

Interactive BIOS simulator

HP 17-cn0xxx Laptop

Welcome to the interactive BIOS simulator for the
HP 17-cn0xxx Laptop

Here's how to use it...

[BIOS Utility Menus](#): (Click the link to navigate to the individual menus)

On this page you will find thumbnail images of each of the product's BIOS utility menus. To view a specific menu in greater detail, simply click that thumbnail. Just as in the live BIOS, on each menu, you can select the tab of each of the other utility menus to navigate directly to that menu.

Menu options:

While the menu options cannot be toggled, many of them offer item specific information about that option. To view this information, use the cursor to rollover the option and the information will present in a pane on the right of the BIOS screen.

That's it!

On every page there is a link that brings you back to either this Welcome page or the BIOS Utility Menus page enabling you to navigate to whatever BIOS option you wish to review.

BIOS Utility Menus

Main

Security

Configuration

Boot Options

Exit

Main Menu



Main

System Time	[06:00:33]
System Date	04/26/2021
Product Name	HP Laptop 17-cp0xxx
System Family	HP Notebook
Product Number	1234567#ABA
System Board ID	8844
Processor Type	AMD Ryzen 3 3250U with Radeon Graphics
Processor Speed	2600 MHz
Total Memory	16 GB
BIOS Vendor	AMI
BIOS Revision	B.07M02
Serial Number	0000760LKQ
UUID	B1C8947D-ABAC-CE4F-8FB6-610F132-85A6A
System Board CT Number	
Factory installed OS	Win10
Primary Battery SN	32577 11/21/2020
Build ID	21WW1EUT6ag#SABA#DABA
Feature Byte	3K3Q 6b7K 7P7W aBap aqas awbc bhcb dUdp dqfP m9n3 n4 .Bt

1

2

Item Specific Help

1. Provides firmware revision information of devices built in the system.
2. View System Log.

Main Menu



Main

Device Firmware Revision

Embedded Controller 73.10

GOP (Graphic Output Protocol) 2.8.0

Item Specific Help

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

TPM Device

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

TPM State

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Clear TPM

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. Clearing the TPM causes you to lose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM. TPM can be cleared only when you confirm the request via the Physical presence check prompted by the BIOS during the next startup. If you select Yes, TPM security setting and content will be cleared. After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Item Specific Help

1. Select the display language for the BIOS.
2. Hardware VT enables a processor feature for running multiple simultaneous Virtual Machines allowing specialized software applications to run in full isolation of each other.
3. Set the Fan Always On
4. Disabled: Requires pressing fn key + f1 through f12 to activate action keys
Enabled: Requires pressing only f1 through f12 to activate action keys
5. This item enables or disables the reporting of battery remaining time from the BIOS to the operating system. If disabled, the operating system displays battery life in a percentage only.
6. Dynamic battery protection to optimize battery pack longevity.
7. Set the Keyboard backlight to turn off after specified period of internal keyboard/touch pad inactivity.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Language

[This area is currently blank, representing the configuration options for the selected 'Language' item.]

Item Specific Help

[This area is currently blank, representing the help text for the selected 'Language' item.]

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Virtualization Technology

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Fan Always On

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Action Keys Mode

[Detailed configuration options for Action Keys Mode]

Item Specific Help

[Help text for Action Keys Mode]

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Keyboard Backlight Timeout

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Battery Remaining Time

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- Battery Remaining Time
- Adaptive Battery Optimizer
- Keyboard Backlight Timeout

Adaptive Battery Optimizer

[Empty configuration area]

Item Specific Help

[Empty help area]

Boot Options Menu



Boot Options

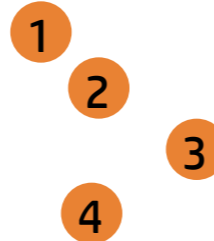
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol

Platform Key
Pending Action

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
▶ OS Boot Manager

Enrolled-MSFT
None



Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. The HP logo is in the top left. The menu items are: Post Hotkey Delay (sec), USB Boot, Network Boot, Network Boot Protocol, Platform Key, Pending Action, Load HP Factory Default Keys, Load MSFT Debug Policy Keys, UEFI Boot Order (with a sub-option OS Boot Manager), and Enrolled MSFT (with a sub-option None). A blue box highlights the 'Post Hotkey Delay (sec)' option. Four numbered callouts (1-4) are placed to the right of the menu items: 1 points to USB Boot, 2 to Network Boot, 3 to Network Boot Protocol, and 4 to Enrolled MSFT. A 'Boot Options' title bar is at the top right of the menu area. On the far right, there is a 'Item Specific Help' section with four numbered instructions.

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot

Network Boot

Network Boot Protocol

Platform Key

Pending Action

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

 ▶ OS Boot Manager

Enrolled MSFT

None

Post Hotkey Delay (sec)

Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. On the left is the HP logo. The menu items are: Post Hotkey Delay (sec), USB Boot, Network Boot, Network Boot Protocol, Platform Key, Pending Action, Enrolled MSFT, None, Load HP Factory Default Keys, Load MSFT Debug Policy Keys, UEFI Boot Order, and OS Boot Manager. A blue box highlights the 'USB Boot' option, with a white line indicating it is selected. Four numbered callouts (1-4) point to the USB Boot, Network Boot, Network Boot Protocol, and Enrolled MSFT options respectively. On the right, a 'Boot Options' header is above a 'Item Specific Help' sidebar containing four numbered instructions.

hp

Boot Options

Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Platform Key
Pending Action
Enrolled MSFT
None
Load HP Factory Default Keys
Load MSFT Debug Policy Keys
UEFI Boot Order
 ▶ OS Boot Manager

Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu



Boot Options

Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol

1
2
4

3

Platform Key
Pending Action

Enrolled MSFT
None

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
▶ OS Boot Manager

Network Boot

Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure IBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu



Boot Options

Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol

1
2
4

3

Platform Key
Pending Action

Enrolled MSFT
None

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
▶ OS Boot Manager

Network Boot Protocol

Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure IBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. On the left is the HP logo. The menu items are: Post Hotkey Delay (sec), USB Boot, Network Boot, Network Boot Protocol, Platform Key, Pending Action, Load HP Factory Default Keys, Load MSFT Debug Policy Keys, UEFI Boot Order (with a sub-option OS Boot Manager), and a highlighted Secure Boot option. Four orange callout boxes with numbers 1, 2, 3, and 4 point to USB Boot, Network Boot, Network Boot Protocol, and Enrolled MSFT respectively. On the right, a 'Boot Options' header is above a 'Item Specific Help' sidebar containing four numbered instructions.

hp

Boot Options

Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Platform Key
Pending Action
Load HP Factory Default Keys
Load MSFT Debug Policy Keys
UEFI Boot Order
 ▶ OS Boot Manager
Secure Boot

Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order .
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure IBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Exit Menu



Exit

Ignore Changes and Exit ¹ ² ³

Item Specific Help

1. Exit System Setup and save your changes to CMOS.
2. Exit utility without saving Setup data to CMOS.
3. Load default values for all SETUP items.

Exit Menu



Exit

Ignore Changes and Exit

- 1
- 2
- 3

Save Changes and Exit?

Item Specific Help

1. Exit System Setup and save your changes to CMOS.
2. Exit utility without saving Setup data to CMOS.
3. Load default values for all SETUP items.

Exit Menu



Exit

Ignore Changes and Exit

- 1
- 2
- 3

Load Setup Defaults?

Item Specific Help

1. Exit System Setup and save your changes to CMOS.
2. Exit utility without saving Setup data to CMOS.
3. Load default values for all SETUP items.