Interactive BIOS simulator

HP Spectre 16 x360 Convertible PC

Welcome to the interactive BIOS simulator for the HP Spectre 16 x360 Convertible 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 System Date Product Name System Family Product Number System Board ID Processor Type Total Memory BIOS Vendor

Serial Number UUID System Board CT Number Factory installed OS Primary Battery SN 1

Build ID Feature Byte [22:02:59] [07/27/2021] HP Spectre x360 2-in-1 Lapto HP Spectre 540HPT6#ABA 891A 11th Gen Intel(R) Core(TM) i7 16 GB Insyde B.08.TPDL4

CND11818GC 043A502D-30A6-EB11-8104 PXXXXA11UF5J8K Win10 01174 04/14/2021

21WW2FAT6aj#SABA#DABA 3K3X 476b 7NaB aHap aqaw kFkH m9 .RG

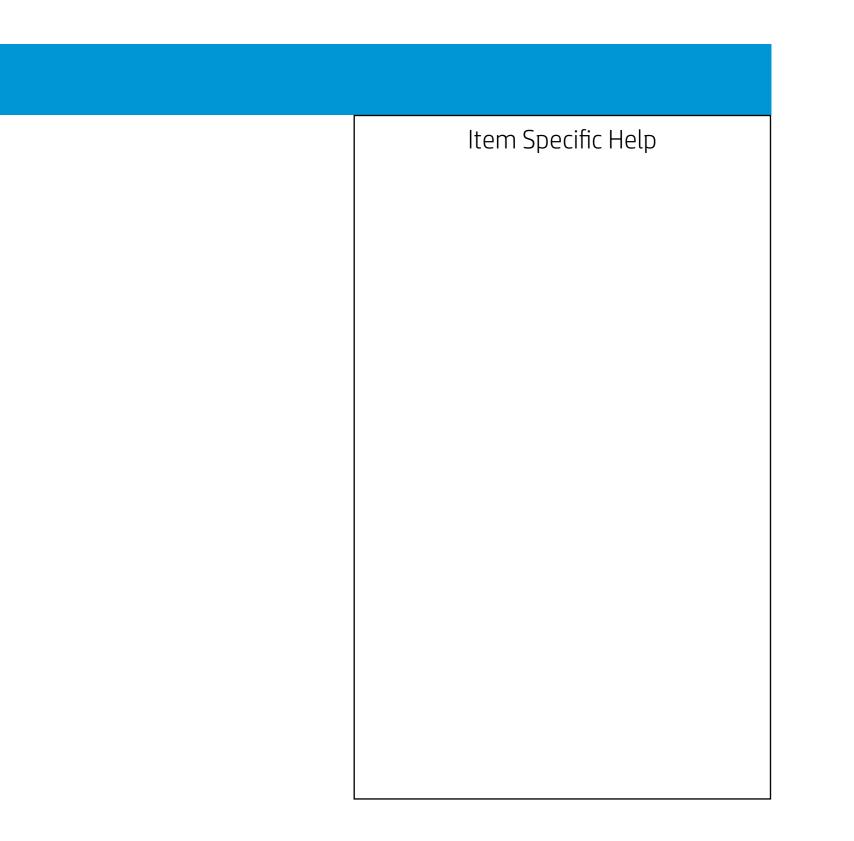
Main Menu



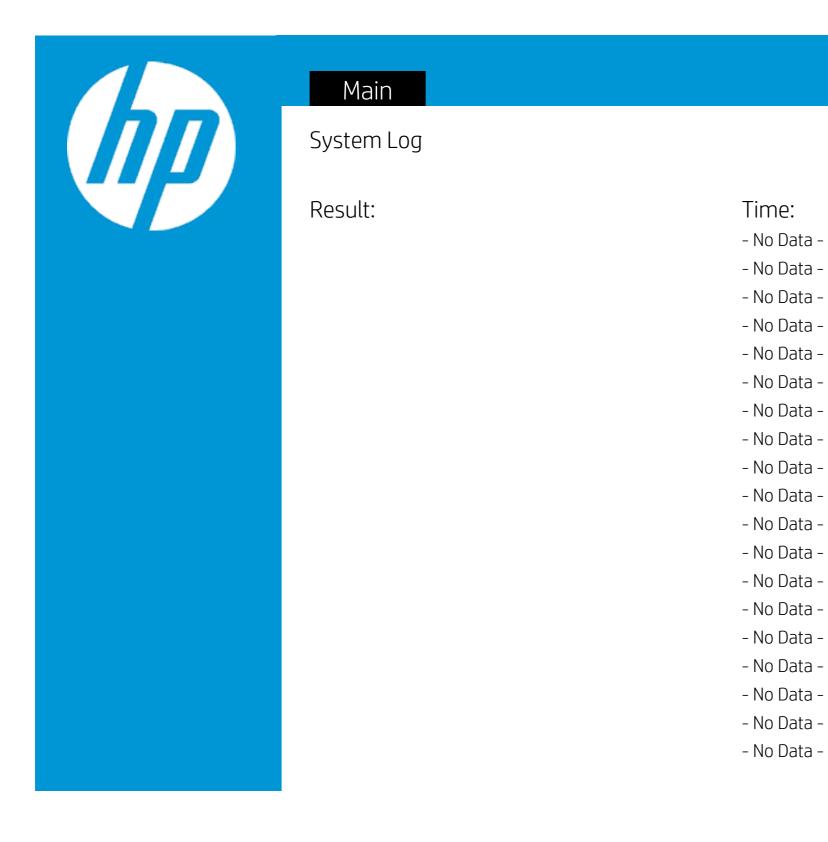
Main

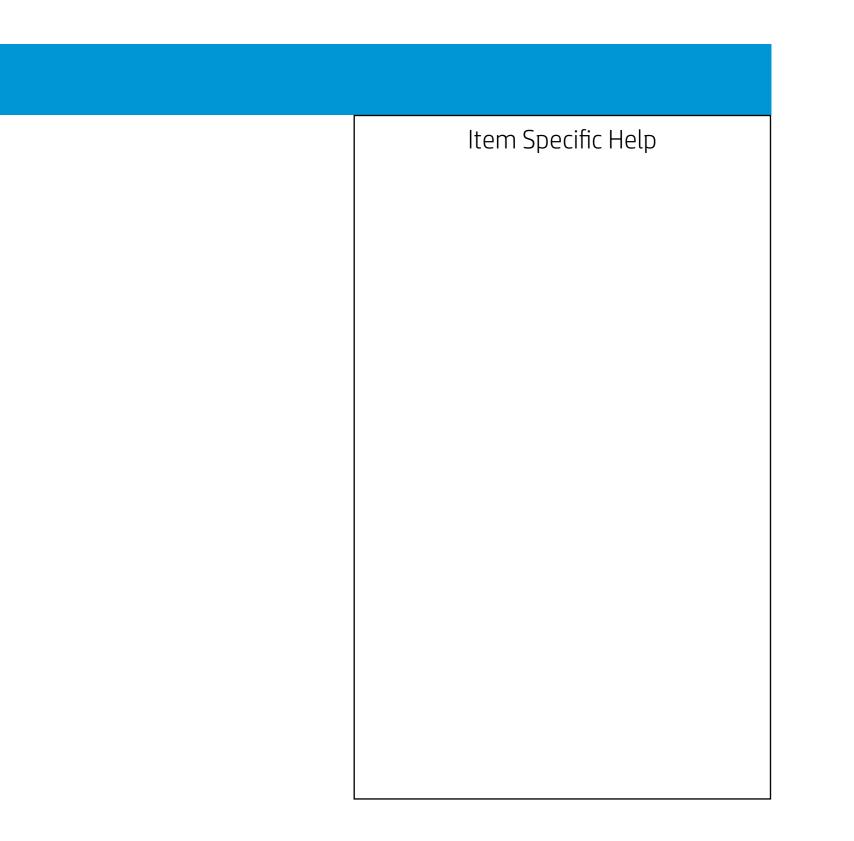
Device Firmware Revision

Embedded Controller	82.18
Intel ME (Management Engine)	15.0.30.1716
Intel ISH (Integrated Sesor Hub)	5.4.1.4468
GOP (Graphic Output Protocol)	17.0.1060
USB Type-C Controller(s)	00.35
Thunderbolt Controller(s)	14.0.0.4100
Thunderbolt Retimer	2.17



Main Menu





3



	Security	
Administrator Passw	vord	1
Power-On Password		2
HP SpareKey		
HP SpareKey Enrolln	nent	
TPM Device		

- 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 Prsenece 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.

3



	Security	
Administrator Passw	vord	1
Power-On Password		2
HP SpareKey		
HP SpareKey Enrolln	nent	
TPM Device		

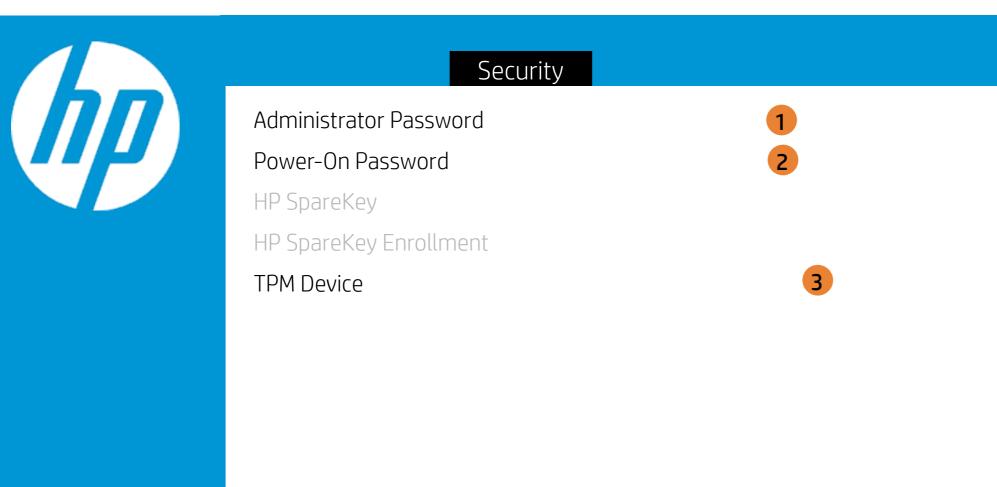
- 1. Administrator Password prevents unauthorized access to the Setup Utilities.
- 2. Power-On Password prevents unauthorized computer system start (boot).
- 3. If the item is set to HIdden, the TPM device is not visible to the operating system.
- 4. If the TPM device setting is set to Hidden, the BIOS 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 Prsenece 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.

3



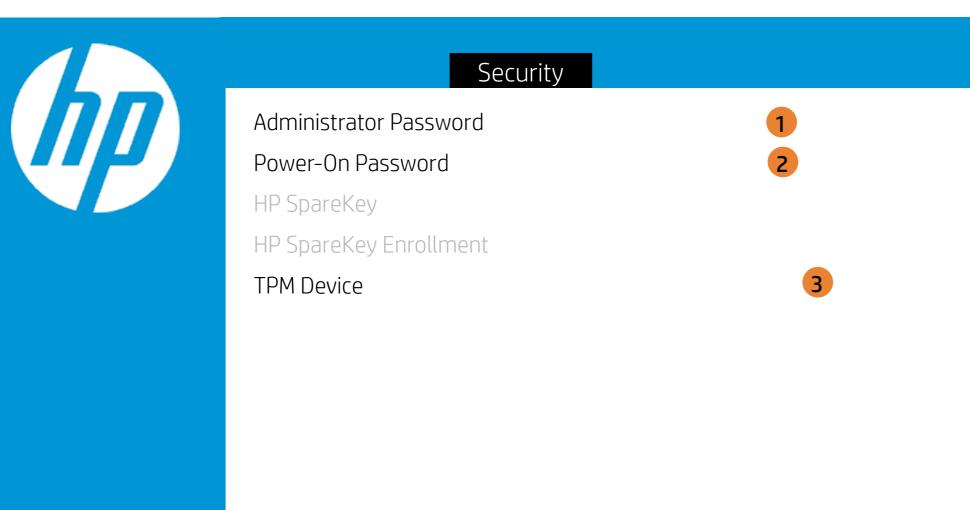
	Security	
Administrator Passw	vord	1
Power-On Password		2
HP SpareKey		
HP SpareKey Enrolln	nent	
TPM Device		

- 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 Prsenece 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.



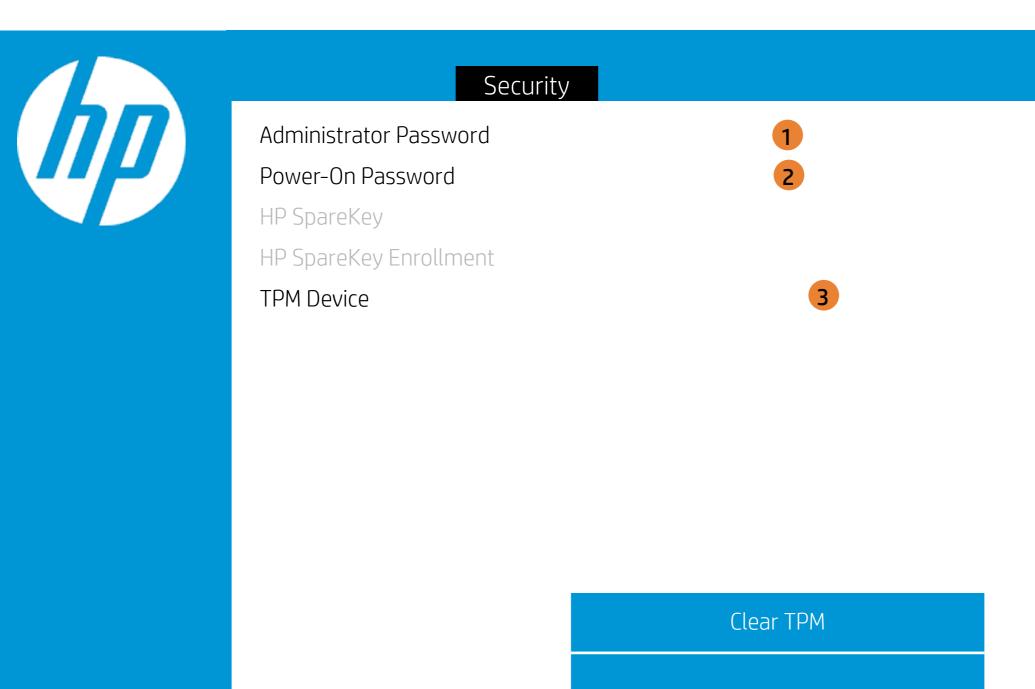
TPM Device

- 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 Prsenece 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.



TPM State

- 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 Prsenece 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.



- 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 Prsenece 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.

3



	Security	
Administrator Passw	vord	1
Power-On Password		2
HP SpareKey		
HP SpareKey Enrolln	nent	
TPM Device		

- 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 Prsenece 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.



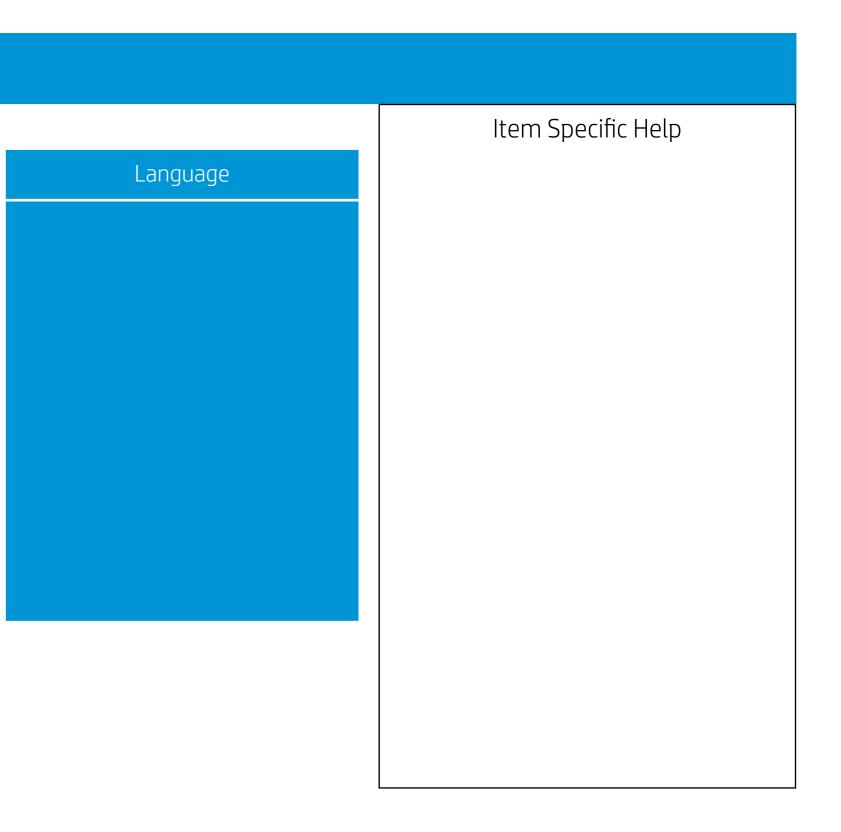
	Configuration	
Language		1
Virtualization Technology		2
Hyper-Threading		3
Fan Always On		4
Action Keys Mode		5
USB Charging		6
Battery Remaining Time		7
Adaptive Battery Optimizer		8
Keyboard Backlight Timeout		9
High resolution mode on USB-C DP all	t mode dock	10
In-bag detection		11
Auto resume		12
High resolution mode on USB-C DP all		10

	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 trough 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.	Set the Keyboard backlight to turn off after specified period of internal Keyboard/Touch Pad inactivity
10	. 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.
11	. The PC will detect when it is put in a bag or backpack and go into hibernation mode automatically.
12	. Auto resume from S4/S5 when lid is opened

Configuration



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



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 Auto resume

Virt

	Item Specific Help
tualization Technology	

Configuration



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

	Item Specific Help
Fan Always On	



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



	Item Specific Help
Hyper-Threading	

Configuration



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

	Item Specific Help
In bag detection	
In-bag detection	

Configuration



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

	Item Specific Help
Action Keys Mode	

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 Auto resume

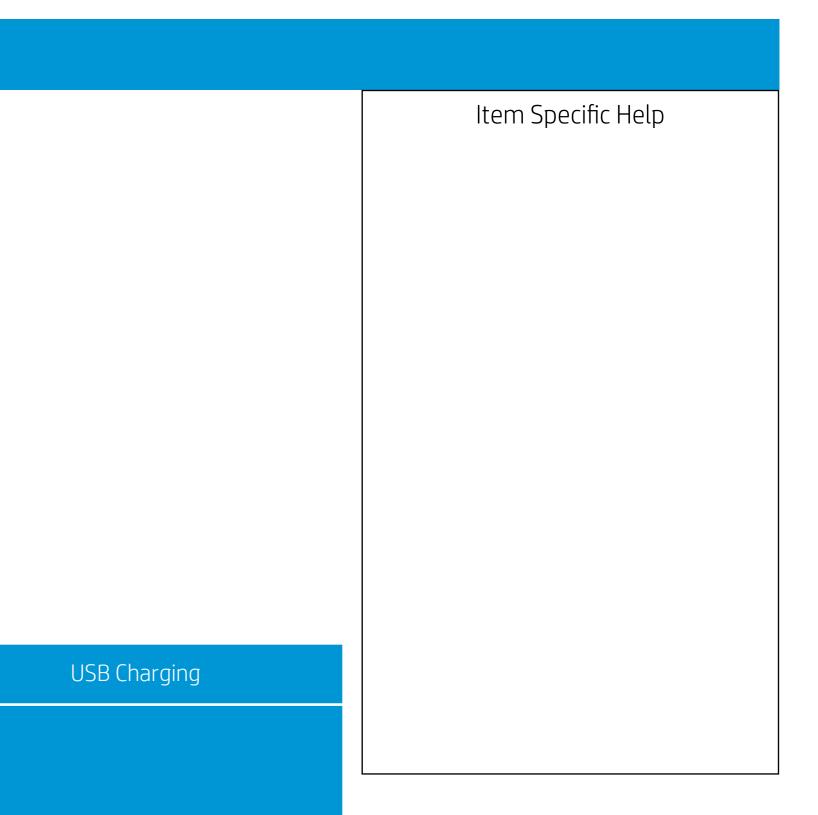
Keyl

	Item Specific Help
board Backlight Timeout	

Configuration



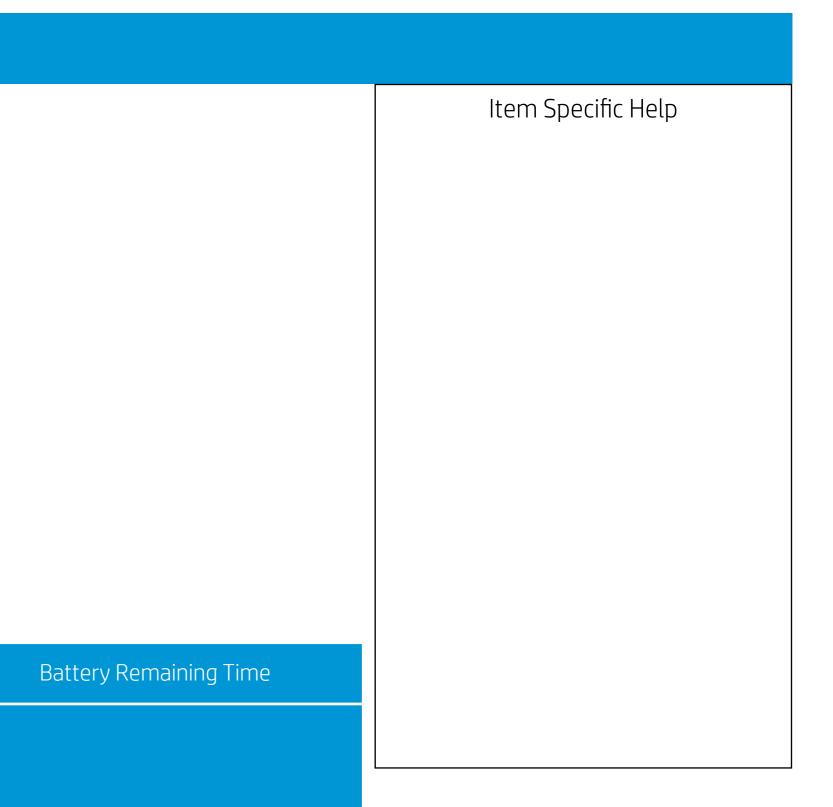
Language Virtualization Technology Hyper-Threading Fan Always On Action Keys Mode USB Charging Battery Remaining Time Adaptive Battery Optimizer Keyboard Backlight Timeout



Configuration



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



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 Auto resume

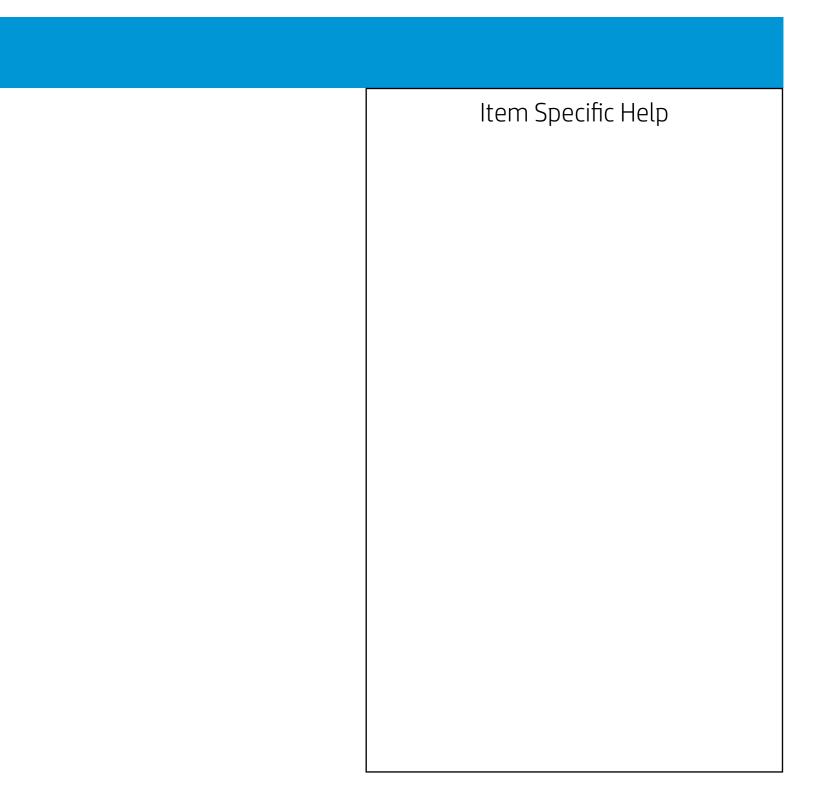
Ad

	Item Specific Help
aptive Battery Optimizer	

Configuration



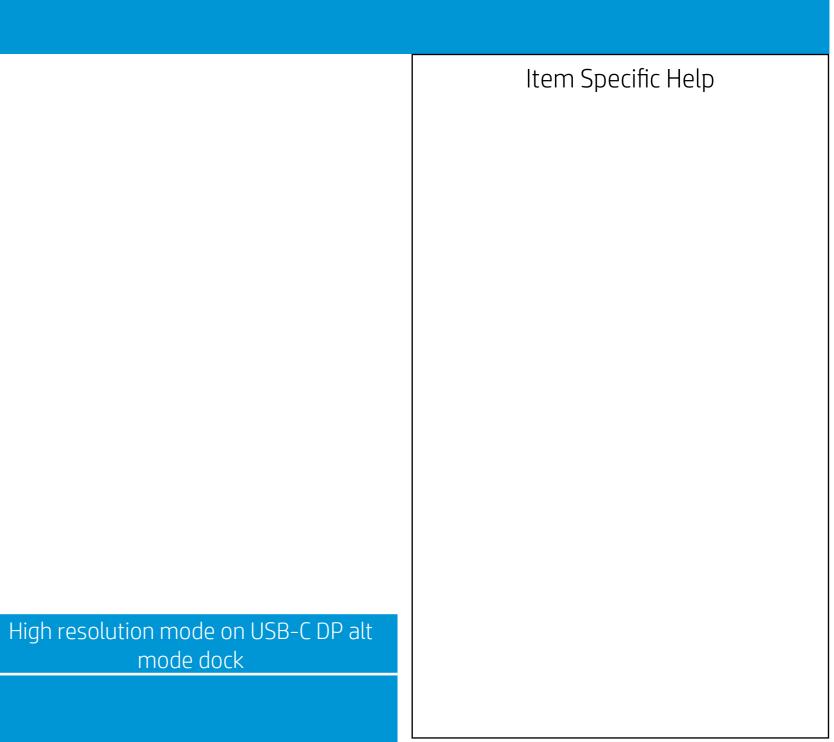
UEFI HII Configuration



Configuration



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



Configuration



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

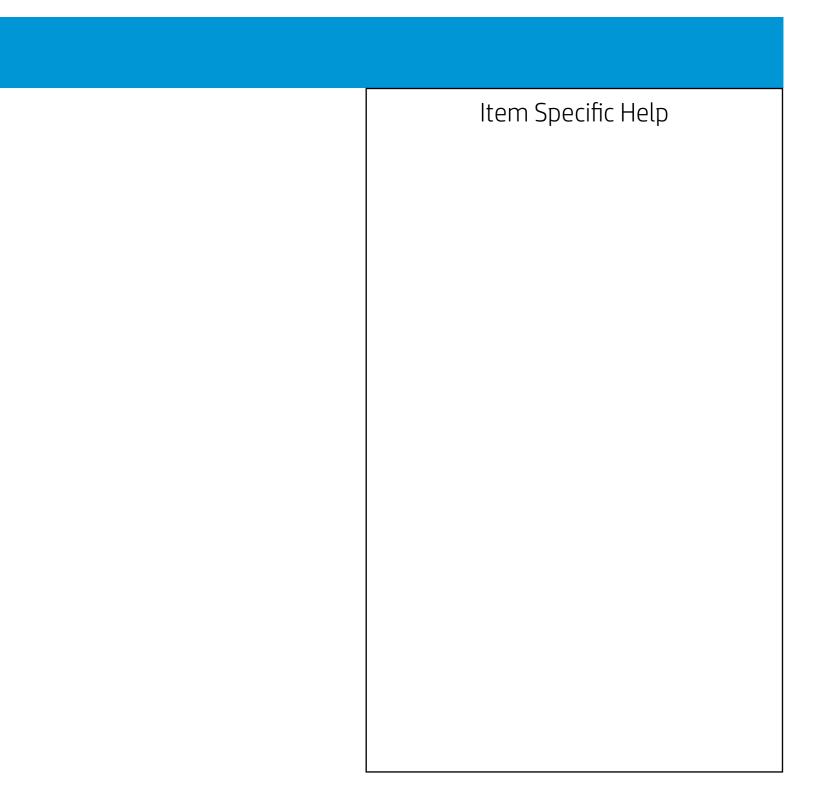
	Item Specific Help
Auto Resume	



Configuration

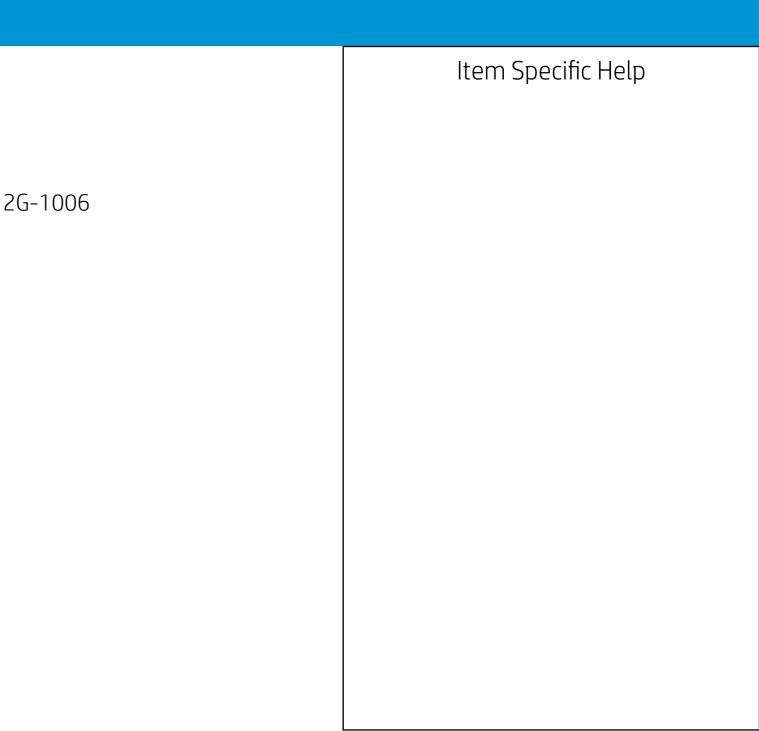
Intel(R) RST 18.1.1.5201 RST VMD Driver

Non-RAID Phyisical Disks:





	Configuration
RAID VOLUME INFO	
Port:	0.0
Model Number:	WDC PC SN730 SDBPNTY-5120
Serial Number:	476.9GB
Status:	Non-RAID
Controller Type:	NVMe
Controller Interface:	PCIe



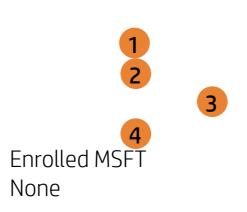


Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

UEFI Boot Order ► OS Boot Manager



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

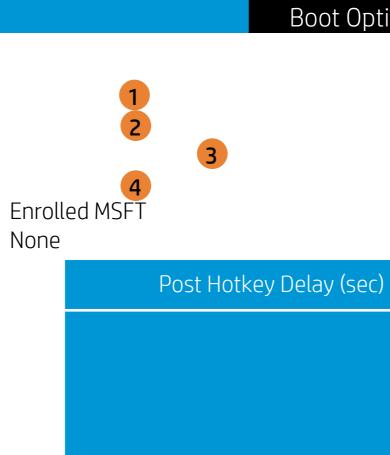


Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol

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



tions	
	Item Specific Help
	1. Enable/Disable USB boot.
	 Enable/Disable network boot during boot time.
	3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se-
)	lected, BIOS will use IPv4 first.
	4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

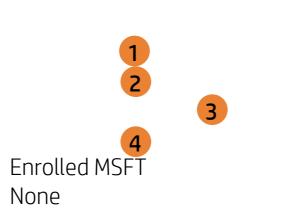


Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol

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



USB Boot

Boot Options	
	Item Specific Help
	1. Enable/Disable USB boot.
	 Enable/Disable network boot during boot time.
	 Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.
Boot	4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.



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



Network Boot

Boot Options	
	Item Specific Help
	1. Enable/Disable USB boot.
	 Enable/Disable network boot during boot time.
	 Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.
ork Boot	4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

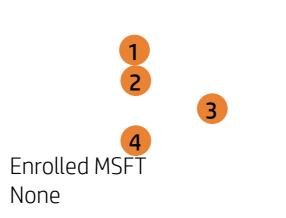


Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol

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



Network Boot Protocol

Root Options	
Boot Options	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 se-
oot Protocol	4. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

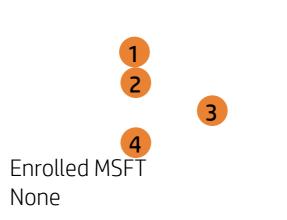


Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

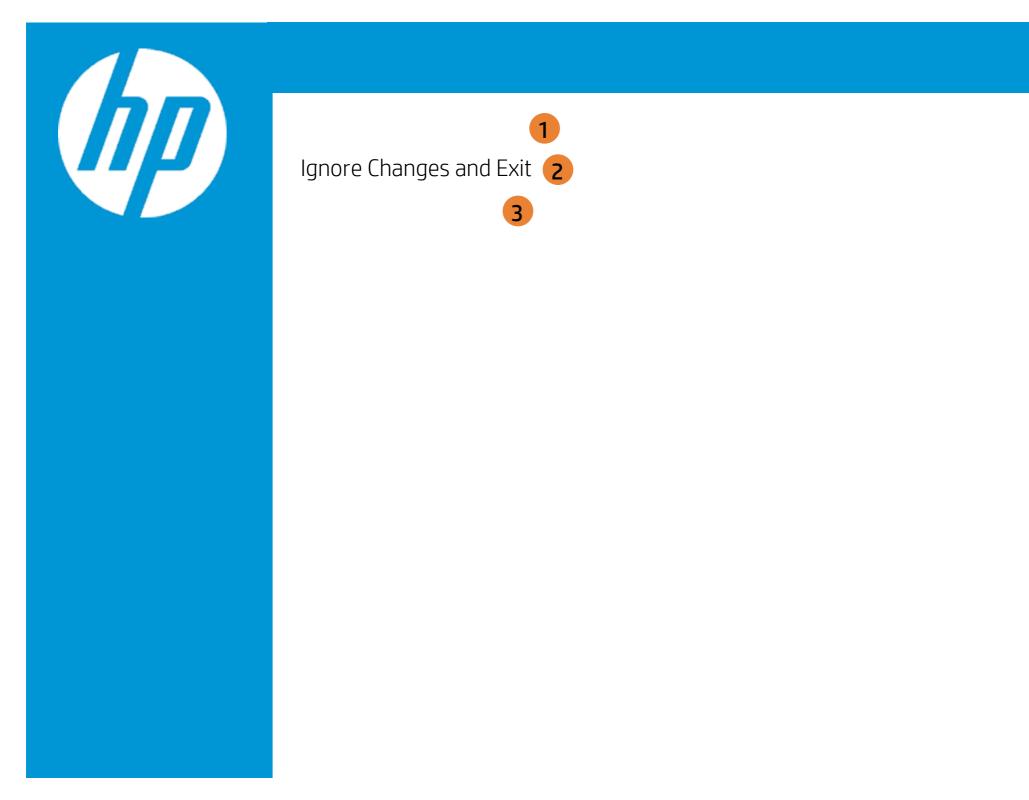
UEFI Boot Order ► OS Boot Manager Internal CD/DVD ROM Drive



Secure Boot

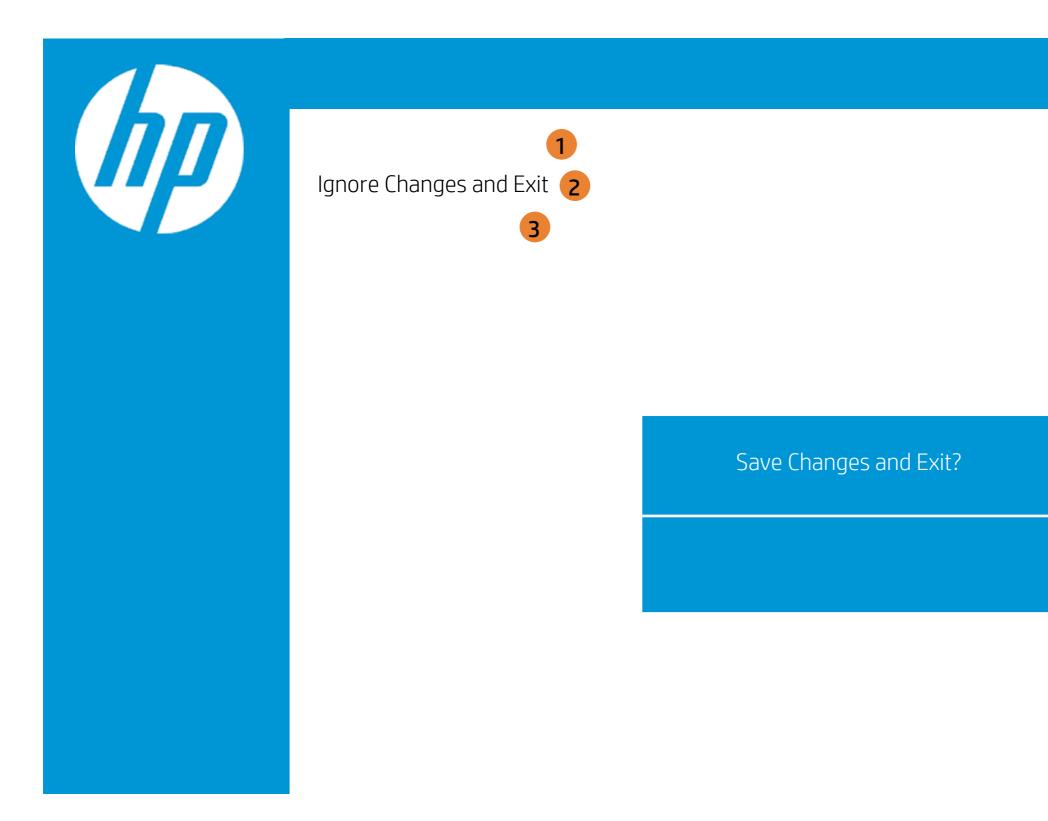
Boot Options	
	Item Specific Help
	1. Enable/Disable USB boot.
	2. Enable/Disable network boot during boot time.
	3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.
re Boot	4. Secure Boot flow control. Secure Boot is possible only if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

Exit Menu



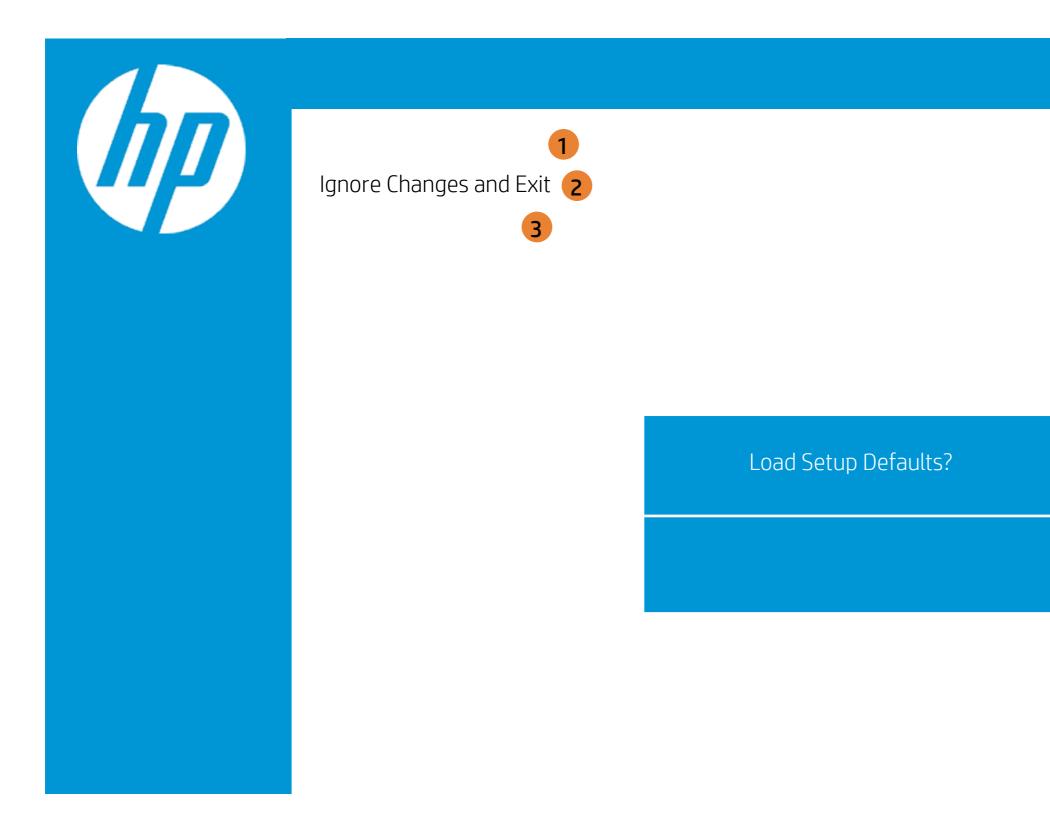
Exit	
	Item Specific Help
	1. Exit System Setup and save your changes to CMOS.
	2. Exit utility without saving Setup data to CMOS.
	3. Load default values for all SETUP items.

Exit Menu



Exit	
	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	
	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.