ion polymer battery technology is the potential for swelling of the battery cells.

Swollen battery may impact the performance of the laptop. To prevent possible further damage to the device enclosure or internal components leading to malfunction, discontinue the use of the laptop and discharge it by disconnecting the AC adapter and letting the battery drain.

Swollen batteries should not be used and should be replaced and disposed of properly. We recommend contacting Dell product support for options to replace a swollen battery under the terms of the applicable warranty or service contract, including options for replacement by a Dell authorized service technician.

The guidelines for handling and replacing Lithium-ion batteries are as follows:

- Exercise caution when handling Lithium-ion batteries.
- Discharge the battery before removing it from the computer. To discharge the battery, unplug the AC adapter from the computer and operate the computer only on battery power. When the computer will no longer turn on when the power button is pressed, the battery is fully discharged.
- Do not crush, drop, mutilate, or penetrate the battery with foreign objects.
- Do not expose the battery to high temperatures, or disassemble battery packs and cells.
- Do not apply pressure to the surface of the battery.
- Do not bend the battery.
- Do not use tools of any type to pry on or against the battery.
- If a battery gets stuck in a device as a result of swelling, do not try to free it as puncturing, bending, or crushing a battery can be dangerous.
- Do not attempt to reassemble a damaged or swollen battery into a laptop.
- Swollen batteries that are covered under warranty should be returned to Dell in an approved shipping container (provided by Dell)—this step is to comply with transportation regulations. Swollen batteries that are not covered under warranty should be disposed of at an approved recycling center. Contact Dell product support at <https://www.dell.com/support> for assistance and further instructions.
- Using a non-Dell or incompatible battery may increase the risk of fire or explosion. Replace the battery only with a compatible battery purchased from Dell that is designed to work with your Dell computer. Do not use a battery from other computers with your computer. Always purchase genuine batteries from <https://www.dell.com> or otherwise directly from Dell.

Lithium-ion batteries can swell for various reasons such as age, number of charge cycles, or exposure to high heat. For more information about how to improve the performance and lifespan of the laptop battery and to minimize the possibility of occurrence of the issue, see [Dell Laptop Battery - Frequently Asked Questions](#).

## Locate the Service Tag or Express Service Code of your Dell computer

Your Dell computer is uniquely identified by a Service Tag or Express Service Code. To view relevant support resources for your Dell computer, we recommend entering the Service Tag or Express Service Code at [www.dell.com/support](http://www.dell.com/support).

For more information on how to find the Service Tag for your computer, see [Locate the Service Tag for your Dell Laptop](#).

# System diagnostic lights

When blinking in different patterns, the LED on the Caps Lock button indicates the respective issues that your computer is encountering.

## Caps Lock button LED

The following table lists the status of your computer based on the Caps Lock button LED.

**Table 20. Caps Lock button LED**

Caps Lock button LED	Status of computer
<b>Solid white</b>	<ul style="list-style-type: none"><li>• The power adapter is connected, and the battery is fully charged.</li><li>• The power adapter is connected, and the battery has more than five percent charge.</li></ul>
<b>Amber</b>	The computer is running on battery, and the battery has less than five percent charge.
<b>Off</b>	The computer is in sleep state, hibernation, or turned off.

**Table 21. LED codes**

Diagnostic light codes	Problem description
<b>2,1</b>	Processor failure
<b>2,2</b>	System board: BIOS or ROM (Read-Only Memory) failure
<b>2,3</b>	No memory or RAM (Random-Access Memory) detected
<b>2,4</b>	Memory or RAM (Random-Access Memory) failure
<b>2,5</b>	Invalid memory installed
<b>2,6</b>	System-board or chipset error
<b>2,7</b>	Display failure
<b>2,8</b>	Display power failure
<b>3,2</b>	PCI, video card/chip failure
<b>3,3</b>	Recovery image not found
<b>3,4</b>	Recovery image found but invalid
<b>3,5</b>	Power-rail failure
<b>3,6</b>	System BIOS Flash incomplete
<b>3,7</b>	Management Engine (ME) error

# SupportAssist diagnostics

## About this task

The SupportAssist diagnostics (previously known as ePSA diagnostics) performs a complete check of your hardware. The SupportAssist diagnostics is embedded in the BIOS and is launched by it internally. The SupportAssist diagnostics provides a set of options for particular devices or device groups. It allows you to:

- Run tests automatically or in an interactive mode.
- Repeat tests
- Display or save test results
- Run thorough tests to introduce additional test options and provide extra information about the failed device(s)
- View status messages that indicate if the tests are completed successfully
- View error messages that indicate if problems were encountered during the test

**NOTE:** Some tests are meant for specific devices and require user interaction. Ensure that you are present in front of the computer when the diagnostic tests are performed.

For more information, see [SupportAssist Pre-Boot System Performance Check](#).

## Built-in self-test (BIST)

### M-BIST

M-BIST (Built In Self-Test) is the system board's built-in self-test diagnostics tool that improves the diagnostics accuracy of system board embedded controller (EC) failures.

**NOTE:** M-BIST can be manually initiated before POST (Power On Self Test).

### How to run M-BIST

**NOTE:** M-BIST must be initiated on the system from a power-off state either connected to AC power or with battery only.

1. Press and hold both the **M** key on the keyboard and the **power button** to initiate M-BIST.
2. With both the **M** key and the **power button** held down, the Caps Lock button LED may exhibit two states:
  - a. OFF: No fault detected with the system board
  - b. AMBER: Indicates a problem with the system board
3. If there is a failure with the system board, the Caps Lock button LED will flash one of the following error codes for 30 seconds:

**Table 22. LED error codes**

Blinking Pattern		Possible Problem
Amber	White	
2	1	CPU Failure
2	8	LCD Power Rail Failure
1	1	TPM Detection Failure
2	4	Unrecoverable SPI Failure

4. If there is no failure with the system board, the LCD will cycle through the solid color screens described in the LCD-BIST section for 30 seconds and then power off.

## LCD Built-in Self Test (BIST)


Dell laptops have a built-in diagnostic tool that helps you determine if the screen abnormality you are experiencing is an inherent problem with the LCD (screen) of the Dell laptop or with the video card (GPU) and PC settings.

When you notice screen abnormalities like flickering, distortion, clarity issues, fuzzy or blurry image, horizontal or vertical lines, color fade etc., it is always a good practice to isolate the LCD (screen) by running the Built-In Self Test (BIST).

### How to invoke LCD BIST Test

1. Power off the Dell laptop.
2. Disconnect any peripherals that are connected to the laptop. Connect only the AC adapter (charger) to the laptop.
3. Ensure that the LCD (screen) is clean (no dust particles on the surface of the screen).
4. Press and hold **D** key and **Power on** the laptop to enter LCD built-in self test (BIST) mode. Continue to hold the D key, until the system boots up.
5. The screen will display solid colors and change colors on the entire screen to white, black, red, green, and blue twice.
6. Then it will display the colors white, black and red.

7. Carefully inspect the screen for abnormalities (any lines, fuzzy color or distortion on the screen).
8. At the end of the last solid color (red), the system will shut down.

 **NOTE:** Dell SupportAssist Pre-boot diagnostics upon launch, initiates an LCD BIST first, expecting a user intervention confirm functionality of the LCD.

## Recovering the operating system

When your computer is unable to boot to the operating system even after repeated attempts, it automatically starts Dell SupportAssist OS Recovery.

Dell SupportAssist OS Recovery is a standalone tool that is preinstalled in all Dell computers installed with Windows operating system. It consists of tools to diagnose and troubleshoot issues that may occur before your computer boots to the operating system. It enables you to diagnose hardware issues, repair your computer, back up your files, or restore your computer to its factory state.


You can also download it from the Dell Support website to troubleshoot and fix your computer when it fails to boot into their primary operating system due to software or hardware failures.

For more information about the Dell SupportAssist OS Recovery, see *Dell SupportAssist OS Recovery User's Guide* at [www.dell.com/serviceabilitytools](http://www.dell.com/serviceabilitytools). Click **SupportAssist** and then, click **SupportAssist OS Recovery**.

## WiFi power cycle

### About this task

If your computer is unable to access the Internet due to WiFi connectivity issues, a WiFi power cycle procedure may be performed. The following procedure provides the instructions on how to conduct a WiFi power cycle:

 **NOTE:** Some ISPs (Internet Service Providers) provide a modem/router combo device.

### Steps

1. Turn off your computer.
2. Turn off the modem.
3. Turn off the wireless router.
4. Wait for 30 seconds.
5. Turn on the wireless router.
6. Turn on the modem.
7. Turn on your computer.

## Drain residual flea power (perform hard reset)

### About this task

Flea power is the residual static electricity that remains in the computer even after it has been powered off and the battery is removed.

For your safety, and to protect the sensitive electronic components in your computer, you are requested to drain residual flea power before removing or replacing any components in your computer.


Draining residual flea power, also known as a performing a "hard reset", is also a common troubleshooting step if your computer does not turn on or boot into the operating system.

### To drain residual flea power (perform a hard reset)


### Steps

1. Turn off your computer.
2. Disconnect the power adapter from your computer.
3. Remove the [base cover](#).



 **NOTE:** The battery must be disconnected from the system board (see Steps 1 to 2 in [Removing the battery](#)).

4. Press and hold the power button for 20 seconds to drain the flea power.
5. Install the [base cover](#).
6. Connect the power adapter to your computer.
7. Turn on your computer.


 **NOTE:** For more information about performing a hard reset, see the knowledge base article [000130881](#) at [www.dell.com/support](http://www.dell.com/support).

## Backup media and recovery options

It is recommended to create a recovery drive to troubleshoot and fix problems that may occur with Windows. Dell proposes multiple options for recovering Windows operating system on your Dell PC. For more information, see [Dell Windows Backup Media and Recovery Options](#).


## Real Time Clock—RTC reset

The Real Time Clock (RTC) reset function allows you or the service technician to recover the recently launched model Dell Latitude and Precision systems from **No POST/No Boot/No Power** situations. You can initiate the RTC reset on the system from a power-off state only if it is connected to AC power. Press and hold the power button for 25 seconds. The system RTC reset occurs after you release the power button.

 **NOTE:** If AC power is disconnected from the system during the process or the power button is held longer than 40 seconds, the RTC reset process gets aborted.

The RTC reset will reset the BIOS to Defaults, un-provision Intel vPro and reset the system date and time. The following items are unaffected by the RTC reset:

- Service Tag
- Asset Tag
- Ownership Tag
- Admin Password
- System Password
- HDD Password
- Key Databases
- System Logs

 **NOTE:** The IT administrator's vPro account and password on the system will be un-provisioned. The system needs to go through the setup and configuration process again to reconnect it to the vPro server.

The below items may or may not reset based on your custom BIOS setting selections:



- Boot List
- Enable Legacy Option ROMs
- Secure Boot Enable
- Allow BIOS Downgrade

# Getting help and contacting Dell

## Self-help resources


You can get information and help on Dell products and services using these self-help resources:


**Table 23. Self-help resources**

Self-help resources	Resource location
Information about Dell products and services	<a href="http://www.dell.com">www.dell.com</a>
My Dell app	
Tips	
Contact Support	In Windows search, type <code>Contact Support</code> , and press Enter.
Online help for operating system	<a href="http://www.dell.com/support/windows">www.dell.com/support/windows</a> <a href="http://www.dell.com/support/linux">www.dell.com/support/linux</a>
Access top solutions, diagnostics, drivers and downloads, and learn more about your computer through videos, manuals and documents.	Your Dell computer is uniquely identified by a Service Tag or Express Service Code. To view relevant support resources for your Dell computer, enter the Service Tag or Express Service Code at <a href="http://www.dell.com/support">www.dell.com/support</a> .  For more information on how to find the Service Tag for your computer, see <a href="#">Locate the Service Tag on your computer</a> .
Dell knowledge base articles for a variety of computer concerns	<ol style="list-style-type: none"> <li>1. Go to <a href="http://www.dell.com/support">www.dell.com/support</a>.</li> <li>2. On the menu bar at the top of the Support page, select <b>Support &gt; Knowledge Base</b>.</li> <li>3. In the Search field on the Knowledge Base page, type the keyword, topic, or model number, and then click or tap the search icon to view the related articles.</li> </ol>

## Contacting Dell

To contact Dell for sales, technical support, or customer service issues, see [www.dell.com/contactdell](http://www.dell.com/contactdell).

 **NOTE:** Availability varies by country/region and product, and some services may not be available in your country/region.

 **NOTE:** If you do not have an active Internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell product catalog.