

Interactive BIOS simulator

HP Pavilion Gaming Laptop 17-cd0xxx

Welcome to the interactive BIOS simulator for the
HP Pavilion Gaming Laptop 17-cd0xxx

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	[16:45:28]
System Date	05/06/2019
Product Name	HP Pavilion Gaming Laptop 17-cd0xxx
System Family	HP Pavilion
Product Number	FPC7001#ABA
System Board ID	85FD
Born On Date	00/00/0000
Processor Type	Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz
Total Memory	12 GB
BIOS Vendor	Insyde
BIOS Version	B.08. TPD4
Serial Number	CND90754KG
UUID	424CBD9A-A02D-E911-8BB6-B00CD1E71D89
System Board CT Number	PXXXXA5WVBYT5S
Factory installed OS	Win10
Primary Battery SN	01041 01/24/2019
Build ID	19WW1MAT6ah#SABA#DABA
Feature Byte	3K3Q 3X47 6b7B 7K7W aBap aqaw bCbh cbdU dpdq fPfd hZ .Dd

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	43.14
Intel ME (Management Engine)	12.0.30.1406
GOP (Graphic Output Protocol)	9.0.1085
Discrete GOP (Graphic Output Protocol)	3000F
Discrete VBIOS Version	86.07.6C.00.A
USB Type-C Controller(s)	F7.07.10.9C.06

Item Specific Help

Security Menu



Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device

1

2

3

4

Item Specific Help

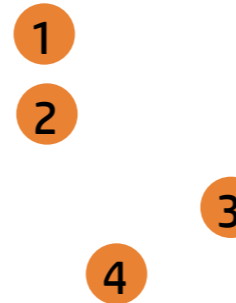
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



Item Specific Help

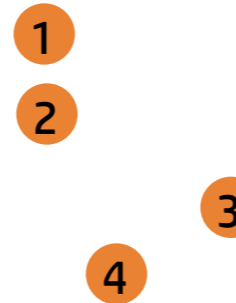
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



Item Specific Help

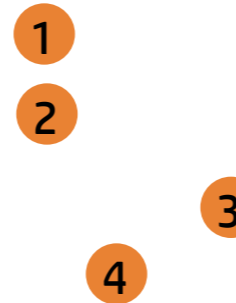
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



Intel Software Guard Extensions (SGX)

Item Specific Help

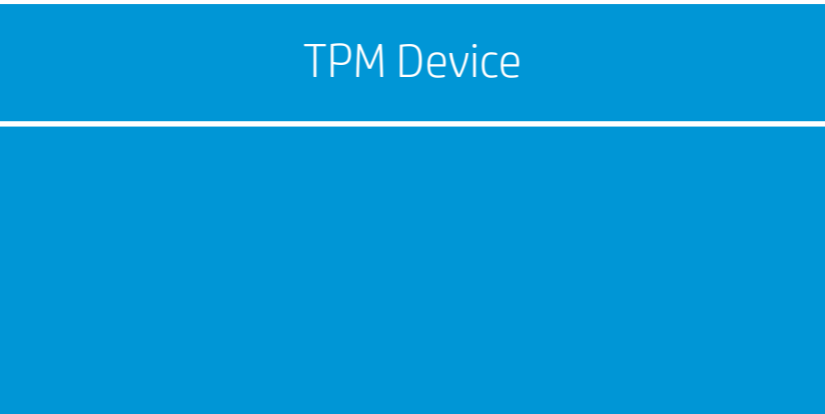
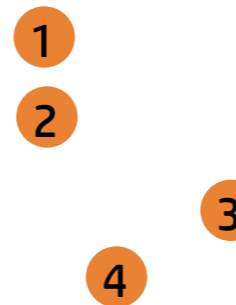
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



Item Specific Help

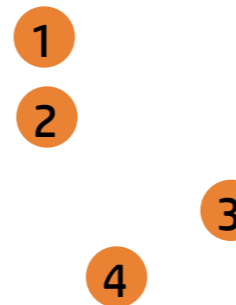
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



TPM State

Item Specific Help

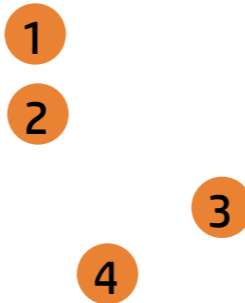
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



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. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. 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.
6. 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.
7. 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
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device

1

2

3

4

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. 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.
6. 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.
7. 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 1
- Virtualization Technology 2
- Fan Always On 3
- Action Keys Mode 4
- USB Charging 5
- Battery Remaining Time 6
- Battery Care Function 7

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

- 1
- 2
- 3
- 4
- 5

Language

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

Virtualization Technology

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

Fan Always On

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

Action Keys Mode

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

USB Charging

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

Battery Remaining Time

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Deice such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. This item enables or disables the reporting of battery remaining time from the BIOS to the operating system. If disabled, the operating sustem displays battery life in a percentage only.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Fan Always On
- Action Keys Mode
- USB Charging
- Battery Remaining Time
- Battery Care Function

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

Battery Care Function

Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets 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. Allow the system to charge the USB Device such as mobile phone in S4 (Hibernation) or S5 (off) state.
6. 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.
7. Battery Care Function (100%): The battery charge stops at 91-100%.
Battery Care Function (80%): The battery charge stops at 76-80%.
Battery Care Function (50%): The battery charge stops at 46-50%.

Configuration Menu



Configuration

UEFI HII Configuration

1

Item Specific Help

1. This formset allows the user to manage RAID volumes on the Intel(R) RAID Controller

Configuration Menu



Configuration

Intel(R) RST 17.0.0.3808 RAID Driver

Optane Volume:

Item Specific Help

Configuration Menu



Configuration

OPTANE VOLUME INFO

Disable mode: Safe
Size: 931.5GB

1

Volume member disks:

2

2

Item Specific Help

- 1. Disable Optane Volume
- 2. Select to see more information about disk

Configuration Menu



Configuration

DISABLE OPTANE VOLUME

Preserve user data Enabled

Are you sure you want to disable? <No>

▶ Disable

Item Specific Help

Configuration Menu



Configuration

PHYSICAL DISK INFO

Port:	0.0
Model Number:	HGST HTs721010A9E630
Serial Number:	JR1000BNKB79LE
Size:	931.5GB
Status:	Non-RAID
Controller Type:	AHCI
Controller Interface:	SATA

Item Specific Help

Configuration Menu




Configuration

PHYSICAL DISK INFO

Port:	1.0
Model Number:	INTEL MEMPEK1J016GAH
Serial Number:	PHBT84509M0016N
Size:	13.4GB
Status:	Cache
Controller Type:	NVMe
Controller Interface:	PCIe

Item Specific Help

Boot Options Menu



Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Legacy Support **4**

Platform Key **5** Enrolled MSFT

Pending Action None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- ▶ OS Boot Manager
- Internal CD/DVD ROM Drive

Legacy Boot Order

- ▶ Internal Hard Drive
- Internal CD/DVD ROM Drive

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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

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, Legacy Support, Platform Key, Pending Action, Enrolled MSFT, None, Post Hotkey Delay (sec), Load HP Factory Default Keys, Load MSFT Debug Policy Keys, UEFI Boot Order (with sub-items OS Boot Manager and Internal CD/DVD ROM Drive), Legacy Boot Order (with sub-items Internal Hard Drive and Internal CD/DVD ROM Drive). A 'Boot Options' tab is highlighted at the top. A 'Post Hotkey Delay (sec)' sub-menu is open, showing a blue bar with the text 'Post Hotkey Delay (sec)'. Five numbered callouts (1-5) are placed over the menu items: 1 over USB Boot, 2 over Network Boot, 3 over Network Boot Protocol, 4 over Legacy Support, and 5 over Enrolled MSFT.

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot

Network Boot

Network Boot Protocol

Legacy Support

Platform Key

Pending Action

Enrolled MSFT

None

Post Hotkey Delay (sec)

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- ▶ OS Boot Manager
- Internal CD/DVD ROM Drive

Legacy Boot Order

- ▶ Internal Hard Drive
- Internal CD/DVD ROM Drive

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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. 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
Legacy Support

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

Legacy Boot Order
▶ Internal Hard Drive
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. When Legacy Support is enabled, BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7, Windows Vista, Windows XP and DOS. When legacy Support is disabled, BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot into operating system after changing this setting.
5. 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
Legacy Support

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

Legacy Boot Order
▶ Internal Hard Drive
Internal CD/DVD ROM Drive

Network Boot

1
2
3
4
5

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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. 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
Legacy Support

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

Legacy Boot Order
▶ Internal Hard Drive
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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. 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**

Legacy Support **4**

Platform Key

Pending Action

Enrolled MSFT **5**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Internal CD/DVD ROM Drive

Legacy Boot Order

▶ Internal Hard Drive

Internal CD/DVD ROM Drive

Legacy Support

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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. 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**

Legacy Support **4**

Platform Key

Pending Action

Enrolled MSFT **5**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Internal CD/DVD ROM Drive

Legacy Boot Order

▶ Internal Hard Drive

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. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to support newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.
5. 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.