aaa

Interactive BIOS simulator

HP Pavilion Gaming Laptop 15-dk0xxx

Welcome to the interactive BIOS simulator for the
HP Pavilion Gaming Laptop 15-dk0xxx

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.

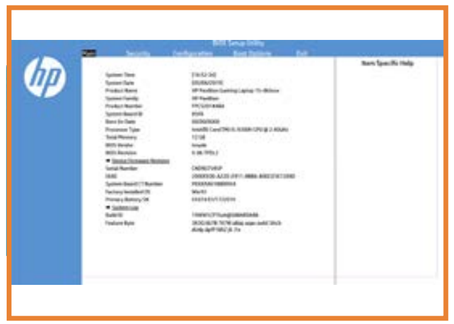
Menu options:
While the menu options cannot be toggled, many of them offer item specific information about that option. To view this information, use the cursor to rollover the option and the information will present in a pane on the right of the BIOS screen.

That's it!

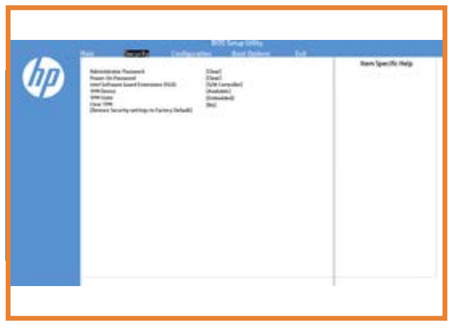
On every page there is a link that brings you back to either this Welcome page or the BIOS Utility Menus page enabling you to navigate to whatever BIOS option you wish to review.

BIOS Utility Menus

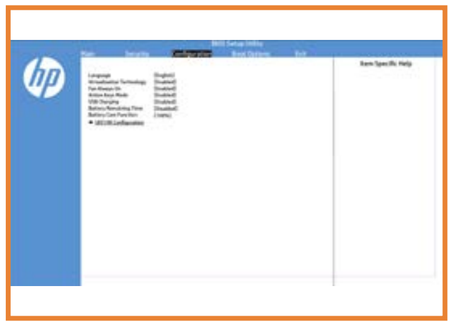
Back to Welcome Page



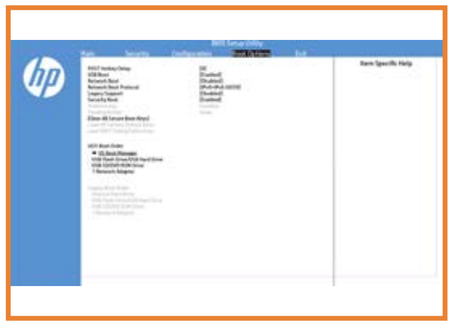
Main



Security



Configuration



Boot Options

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

System Time	[16:52:34]
System Date	[05/06/2019]
Product Name	HP Pavillion Gaming Laptop 15-dk0xxx
System Family	HP Pavillion
Product Number	FPC5201#ABA
System Board ID	85FA
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 Revision	V.08.TPDL2
➡ Device Firmware Revision	
Serial Number	CND907545P
UUID	2000FE00-A22D-E911-8BB6-B00CD1E7209D
System Board CT Number	PXXXXA61WBXRU4
Factory Installed OS	Win10
Primary Battery SN	01074 01/17/2019
➡ System Log	
Build ID	19WW1CPT6ah@SABA#DABA
Feature Byte	3K3Q 6b7B 7K7W aBap aqas awbC bhcb dUdp dpfP fdhZ j6 .Fn

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Item Specific Help

System Time	[16:52:34]
System Date	[05/06/2019]
Product Name	HP Pavillion Gaming Laptop 15-dk0xxx
System Family	HP Pavillion
Product Number	FPC5201#ABA
System Board ID	85FA
Born On Date	00/00/0000
Processor Typ	-9300H CPU @ 2.40GHz
Total Memory	
BIOS Vendor	
BIOS Revision	
➡ Device Firr	
Serial Number	CND907345P
UUID	2000FE00-A22D-E911-8BB6-B00CD1E7209D
System Board CT Number	PXXXXA61WBXRU4
Factory Installed OS	Win10
Primary Battery SN	01074 01/17/2019
➡ System Log	
Build ID	19WW1CPT6ah@SABA#DABA
Feature Byte	3K3Q 6b7B 7K7W aBap aqas awbC bhcb dUdp dpfP fdhZ j6 .Fn

System Time

15	52	23
16	53	24
17	54	25

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Item Specific Help

System Time	[16:52:34]
System Date	[05/06/2019]
Product Name	HP Pavillion Gaming Laptop 15-dk0xxx
System Family	HP Pavillion
Product Number	FPC5201#ABA
System Board ID	85FA
Born On Date	00/00/0000
Processor Typ	-9300H CPU @ 2.40GHz
Total Memory	
BIOS Vendor	
BIOS Revisior	
➡ Device Firr	
Serial Number	
UUID	2000FE00-A22D-E911-8BB6-B00CD1E7209D
System Board CT Number	PXXXXA61WBXRU4
Factory Installed OS	Win10
Primary Battery SN	01074 01/17/2019
➡ System Log	
Build ID	19WW1CPT6ah@SABA#DABA
Feature Byte	3K3Q 6b7B 7K7W aBap aqas awbC bhcb dUdp dpfP fdhZ j6 .Fn

System Date

04	05	2018
05	06	2019
06	07	2020

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Device Firmware Revision

Embedded Controller	42.14
Intel ME (Management Engine)	12.0.30.1406
GOP (Graphic Output Protocol)	9.0.1085
Discrete GOP (Graphica Output Protocol)	3000F
Discrete VBIOS Version	86.07.6C.00.0A
USB Type-C Controller(s)	F7.07.10.9C.06

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

System Log

Result	Time:
	- 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
	- No Data
	- No Data
	- No Data

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]

Set Administrator Password

Enter New Password [_____]

Confirm New Password [_____]

Item Specific Help

Administrator Password prevents unauthorized access to the Setup Utilities. To disable the audible password prompt (beeping sound), set the POST Hotkey Delay (sec) option to 0. This also disables the audible prompt for Power-On Password.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]

Set Power On Password

Enter New Password [_____]

Confirm New Password [_____]

Item Specific Help

Power-On Password prevents unauthorized access to the Setup Utilities. To disable the audible password prompt (beeping sound), set the POST Hotkey Delay (sec) option to 0. This also disables the audible prompt for Administrator Password.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]

Item Specific Help

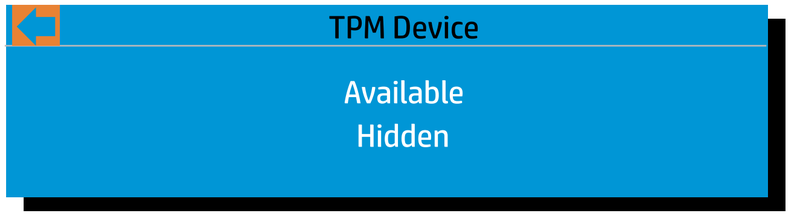
Enable/Disable Intel Software Guard Extensions (SGX).

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]



Item Specific Help

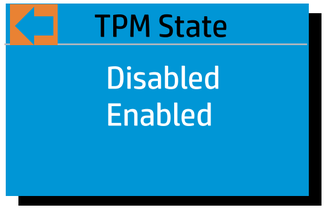
If the Item is set to “Hidden”, the TPM device is not visable in the Operating System.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]



Item Specific Help

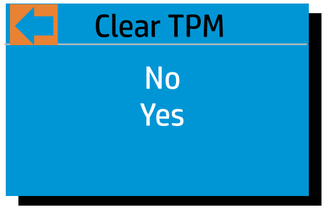
If the TPM device is hidden, this option is hidden. When the TPM device is changed to Available, this option is shown without the need to restart the computer. The TPM state is saved if the TPM device is changed to Hidden. The next time the TPM device is changed to Available, the previous setting will be restored.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]



Item Specific Help

If the TPM device is hidden, this option is hidden.

A confirmation message will be displayed during the next system startup to confirm you want to clear the TPM.

For TPM 1.2 the BIOS sends the TPM_Force-Clear command to clear the TPM.

For TPM 2.0, the BIOS sends the TPM2_Clear command to clear the Storage and Endorse-ment Hierarchy.

Once the TPM is cleared, the BIOS disables TPM Power-On Authentication.

After the BIOS clears the TPM or you reject clearing the TPM during the physical pres-ence check in POST, the setting is reverted back to No.

The setting of the TPM State shall stay the same before and after the “Clear TPM“ op-eration. Clear TPM is also set to No without any action taken if the user selects No for the Physical Presence prompt.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Administrator Password	[Clear]
Power-On Password	[Clear]
Intel Software Guard Extensions (SGX)	[S/W Controller]
TPM Device	[Available]
TPM State	[Embedded]
Clear TPM	[No]

[Restore Security settings to Factory Default]

Item Specific Help

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 Feature Reset Request

A request to Reset Security Defaults is pending. Please enter the pass code displayed below to complete the change. If you did not initiate this request, press the ESC key to continue without accepting the pending change.

Reset Security Defaults (023)

2866 2866 - ENTER - to complete the change

ESC ESC - continue without changing

For more information, please visit www.hp.com/go/techcenter/startup

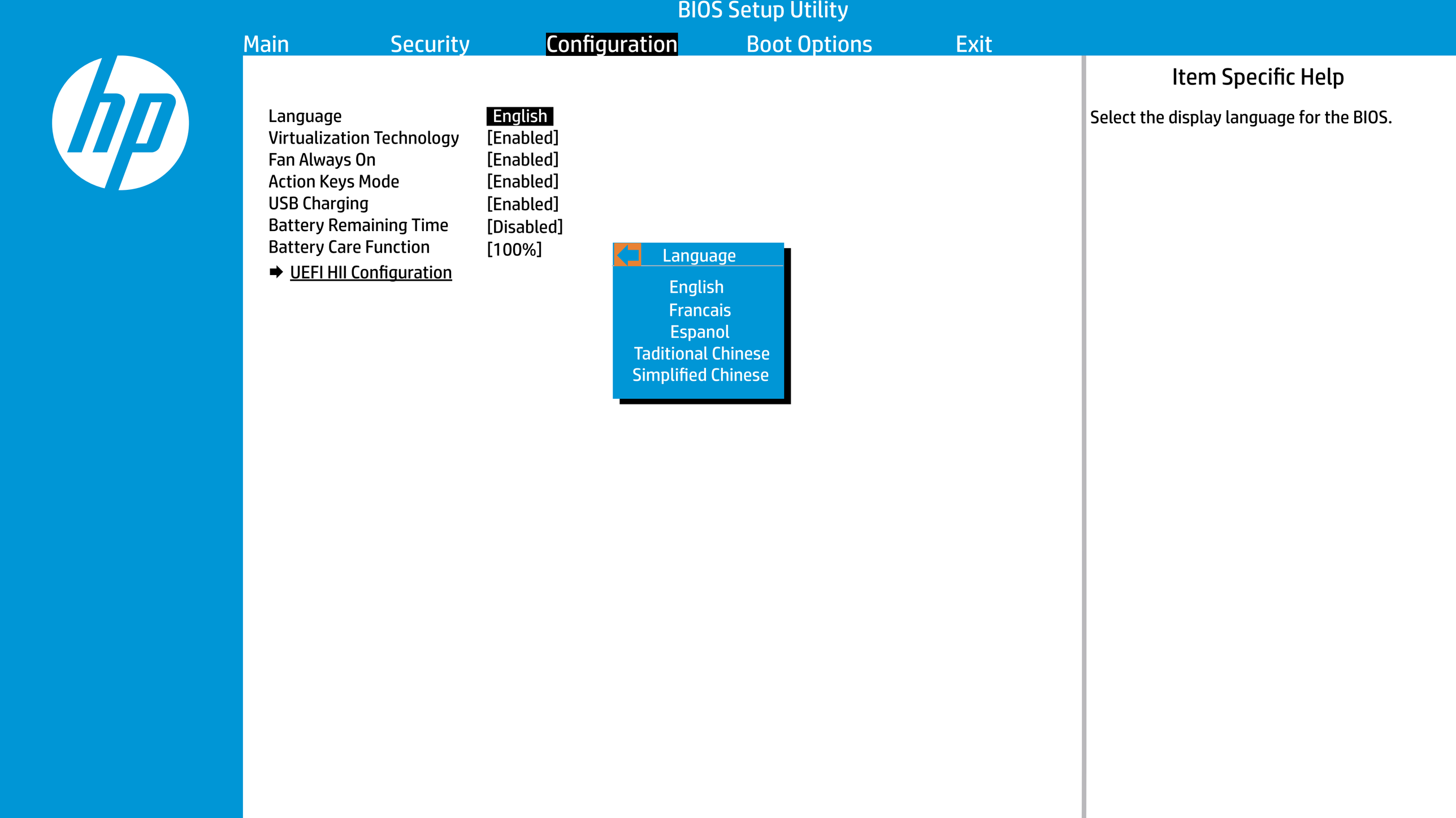
BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Item Specific Help


BIOS Setup Utility
Main
Security
Configuration
Boot Options
Exit
Language
English
Virtualization Technology
[Enabled]
Fan Always On
[Enabled]
Action Keys Mode
[Enabled]
USB Charging
[Enabled]
Battery Remaining Time
[Disabled]
Battery Care Function
[100%]
UEFI HII Configuration
Language
English
Francais
Espanol
Taditional Chinese
Simplified Chinese
Item Specific Help
Select the display language for the BIOS.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Virtualization Technology

Disabled
Enabled

Item Specific Help

Hardware VT Enables a processor feature for running multiple simultaneous Virtual Machines allowing specialized software applications to run in full isolation of each other. HP recommends that this feature remain disabled unless specialized applications are being used.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Fan Always On

Disabled

Enabled

Item Specific Help

Set the Fan Always On (or Off).

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Action Keys Mode

Disabled

Enabled

Item Specific Help

Set the Fan Always On (or Off).

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

USB Charging

Disabled

Enabled

Item Specific Help

Allow the systen to charge the USB device such as mobile phones in S4 (Hibernation) or S5 (off) state.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Battery Remaining Time

Disabled
Enabled

Item Specific Help

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.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Language	[English]
Virtualization Technology	[Enabled]
Fan Always On	[Enabled]
Action Keys Mode	[Enabled]
USB Charging	[Enabled]
Battery Remaining Time	[Disabled]
Battery Care Function	[100%]

➡ UEFI HII Configuration

Battery Care Function

100%
80%
50%

Item Specific Help

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%.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

UEFI HII Configuration

➡ Intel(R) Rapid Storage Technology

ESC

Item Specific Help

This format allows the user to manage RAID volumes on the Intel(R) RAID Controller

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Intel(R) RST 17.0.0.3808 RAID Driver

Optane Volume

➡ Intel(R) Optane 931.5GB

ESC

Item Specific Help

Select to see more information about the Intel Optane Volume

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Optane Volume Info

Optane Mode Safe
Size 931.5GB
➡ Disable

ESC

Volume member disks
➡ SATA 0.0 ST1000LM049-2GH172 WGS3J023 931.5GB
➡ PCIE 1.0, INTEL MEMPEK1J016GAH PHBT845507Y1016N. 13.4GB

Item Specific Help

Disable Optane Volume

BIOS Setup Utility

Main Security Configuration Boot Options Exit

DISPLAY OPTANE VOLUME

Preserve user data Enabled

ESC

Are you sure you want to disable [No]

➡ Disable

Item Specific Help

Select whether to preserve user data

BIOS Setup Utility

Main Security Configuration Boot Options Exit

DISPLAY OPTANE VOLUME

Preserve user data Press Link “Disable” To Confirm

ESC

Are you sure you want to disable [Yes]

➡ Disable

Item Specific Help

Select whether to preserve user data

BIOS Setup Utility

Main Security Configuration Boot Options Exit

PHYSICAL DISK INFO

ESC

Port	0.0
Model Number	ST1000LM049-2GH1.72
Serial Number	WGS3J023
Size	931.5GB
Status	Non-RAID
Controller Type	AHCI
Controller Interface	SATA

Item Specific Help

BIOS Setup Utility

Main Security Configuration Boot Options Exit

PHYSICAL DISK INFO

ESC

Port	1.0
Model Number	Intel MEMPEK1J016GAH
Serial Number	PHBT845507Y1016N
Size	13.4GB
Status	Cache
Controller Type	NVMx
Controller Interface	PCIe

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Item Specific Help

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

POST Hotkey Delay (sec)

0
5
10
15
20

Item Specific Help

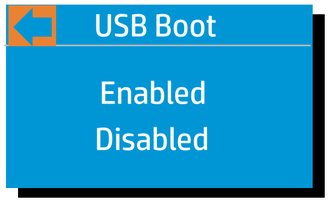
POST Hotkey Delay (sec) Controls the amount of time given to press the function key to enter the Setup Utilities when the system starts. To disable the audible password prompt (beeping sound) for both the Administrator Password and Power-On Password, set the POST Hotkey Delay (sec) option to 0.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay [0]
USB Boot [Enabled]
Network Boot [Disabled]
Network Boot Protocol [IPv4+IPv6 (UEFI)]
Legacy Support [Disabled]
Security Boot [Enabled]
Platform Key Enrolled
Pending Action None
[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor



Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Item Specific Help

Enable/Disable USB Boot.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Network Boot
Enabled
Disabled

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Item Specific Help

Enable/Disable network boot during boot time.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay [0]
USB Boot [Enabled]
Network Boot [Disabled]
Network Boot Protocol [IPv4+IPv6 (UEFI)]
Legacy Support [Disabled]
Security Boot [Enabled]
Platform Key Enrolled
Pending Action None
[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Network Boot Protocol

IPv4 (UEFI)
IPv6 (UEFI)
IPv4+ IPv6 (UEFI)

Item Specific Help

Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Support
Enabled
Disabled

Item Specific Help

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.

BIOS Setup Utility

Main Security Configuration **Boot Options** Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Changing this setting may make the system unable to boot the OS. Do you want to make this change?

Yes No

Item Specific Help

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.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]
Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
➡ OS Boot Manager
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Legacy Boot Order
Internal Hard Drive
USB Flash Drive/USB Hard Drive
USB CD/DVD ROM Drive
1 Network Adaptor

Security Boot
Enabled
Disabled

Item Specific Help

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.

BIOS Setup Utility

Main | Security | Configuration | Boot Options | Exit

POST Hotkey Delay	[0]
USB Boot	[Enabled]
Network Boot	[Disabled]
Network Boot Protocol	[IPv4+IPv6 (UEFI)]
Legacy Support	[Disabled]
Security Boot	[Enabled]
Platform Key	Enrolled
Pending Action	None

[Clear All Secure Boot Keys]

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

➡ OS Boot Mar

USB Flash Drive

USB CD/DVD RO

1 Network Ada

Changing all Secure Boot Keys will disable Secure boot. Please enter the pass code displayed below to complete the action or press the ESC key to cacel.

ESC

Pass Code: 5544

[redacted]

Legacy Boot Order

Internal Hard Drive

USB Flash Drive/USB Hard Drive

USB CD/DVD ROM Drive

1 Network Adaptor

Item Specific Help

Clears all secure boot keys and certificates from secure boot databases. This option disables secure boot.

BIOS Setup Utility

Main Security Configuration Boot Options Exit

Item Specific Help