

Interactive BIOS simulator

HP ENVY 17-ch0xxx Laptop PC

Welcome to the interactive BIOS simulator for the
HP ENVY 17-ch0xxx Laptop PC

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	[22:02:59]
System Date	01/01/2020
Product Name	HP ENVY Laptop 17-ch0xxx
System Family	HP Envy
Product Number	4810MK01A006
System Board ID	88B6
Processor Type	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz
Total Memory	32 GB
BIOS Vendor	Insyde
BIOS Revision	B.20
Serial Number	ABC050007T
UUID	5EF5E158-3A85-11EB-925B-DC1BA107500C
System Board CT Number	4550MK01DA1004
Factory installed OS	Win10
Primary Battery SN	00200 10/29/2020
Build ID	21WW1TIT6aj#SABA#DABA
Feature Byte	3K3Q 6b7K 7NaB apaq asaw bBbh cdbU dXdp dqfP hAhZ kFkh m9 .ra

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	62.17
Intel ME (Management Engine)	15.0.2.1377
GOP (Graphic Output Protocol)	17.0.1045
USB Type-C Controller(s)	F5.09.05.04.04
Thunderbolt Controller(s)	14.0.0.3401
Thunderbolt Retimer	2.15

Item Specific Help

Main Menu



Main

System Log

Result:

0607

0607

Time:

031921-014724

031921-014640

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

- No Data -

Item Specific Help

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next start-up. If you select Yes, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Security Menu



Security

Administrator Password

1

Power-On Password

2

TPM Device

3

Fingerprint Reset on Reboot

Fingerprint Reset on Reboot

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. If the TPM device setting is set to Hidden, the BIOS hides this item. The 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, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
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.
7. Changing this setting will erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Configuration Menu



Configuration

- Language 1
- Virtualization Technology 2
- Hyper-Threading 3
- Fan Always On 4
- Action Keys Mode 5
- USB Charging 6
- Battery Remaining Time 7
- Adaptive Battery Optimizer 8
- Keyboard Backlight Timeout

- High resolution mode on USB-C DP alt mode dock 9

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. Enables a single processor core to execute two or more threads concurrently.
4. Set the Fan Always On
5. Disabled: Requires pressing fn key + f1 through f12 to activate action keys
Enabled: Requires pressing only f1 through f12 to activate action keys
6. Allow the system to charge the USB device such as mobile phone in S4 (Hibernation) or S5 (off) state.
7. 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.
8. Dynamic battery protection to optimize battery pack longevity.
9. All USB devices on the dock will connect at USB 2.0 speed, and the Gigabit NIC will experience reduced performance when high resolution mode is enabled.

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Language

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Virtualization Technology

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Fan Always On

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Hyper-Threading



Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Action Keys Mode

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Keyboard Backlight Timeout

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

USB Charging

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Battery Remaining Time

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

Adaptive Battery Optimizer

Item Specific Help

Configuration Menu



Configuration

UEFI HII Configuration

Item Specific Help

Configuration Menu



Configuration

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

- High resolution mode on USB-C DP alt mode dock
- In-bag detection

High resolution mode on USB-C DP alt mode dock

Item Specific Help

Configuration Menu



Configuration

Intel(R) RST 18.0.0.4897 RST VMD Driver

Optane Volume:

Item Specific Help

Configuration Menu



Configuration

OPTANE VOLUME INFO

Disable mode: Safe
Size: 953.8GB

Volume member disks:

Item Specific Help

Configuration Menu



Configuration

DISABLE OPTANE VOLUME

Preserve user data:

Are you sure you want to disable?

Item Specific Help

Configuration Menu



Configuration

PHYSICAL DISK INFO

Port :	0.0
Model Number:	INTEL HBRPEKNX0203AH
Serial Number:	TE023500AR1P0C
Size:	953.8GB
Status:	Non-RAID
Controller Type:	NVMe
Controller Interface :	TG

Item Specific Help

Configuration Menu




Configuration

PHYSICAL DISK INFO

Port :	1.0
Model Number:	INTEL HBRPEKNX0203AHO
Serial Number:	TE023500AR1P0C-2
Size:	27.2GB
Status:	Non-RAID
Controller Type:	NVMe
Controller Interface :	TG

Item Specific Help

Boot Options Menu



Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key **4** Enrolled MSFT

Pending Action 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. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

Boot Options Menu

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
 - Internal CD/DVD ROM Drive

Enrolled MSFT

None

Post Hotkey Delay (sec)

Item Specific Help

1. Enable/Disable USB boot.
2. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

Boot Options Menu

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key

Pending Action

Enrolled MSFT **4**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Internal CD/DVD ROM Drive

USB Boot

Item Specific Help

1. Enable/Disable USB boot.
2. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

Boot Options Menu

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key

Pending Action

Enrolled MSFT **4**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Internal CD/DVD ROM Drive

Network Boot

Item Specific Help

1. Enable/Disable USB boot.
2. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

Boot Options Menu

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
- Internal CD/DVD ROM Drive

Network Boot Protocol

Item Specific Help

1. Enable/Disable USB boot.
2. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

Boot Options Menu

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
- Internal CD/DVD ROM Drive

Secure Boot

Item Specific Help

1. Enable/Disable USB boot.
2. Enable/Disable network boot during boot time.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

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.