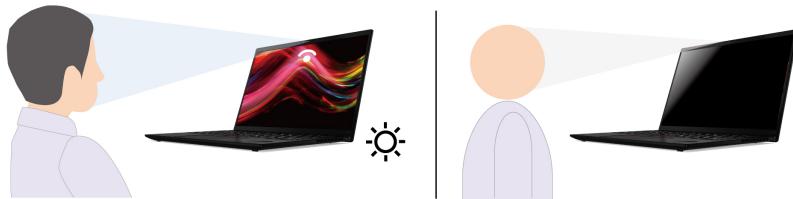


- **Zero Touch Login:** Wake your computer from sleep mode. With Windows Hello Facial Recognition, you can log in without touching your computer.



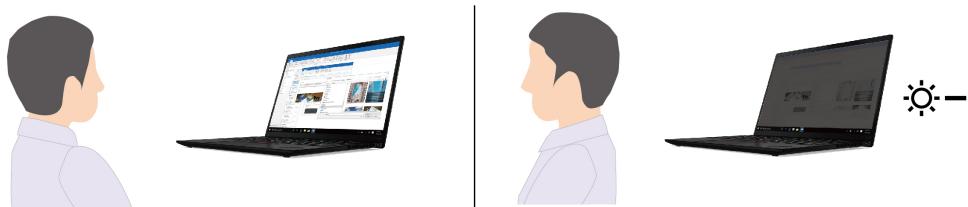
**Note:** When **Face Sensing** is enabled, only users who have set up Windows Hello Face can wake the computer up.



- **Zero Touch Lock:** Lock your computer screen automatically whenever you step away.



- **Adaptive Dimming:** Track your attention based on head position and eye contact with the display. When your focus is not on your computer screen, the display will dim to save battery power.



#### Notes:

- The feature does not work in the following cases:
  - the computer is in tent, tablet, or stand mode.
  - the computer is in hibernation mode or has been turned off.
  - the camera shutter is closed.
  - you set the power options to never turn off the display in the OS settings.
- The feature might not work properly in the following cases:
  - when used in bright back light or very dark environment.

- when your face is partially hidden by your clothing or mask.
- when the camera recognizes a face image behind you like a poster or picture.
- For some countries or regions, this feature might be disabled according to local regulations.

---

## Lock on leave function (for selected models only)

Your computer with FHD camera supports the lock on leave function with ultrasound-based human presence detection. The computer display will first dim and then lock when it senses you have walked away. This provides added security and improves battery life.



Lock on leave function is enabled by default. To change the settings:

1. Open the Vantage app, and then click **Device** → **Smart Assist**.
2. Slide the **Zero Touch Lock** switch to disable or enable the function.

### Notes:

- The lock on leave function does not work if you set the power options to never turn off the display in the OS settings.
- If the Vantage app is uninstalled, this function will be enabled automatically. You can change the settings through the UEFI BIOS menu:
  1. Restart the computer. When the logo is displayed, press F1 to enter the UEFI BIOS menu.
  2. Select **Security** → **Intelligent Security**.
  3. Slide the **User Presence Sensing** switch to disable or enable the function.
- For some countries or regions, the lock on leave function might be disabled according to local regulations.

---

## Protect your privacy (for selected models)

### Use the ePrivacy screen

Your computer might come with an ePrivacy screen. It can reduce screen visibility from side angles to protect screen content against visual hacking. By default, this function is disabled. You can press F12 or Fn + D to enable it. You will be prompted by the on-screen icon or every time the function is enabled or disabled.

Your ePrivacy screen can be automatically enabled in case that you are required to input passwords. By default, this automatic function for passwords is disabled. You can enable it on the Vantage app.

### Set the privacy level

The privacy level of this function varies depending on the screen brightness level, the contrast ratio, and the physical environment where you are using this function.

- Press F5 to increase the privacy level.

- Press F6 to decrease the privacy level.

---

## Protect data against power loss

NVMe (Non-Volatile Memory express) M.2 solid-state drive features the Lenovo-unique PLP (Power Loss Protection) function to avoid data loss or damage. If your computer is not responding and you might have to shut down your computer by pressing and holding the power button for several seconds. In this case, the PLP function enables your computer data to be saved timely. However, there is no guarantee that all data is saved in any situation. To check the type of your M.2 solid-state drive:

1. Restart the computer. When the logo screen is displayed, press F10 to enter the Lenovo diagnostics window.
2. On the TOOLS tab, select **SYSTEM INFORMATION → STORAGE** using the arrow keys.
3. Locate the **Device Type** section to check the information.

---

## UEFI BIOS passwords

You can set passwords in UEFI (Unified Extensible Firmware Interface) BIOS (Basic Input/Output System) to strengthen the security of your computer.

### Password types

You can set a power-on password, supervisor password, system management password, or NVMe password in UEFI BIOS to prevent unauthorized access to your computer. However, you are not prompted to enter any UEFI BIOS password when your computer resumes from sleep mode.

#### Power-on password

If you set a power-on password, a window is displayed on the screen when you turn on the computer. Enter the correct password to use the computer.

#### Supervisor password

The supervisor password protects the system information stored in UEFI BIOS. When entering the UEFI BIOS menu, enter the correct supervisor password in the window prompted. You also can press Enter to skip the password prompt. However, you cannot change most of the system configuration options in UEFI BIOS.

If you have set both the supervisor password and power-on password, you can use the supervisor password to access your computer when you turn it on. The supervisor password overrides the power-on password.

#### System management password

The system management password can also protect the system information stored in UEFI BIOS like a supervisor password, but it has lower authority by default. The system management password can be set through the UEFI BIOS menu or through Windows Management Instrumentation (WMI) with the Lenovo client-management interface.

You can enable the system management password to have the same authority as the supervisor password to control security-related features. To customize the authority of the system management password through the UEFI BIOS menu:

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Security → Password → System Management Password Access Control**.
3. Follow the on-screen instructions.

If you have set both the supervisor password and the system management password, the supervisor password overrides the system management password. If you have set both the system management password and the power-on password, the system management password overrides the power-on password.

### **NVMe passwords**

The NVMe password prevents unauthorized access to the data on the storage drive. When an NVMe password is set, you are prompted to type a correct password each time you try to access the storage drive.

- **Single Password**

When a Single NVMe password is set, the user must enter the user NVMe password to access files and applications on the storage drive.

- **Dual Password (User + Admin)**

The admin NVMe password is set and used by a system administrator. It enables the administrator to access any storage drive in a system or any computer connected in the same network. The administrator can also assign a user NVMe password for each computer in the network. The user of the computer can change the user NVMe password as desired, but only the administrator can remove the user NVMe password.

When prompted to enter an NVMe password, press F1 to switch between the admin NVMe password and user NVMe password.

**Notes:** The NVMe password is not available in the following situations:

- A Trusted Computing Group (TCG) Opal-compliant storage drive and a TCG Opal management software program are installed in the computer, and the TCG Opal management software program is activated.
- An eDrive storage drive is installed in the computer preinstalled with the Windows operating system.

## **Set, change, and remove a password**

Before you start, print these instructions.

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Security** → **Password** by using the arrow keys.
3. Select the password type. Then, follow the on-screen instructions to set, change, or remove a password.

You should record all your passwords and store them in a safe place. If you forget any of your passwords, any potential repair actions required are not covered under warranty.

### **What to do if you forget your power-on password**

If you forget your power-on password, do the following to remove the power-on password:

- If you have set a supervisor password and remember it:
  1. Restart the computer. When the logo screen is displayed, immediately press F1.
  2. Type the supervisor password to enter the UEFI BIOS menu.
  3. Select **Security** → **Password** → **Power-On Password** by using the arrow keys.
  4. Type the current supervisor password in the **Enter Current Password** field. Then, leave the **Enter New Password** field blank, and press Enter twice.
  5. In the Changes have been saved window, press Enter.
  6. Press F10 to save changes and exit the UEFI BIOS menu.

- If you have not set a supervisor password, contact a Lenovo authorized service provider to have the power-on password removed.

### What to do if you forget your NVMe password

If you forget your NVMe password (Single password) or both user and admin NVMe passwords (Dual password), Lenovo cannot reset your passwords or recover data from the storage drive. You can contact a Lenovo authorized service provider to have the storage drive replaced. A fee will be charged for parts and service. If the storage drive is a CRU (Customer Replaceable Unit), you can also contact Lenovo to purchase a new storage drive to replace the old one by yourself. To check whether the storage drive is a CRU and the relevant replacement procedure, see Chapter 6 “CRU replacement” on page 51.

### What to do if you forget your supervisor password

If you forget your supervisor password, there is no service procedure to remove the password. You have to contact a Lenovo authorized service provider to have the system board replaced. A fee will be charged for parts and service.

### What to do if you forget your system management password

If you forget your system management password, do the following to remove the system management password:

- If you have set a supervisor password and remember it:
  1. Restart the computer. When the logo screen is displayed, immediately press F1.
  2. Type the supervisor password to enter the UEFI BIOS menu.
  3. Select **Security** → **Password** → **System Management Password** by using the arrow keys.
  4. Type the current supervisor password in the **Enter Current Password** field. Then, leave the **Enter New Password** field blank, and press Enter twice.
  5. In the Changes have been saved window, press Enter.
  6. Press F10 to save changes and exit the UEFI BIOS menu.
- If you have not set a supervisor password, contact a Lenovo authorized service provider to have the system management password removed.

## Associate your fingerprints with passwords (for selected models)

Do the following to associate your fingerprints with the power-on password and NVMe password:

1. Turn off and then turn on the computer.
2. When prompted, scan your finger on the fingerprint reader.
3. Enter your power-on password, NVMe password, or both as required. The association is established.

When you start the computer again, you can use your fingerprints to log in to the computer without entering your Windows password, power-on password, or NVMe password. To change settings, press F1 to enter the UEFI BIOS menu, and then select **Security** → **Fingerprint**.

**Attention:** If you always use your fingerprint to log in to the computer, you might forget your passwords. Write down your passwords, and keep them in a safe place.

---

## FIDO (Fast Identity Online) authentication

Your computer supports FIDO (Fast Identity Online) authentication feature. This feature works as an alternative to password-based authentication to achieve passwordless authentication. This feature only works when a power-on password is set in UEFI BIOS and the FIDO2 USB device is registered in

ThinkShield™ Passwordless Power-On Device Manager. With this feature, you can input the power-on password or use the registered FIDO2 USB device to power on your computer.

### Register your FIDO2 USB device in ThinkShield Passwordless Power-On Device Manager

1. Turn on the computer.
2. Press F12 during the power-on process.
3. If you set a power-on password, you are prompted to enter the correct password.
4. Select **App Menu → ThinkShield Passwordless Power-On Device Manager** and press Enter.
5. Insert the FIDO2 USB device to register the device by following steps:
  - a. Select the available FIDO2 USB device that you want to register in the **Discovered Devices** field.
  - b. Click **Yes** in the displayed window to confirm the device you selected.
  - c. If you set a power-on password, you are prompted to enter the correct password.
  - d. The **User operation request** window is displayed. You are prompted to press the button on the connected FIDO2 USB device, and then follow the on-screen instruction to close the window.
  - e. Press Esc to exit and restart your computer.

#### Notes:

- If you want to unregister your devices, click the available FIDO2 USB device that you want to unregister in the **My Device** field and enter the correct power-on password for verification.
- If you use more than one FIDO2 USB device with a common identifier for registration, only one device is available.

### Log in to the System with Passwordless Power-On Authentication

1. Restart the computer.
2. **ThinkShield Passwordless Power-On Authentication** window is displayed.
3. Insert your registered FIDO2 USB device for detection.
4. Then follow the on-screen instruction to press the button on your FIDO2 USB device for verification.
5. After your device is verified, the power-on process continues.

**Note:** You should insert the FIDO2 USB device or enter the power-on password within 60 seconds. Otherwise, your computer will shut down automatically.

---

## Chapter 5. Configure advanced settings

---

### UEFI BIOS

UEFI BIOS is the first program that the computer runs. When the computer turns on, UEFI BIOS performs a self test to make sure that various devices in the computer are functioning.

#### Enter the UEFI BIOS menu

Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.

#### Navigate in the UEFI BIOS interface

You can navigate in the UEFI BIOS interface by pressing the following keys:

- F1: General Help
- F9: Setup Defaults
- F10: Save and Exit
- F5 / F6: Change boot priority order
- ↑ ↓ or PgUp / PgDn: Select / Scroll page
- ← →: Move keyboard focus
- Esc: Back / Close dialog
- Enter: Select / Open submenu

#### Set the system date and time

1. Restart the computer. When the logo screen is displayed, press F1.
2. Select **Date/Time** and set the system date and time as desired.
3. Press F10 to save changes and exit.

#### Change the startup sequence

1. Restart the computer. When the logo screen is displayed, press F1.
2. Select **Startup** → **Boot**. Then, press Enter. The default device order list is displayed.

**Note:** No bootable device is displayed if the computer cannot start from any devices or the operating system cannot be found.

3. Set the startup sequence as desired.
4. Press F10 to save the changes and exit.

To change the startup sequence temporarily:

1. Restart the computer. When the logo screen is displayed, press F12.
2. Select the device that you want the computer to start from and press Enter.

#### View UEFI BIOS Event logs

The UEFI BIOS Event log viewer provides the brief information about UEFI BIOS events. Do the following to view the logs:

1. Restart the computer. When the logo screen is displayed, press F1.

2. Select **Main** → **BIOS Event log**. Then, press Enter. The UEFI BIOS Event log interface is displayed.
3. Navigate the interface by pressing the following keys, and then check details by selecting each item.
  - ↑ ↓: Move keyboard focus
  - PgUp / PgDn: Scroll page
  - Enter: Select
  - F3: Exit

The following UEFI BIOS event logs might be listed on your screen depending on UEFI BIOS activities. Each log consists of a date, a time, and a description of the event.

- **Power On** event: This log shows the Power On Self Test (POST) routine has started with the power-on process. It includes the power-on reason, the boot mode, and the shutdown reason.
- **Subcomponent Code Measurement** event: This log shows the subcomponent code measurement has worked. It includes the validation result of each component.
- **System Preboot Authentication** event: This log shows what credential is provided to gain preboot authentication. It includes the installed password, the password type, the input device, and the authentication result.
- **BIOS Password Change** event: This log shows the change history of the UEFI BIOS passwords. It includes the password type, the type and result of the event.
- **Subcomponent Self-healing** event: This log shows the information about the subcomponent where the recovery event occurred. It includes the cause and result of the event, and the recovered firmware version.
- **BIOS Setup Configuration Change** event: This log shows the change history of the UEFI BIOS Setup configuration. It includes the item name and value.
- **Device Change** event: This log shows the change history of devices. It includes the cause and type of the event.
- **System Boot** event: This log shows which device was utilized to boot the system. It includes the boot option, the description, and the file path list.
- **System Tamper** event: This log shows the occurrence of system tamper events. It includes the cause and type of the event.
- **POST Error** event: This log shows the occurrence of errors during the POST routine. It includes the error code.
- **Flash Update** event: This log shows the occurrence of flash update. It includes the cause and result of the event, and the updated firmware version.
- **Set On-Premise** event: This log shows the change history of on-premise boot settings. It includes the value of on-premise settings and the change method.
- **Capsule Update** event: This log shows the occurrence of UEFI capsule firmware update. It includes the cause and result of the event, and the updated firmware version.
- **Log Cleared** event: This log shows UEFI BIOS event logs are cleared. It includes the cause and result of the event.
- **Shutdown / Reboot** event: This log shows the UEFI BIOS is successfully shut down or the system is rebooted. It includes the cause and type of the event.

## Detect memory retraining (for Intel models only)

Memory retraining is a process to initialize the memory module and run diagnostic tests for the memory module in your computer. The memory retraining might occur during POST if any of the following situations is detected:

- Memory module replacement

- Total Memory Encryption setting change in UEFI BIOS
- Memory Reference Code (MRC) change when UEFI BIOS update

When memory retraining occurs, the screen might be blank. You might see the LED indicators on Esc, F1, and F4 blinking sequentially to indicate the progress. Do not press the power button to interrupt the process. Wait a few minutes until the logo screen is displayed.

## Customize BIOS Defaults

The feature provides a solution to backup your preferred BIOS Setup settings. It helps you to save the BIOS Setup settings as customized BIOS default settings, load them to current BIOS settings when needed, and reset the settings to Setup Defaults.

### Save the customized settings configuration

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Restart** → **Save Custom Defaults**.
3. Click **Yes** to save the settings configuration you customized.

### Load the customized settings configuration

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Restart** → **Load Custom Defaults**.
3. Click **Yes** to load the customized settings configuration you saved.

You can also press F9 and click **Custom Defaults** to load the customized settings configuration.

**Note:** **Load Custom Defaults** is unavailable if no customized BIOS default settings are saved.

### Reset the settings configuration to Setup Defaults

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Restart** → **Load Factory Defaults**.
3. Click **Yes** to reset the settings configuration to Setup Defaults.

You can also press F9 and click **Factory Defaults** to reset the settings configuration to Setup Defaults.

## Reset system to factory defaults

This feature allows you to reset the UEFI BIOS to the factory default settings, including all UEFI BIOS settings and internal data. It helps you wipe user data in case that you want to dispose of or reuse your computer.

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Security** → **Reset System to Factory Defaults** and press Enter.
3. Several warning windows might be displayed. Do the following before resetting the system to the factory default settings:
  - a. Deactivate the Absolute Persistence Module.
  - b. Remove the NVMe password if you have set one.
4. For computer models with RAID settings, a window is displayed to remind you of data damage. Select **Yes** to proceed.
5. A window is displayed to confirm all UEFI BIOS settings will be reset. Select **Yes** to proceed.

**Note:** If the **Intel AMT control** and **Absolute Persistence(R) Module** are permanently disabled, these settings cannot be reset successfully.

6. Enter the supervisor password, system management password or power-on password in the window prompted.

Your computer will restart immediately. It takes a few minutes to complete the initialization process. Your computer screen might be blank during this process. This is normal and you should not interrupt it.

**Notes:** Use ThinkShield Secure Wipe feature for ThinkPad 2019 or later models by following steps:

1. Restart the computer. When the logo screen is displayed, press F12 to enter UEFI BIOS boot menu.
2. Press tab to switch to **App Menu**.
3. Select **ThinkShield Secure Wipe** from the list.
4. Follow the on-screen instructions to wipe the disk.

## ThinkShield secure wipe

ThinkShield secure wipe feature is ThinkPad Drive Erase Utility for the Resetting the Cryptographic Key and the Erasing the Solid State Drive. This feature provides you a secure method to wipe all the data on your computer.

Do the following to use ThinkShield secure wipe feature :

1. Restart the computer. When the logo screen is displayed, press F12.
2. Select **App Menu** → **ThinkShield secure wipe**, and then follow the on-screen instructions.

## Recover the UEFI BIOS

If the UEFI BIOS is corrupted or maliciously attacked, it can self-recover and restore your computer from the last uncorrupted and secure backup. This function protects your computer data.

During the UEFI BIOS self-recovery, the screen might be blank. You can check the progress based on blinking modes of the LED indicators on Esc, F1, and F4. For details, refer to the following table.

**Note:** Do not press the power button to interrupt the progress. Wait a few minutes until the logo screen is displayed.

Blinking modes	Self-recovery progress
LED indicator on Esc blinks	0% to 32%
LED indicators on Esc and F1 blink simultaneously	33% to 65%
LED indicators on Esc, F1 and F4 blink simultaneously	66% to 100%

## Update UEFI BIOS

When you install a new program, device driver, or hardware component, you might need to update UEFI BIOS.

Download and install the latest UEFI BIOS update package by one of the following methods:

- Open the Vantage app to check the available update packages. If the latest UEFI BIOS update package is available, follow the on-screen instructions to download and install the package.
- Go to <https://pcsupport.lenovo.com> and select the entry for your computer. Then, follow the on-screen instructions to download and install the latest UEFI BIOS update package.

**Note:** During the UEFI BIOS update process, MRC change might cause memory retraining. Memory retraining is a process to initialize the memory module and run diagnostic tests for the memory module in your computer. When memory retraining occurs, the screen might be blank. You might see the LED indicators on Esc, F1, and F4 blinking sequentially to indicate the progress. Do not press the power button to interrupt the process. Wait a few minutes until the logo screen is displayed.

To know more about UEFI BIOS, visit Knowledge Base of your computer at <https://pcsupport.lenovo.com>.

## Cloud bare metal recovery (for selected models)

This feature enables you to remove all user files on your computer and restore the Windows operating system from Cloud (Microsoft® Connected System Recovery). Before using this feature, read the following information.

### Notes:

- This feature will restore your computer to the Windows operating system preinstalled at the factory. Do not use this feature if a customized operating system is installed on your computer, otherwise the customized functions or applications cannot be restored.
- This feature only works with wired network (connected via the Ethernet connector on your computer) and wireless network (WPA2 personal only).

Do the following to restore the Windows operating system:

1. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
2. Select **Config → Reinstall Windows from Cloud**. Follow the on-screen instructions to enable this feature.
3. Press F10 to save changes and exit.
4. The computer will restart automatically. When the logo screen is displayed, press F12.
5. Select **App Menu → Reinstall Windows from Cloud**, and then follow the on-screen instructions.

If the recovery process fails, you still have other options to restore the Windows operating system. For more information, refer to “Self-help resources” on page 67.

---

## Install a Windows operating system and drivers

This section provides instructions on installing a Windows operating system and device drivers

### Install a Windows operating system

Microsoft® constantly makes updates to the Windows operating system. Before installing a particular Windows version, check the compatibility list for the Windows version. For details, go to <https://support.lenovo.com/us/en/solutions/windows-support>.

### Attention:

- It is recommended that you update your operating system through official channels. Any unofficial update might cause security risks.
- The process of installing a new operating system deletes all the data on your internal storage drive, including the data stored in a hidden folder.

### Notes:

1. For models with a Trusted Platform Module, if you are using the Windows BitLocker® Drive Encryption feature, ensure that you have disabled the feature. You can re-enable the feature after the operating system installation is complete.

2. Ensure that the security-related features (Security Chip, Virtualization, and Secure Boot) are enabled.

To access the security-related features in the UEFI BIOS menu:

- a. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.
- b. Select **Security** and select the security-related features. Then, press Enter. Ensure that the security-related features are enabled.
- c. Press F10 to save the settings and exit.

3. Network connection is required to the installation of Windows 11.

### Installation procedures

1. Connect the drive that contains the operating system installation program to the computer.

To create the installation media, refer to <https://support.microsoft.com/windows>.

2. Restart the computer. When the logo screen is displayed, press F1 to enter the UEFI BIOS menu.

3. Select **Startup** → **Boot** to open the **Boot Priority Order** submenu.

4. Change the startup sequence:

- a. Select the drive that contains the operating system installation program, such as **USB HDD**. Then, press Esc.
- b. Press F10 to save the setting and exit.

**Attention:** After you change the startup sequence, ensure that you select the correct device during a copy, save, or format operation. If you select the wrong device, the data on that device might be erased or overwritten.

**Note:** If the system cannot boot from the selected drive, disable **Secure Boot** and try again. Ensure that you re-enable the feature after the operating system installation is complete.

5. Follow the on-screen instructions to install the device drivers and necessary programs.

### Install device drivers

You should download the latest driver for a component when you notice poor performance from that component or when you added a component. This action might eliminate the driver as the potential cause of a problem. Download and install the latest driver by one of the following methods:

- Open the Vantage app to check the available update packages. Select the update packages you want, and then follow the on-screen instructions to download and install the packages.
- Go to <https://pcsupport.lenovo.com> and select the entry for your computer. Then, follow the on-screen instructions to download and install necessary drivers and software.
- Apply Windows Update to get the latest updates, such as the security patches. Then, follow the on-screen instructions to download and install the necessary updates.

---

## Chapter 6. CRU replacement

Customer Replaceable Units (CRUs) are parts that can be replaced by the customer. The computers contain the following types of CRUs:

- **Self-service CRUs:** Refer to parts that can be replaced easily by customer themselves or by trained service technicians at an additional cost.
- **Optional-service CRUs:** Refer to parts that can be replaced by customers with a greater skill level. Trained service technicians can also provide service to replace the parts under the type of warranty designated for the customer's machine.

If you intend on installing a CRU, Lenovo will ship the CRU to you. CRU information and replacement instructions are shipped with your product and are available from Lenovo at any time upon request. You might be required to return the defective part that is replaced by the CRU. When return is required: (1) return instructions, a prepaid shipping label, and a container will be included with the replacement CRU; and (2) you might be charged for the replacement CRU if Lenovo does not receive the defective CRU within thirty (30) days of your receipt of the replacement CRU. For full details, see the Lenovo Limited Warranty documentation at [https://www.lenovo.com/warranty/llw\\_02](https://www.lenovo.com/warranty/llw_02).

---

### CRU list

The following is a list of CRUs of your computer.

#### Self-service CRUs

- ac power adapter\*
- Base cover assembly
- M.2 solid-state drive
- M.2 solid-state drive bracket
- Nano-SIM-card tray\*
- Lenovo Slim Pen\*
- Power cord\*

#### Optional-service CRUs

- Wireless WAN card\*
- Wireless WAN card bracket\*

\* for selected models

**Note:** Replacement of any parts not listed above, including the built-in rechargeable battery, must be done by a Lenovo-authorized repair facility or technician. Go to <https://support.lenovo.com/partnerlocator> for more information.

---

## Disable Fast Startup and the built-in battery

Before replacing any CRU, ensure that you disable Fast Startup first and then disable the built-in battery.

To disable Fast Startup:

1. Go to **Control Panel** and view by Large icons or Small icons.

2. Click **Power Options**, and then click **Choose what the power buttons do** on the left pane.
3. Click **Change settings that are currently unavailable** at the top.
4. If prompted by User Account Control (UAC), click **Yes**.
5. Clear the **Turn on fast startup** check box, and then click **Save changes**.

To disable the built-in battery:

1. Restart your computer. When the logo screen is displayed, immediately press F1 to enter the UEFI BIOS menu.
2. Select **Config → Power**. The **Power** submenu is displayed.
3. Select **Disable Built-in Battery** and press Enter.
4. Select **Yes** in the Setup Confirmation window. The built-in battery is disabled and the computer turns off automatically. Wait three to five minutes to let the computer cool.

---

## Replace a CRU

Follow the replacement procedure to replace a CRU.

### Base cover assembly

#### Prerequisite

Before you start, read [Generic Safety and Compliance Notices](#) and print the following instructions.

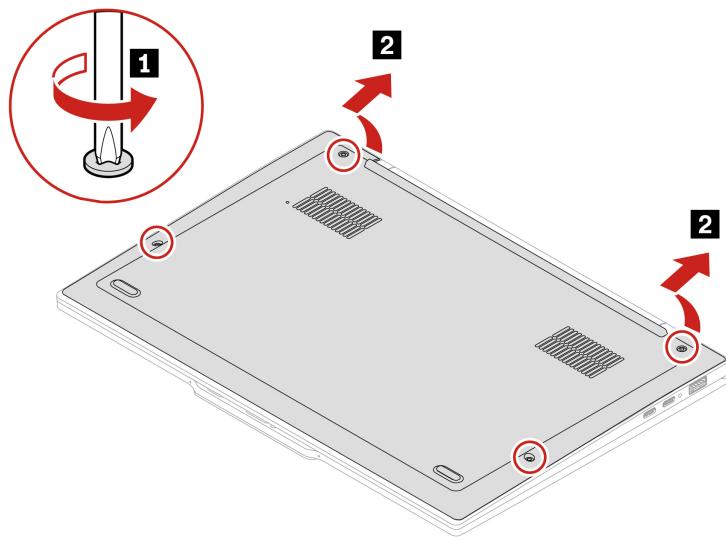
**Notes:** Do not remove the base cover assembly in the following situations. Otherwise, there might be a risk of short circuits.

- When your computer has the removable battery installed
- When your computer is connected to ac power

For access, do the following:

1. Disable the built-in battery. See “Disable Fast Startup and the built-in battery” on page 51.
2. Turn off the computer and disconnect the computer from ac power and all connected cables.
3. Remove the nano-SIM-card tray if your computer comes with one. See “Access networks” on page 11.
4. Close the computer display and turn over the computer.

## Removal procedure



## Troubleshooting

If the computer does not start up after you reinstall the base cover assembly, disconnect the ac power adapter and then reconnect it to the computer.

## Wireless WAN card and wireless WAN card bracket (for selected models)

The following information is only for the computer with user-installable modules. Ensure that you use only a Lenovo-authorized wireless module specifically tested for this computer model. Otherwise, the computer will generate an error-code beep sequence when you turn on the computer.

### Prerequisite

Before you start, read [Generic Safety and Compliance Notices](#) and print the following instructions.

**Attention:** Do not touch the contact edge of the wireless WAN card. Otherwise, the wireless WAN card might get damaged.

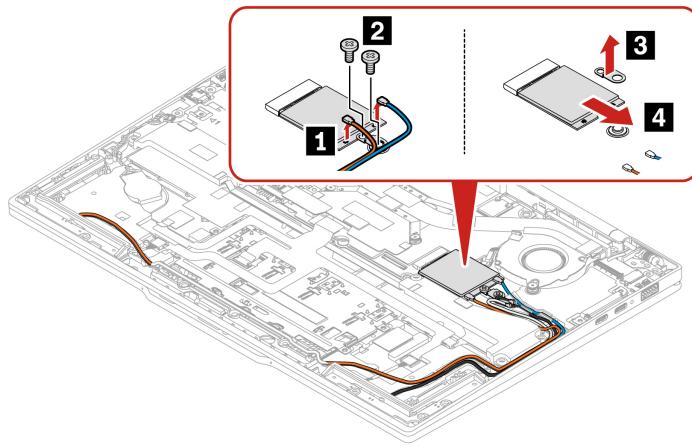
For access, do the following:

1. Disable the built-in battery. See “Disable Fast Startup and the built-in battery” on page 51.
2. Turn off the computer and disconnect the computer from ac power and all connected cables.
3. Remove the nano-SIM-card tray if your computer comes with one. See “Access networks” on page 11.
4. Close the computer display and turn the computer over.
5. Remove the base cover assembly. See “Base cover assembly” on page 52.

### Removal procedure

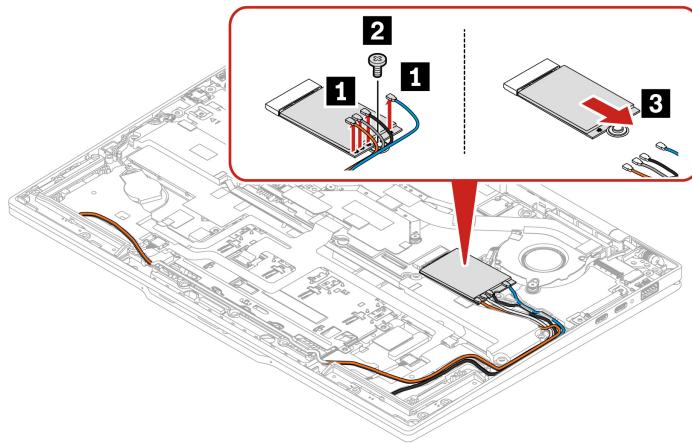
**Note:** A Mylar film might cover the wireless WAN card. To access the wireless WAN card, peel off the film first.

### Type one – Models with 4G wireless WAN card

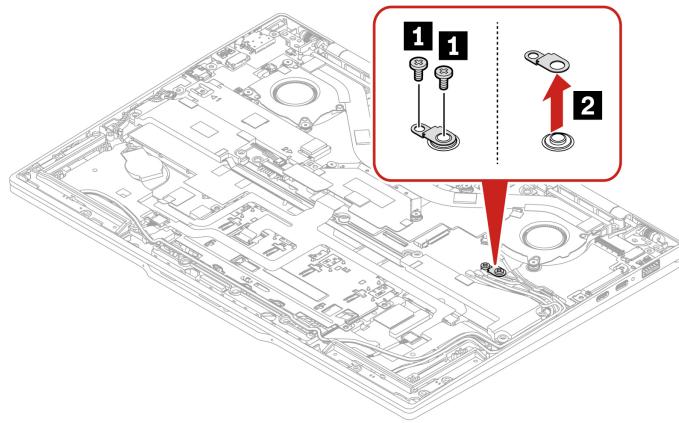


**Note:** Depending on models, the 4G wireless WAN card may be either 4 connectors or 2 connectors.

### Type two – Models with 5G wireless WAN card



### Type three – Models with wireless WAN card bracket only

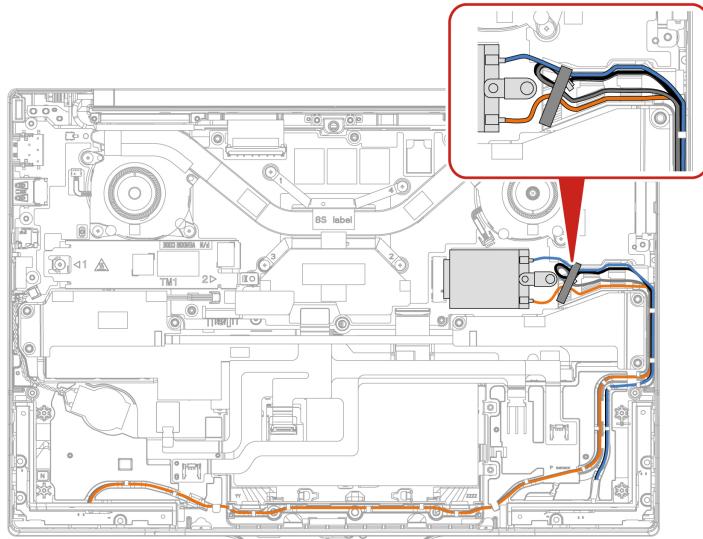


**Note:** Wireless WAN card bracket is needed for 4G models only.

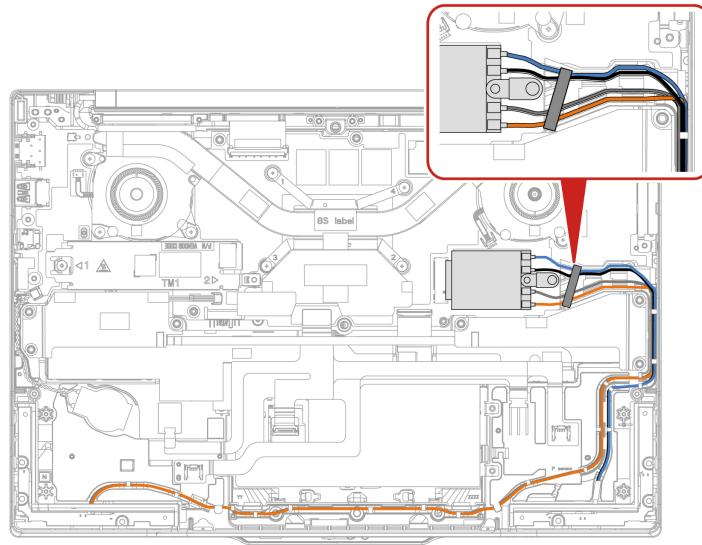
#### Antenna cable routing

The cable routing is different for 4G wireless WAN card and 5G wireless WAN card. Ensure that the antenna cables are installed appropriately when installing a wireless WWAN card.

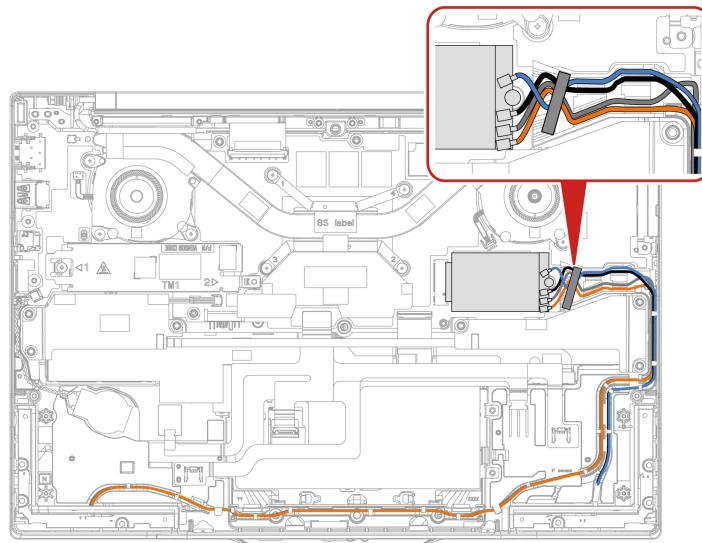
### Type one – 4G wireless WAN card with 2 connectors



### Type two – 4G wireless WAN card with 4 connectors



### Type three – 5G wireless WAN card



#### Notes:

- Keep the tape attached away from the speaker.