Interactive BIOS simulator

HP ENVY All-in-One 32-a0xxx

Welcome to the interactive BIOS simulator for the
HP ENVY All-in-One 32-a0xxx

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

Exit

Main Menu

Back to BIOS Utility Menus

Main | Security | Configuration | Boot Options | Exit

System Time	[22:02:59]
System Date	12/09/2019
Product Name	HP ENVY All-in-One 32-a0xxx
System Family	HP Pavilion
Product Number	NZFPVT#001
System Board ID	86C6
Born On Date	00/00/0000
Processor Type	Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz
Total Memory	16 GB
BIOS Vendor	AMI
BIOS Version	B.07
► Device Firmware Revision (1)	
Serial Number	8CC93416Q4
UUID	94ADA48B-FF63-C57D-8FC8-10AC7D305049
System Board CT Number	PJEBD0A8JCM03C
Factory installed OS	Win10
► System Log (2)	
Build ID	19WW2V1T6af#SABA#DABA
Feature Byte	3E3K 3N4C 4h6b 7K7Q 7S7W 7saB apaq asbh bzcb dUdp dqfP gTHZ j6KK KN .aA

Item Specific Help

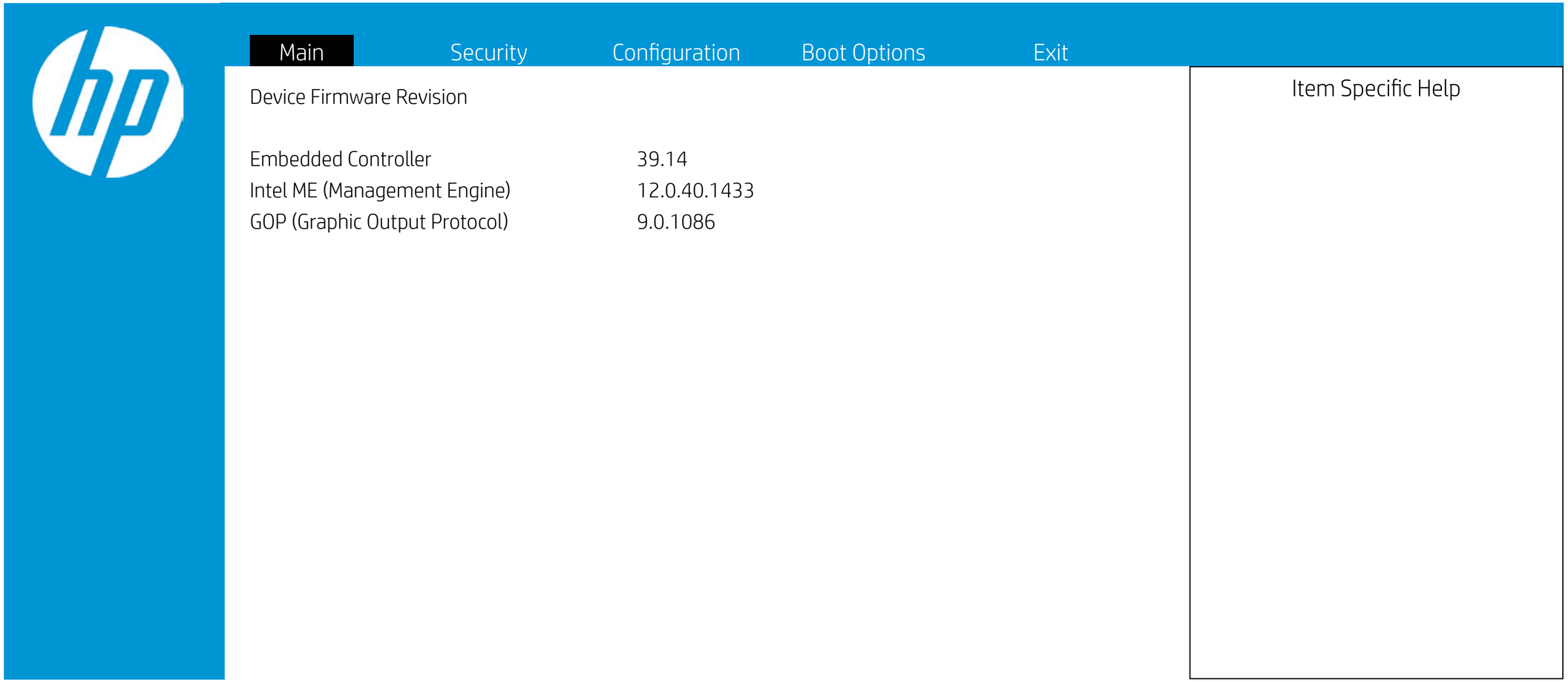
1. Provides firmware revision information of devices built in the system.

2. View System Log.

Back to Welcome Page

Main Menu

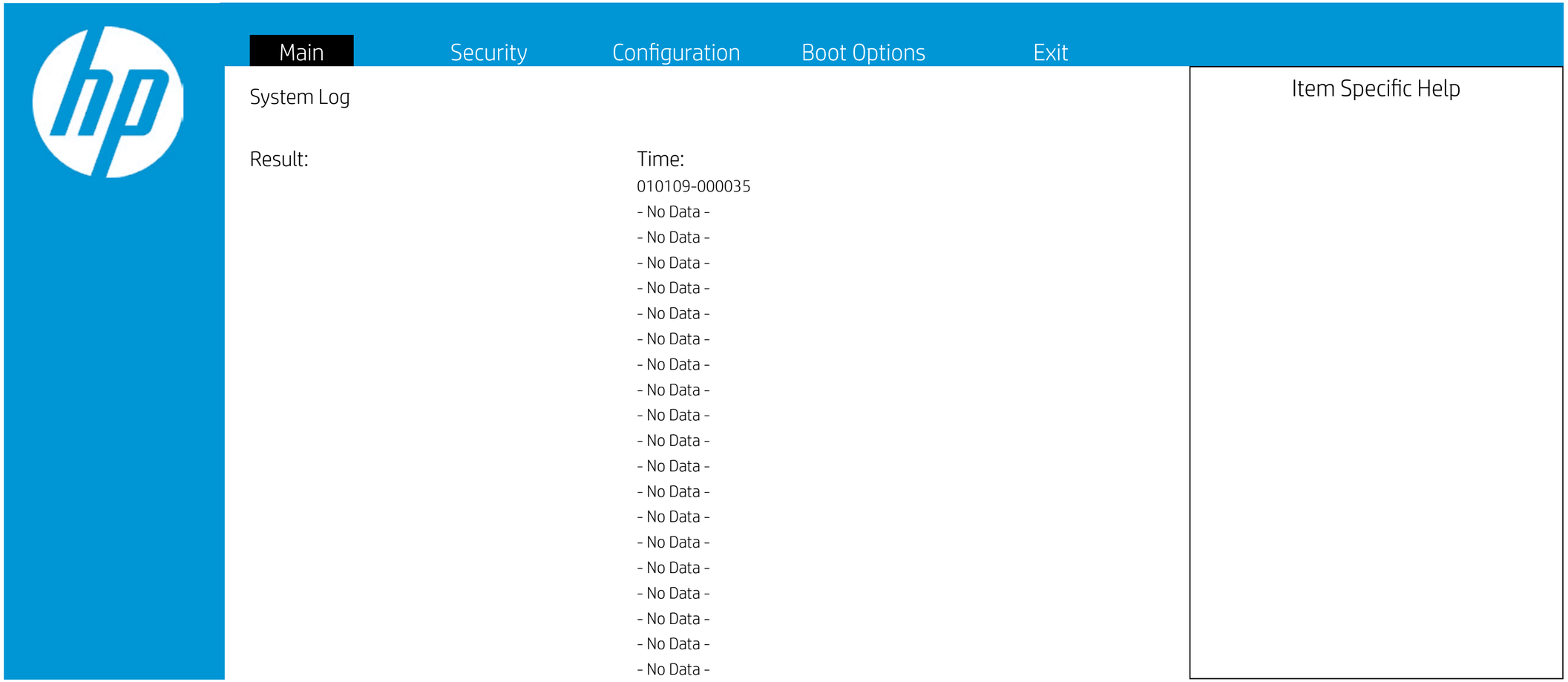
Back to BIOS Utility Menus



Back to Welcome Page

Main Menu

Back to BIOS Utility Menus



Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults 7	

Set Administrator Password

Enter New Password	[ ]
Confirm New Password	[ ]

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

Set Power-On Password

Enter New Password	[ ]
Confirm New Password	[ ]

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

Intel Software Guard Extensions (SGX)

Enabled
Disabled
S/W Controlled

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

TPM Device

Hidden

Available

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

TPM State

Disabled

Enabled

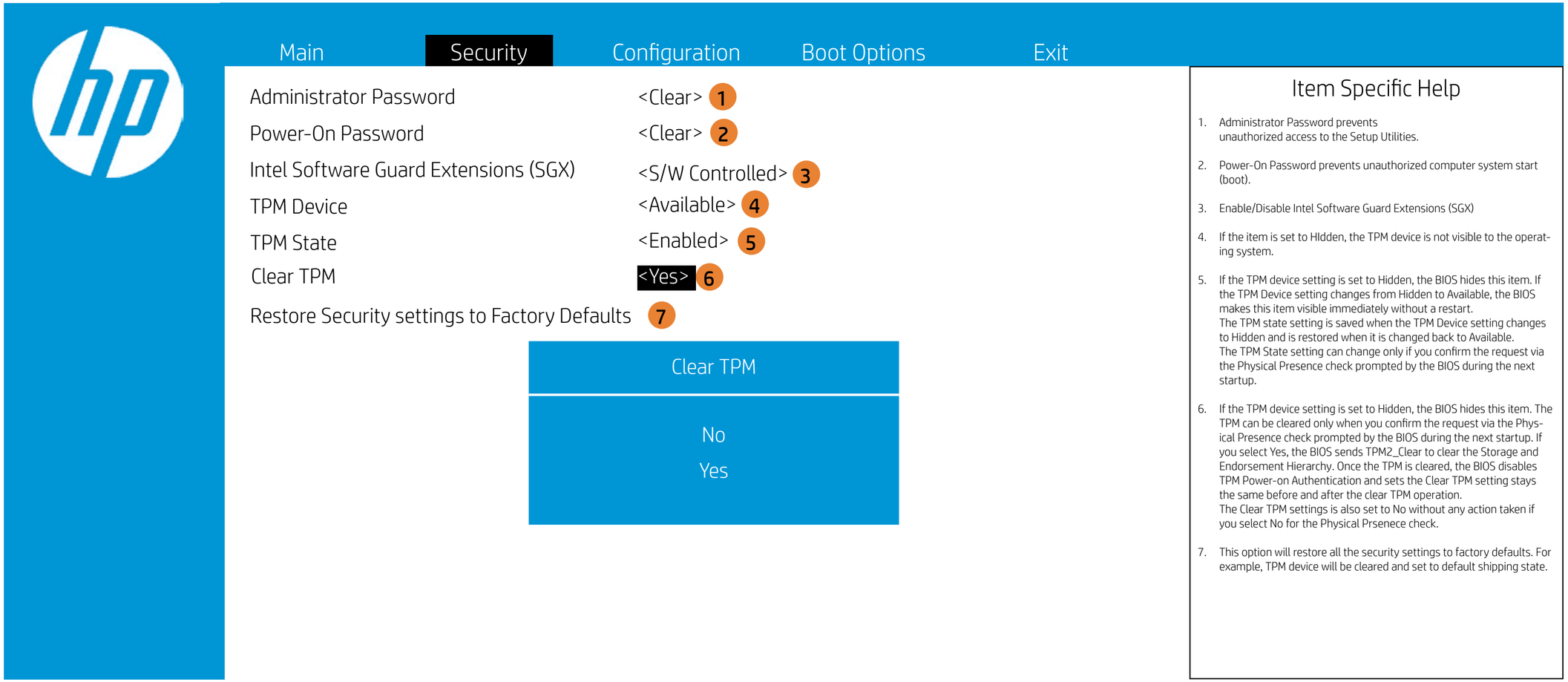
Item Specific Help

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 Prsenece 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.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Back to Welcome Page

Security Menu

Back to BIOS Utility Menus

Main | **Security** | Configuration | Boot Options | Exit

Administrator Password	<Clear> 1
Power-On Password	<Clear> 2
Intel Software Guard Extensions (SGX)	<S/W Controlled> 3
TPM Device	<Available> 4
TPM State	<Enabled> 5
Clear TPM	<Yes> 6
Restore Security settings to Factory Defaults	7

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 EXC key to continiue without accepting the pending change.

Reset Security Defaults (023)

0369 + ENTER - to complete the change

ESC - continue without changing

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

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 Prsenece 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.

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

Main | Security | Configuration | Boot Options | Exit

Language	<English> 1
Virtualization Technology	<Enabled> 2
SATA Emulation	<AHCI> 3
Num Lock State at Power-On	<On> 4
S4/S5 Wake on LAN	<Enabled> 5
► Thermal	

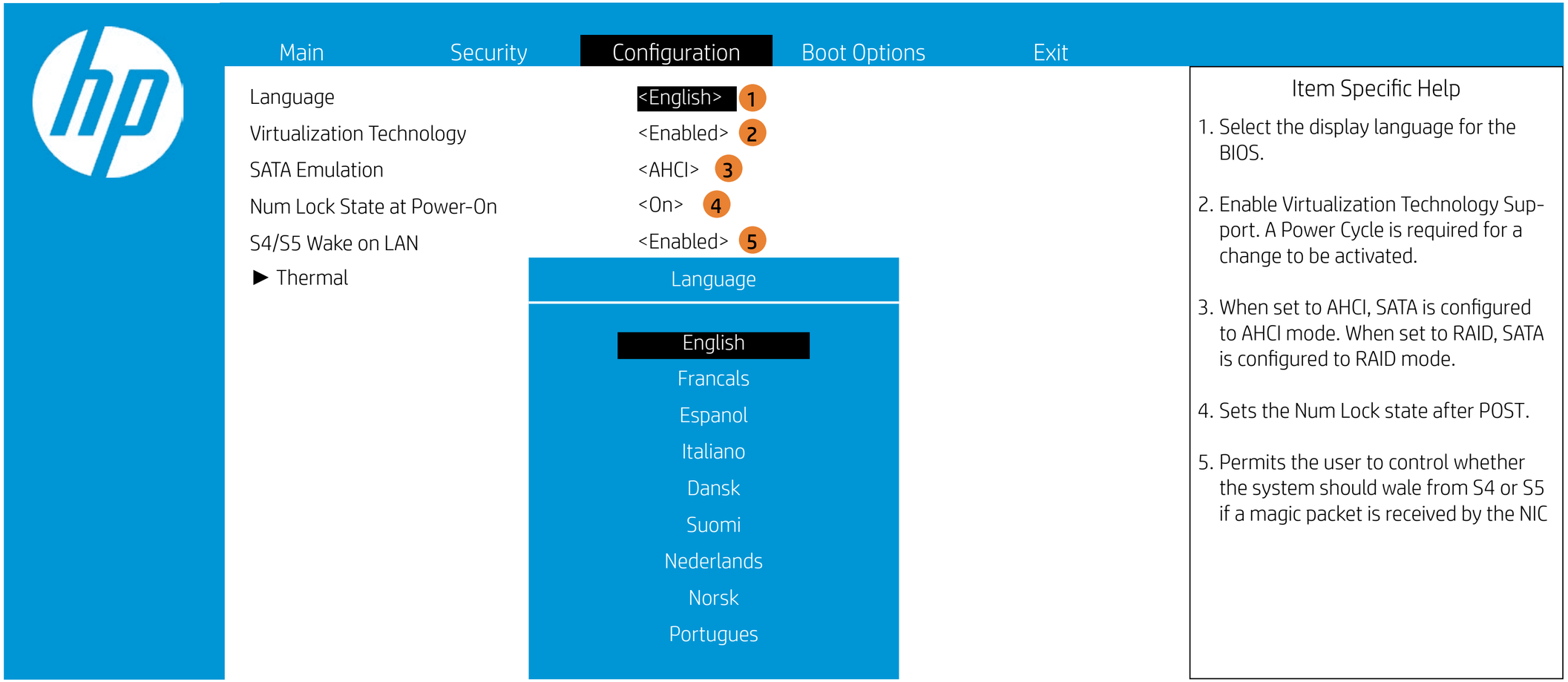
Item Specific Help

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. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
4. Sets the Num Lock state after POST.
5. Permits the user to control whether the system should wale from S4 or S5 if a magic packet is received by the NIC

Back to Welcome Page

Configuration Menu

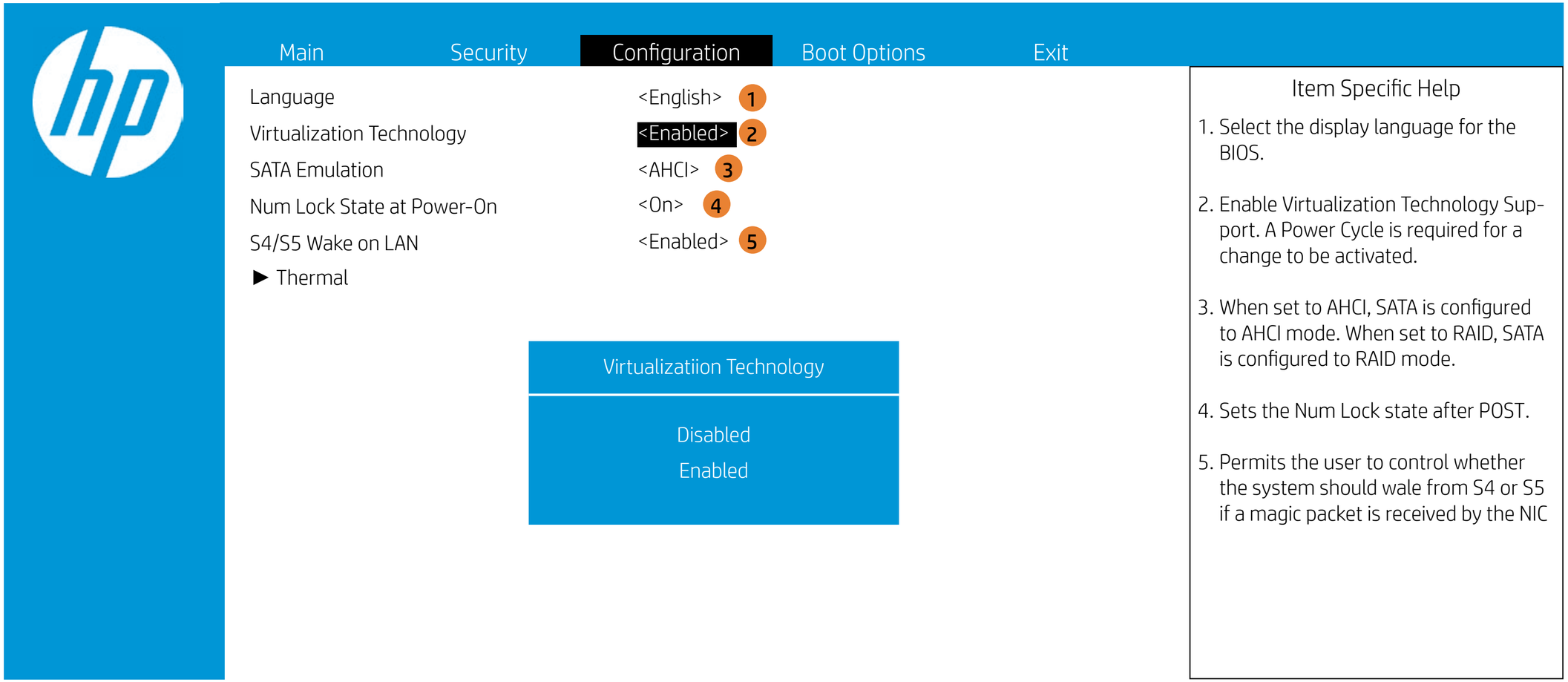
Back to BIOS Utility Menus



Back to Welcome Page

Configuration Menu

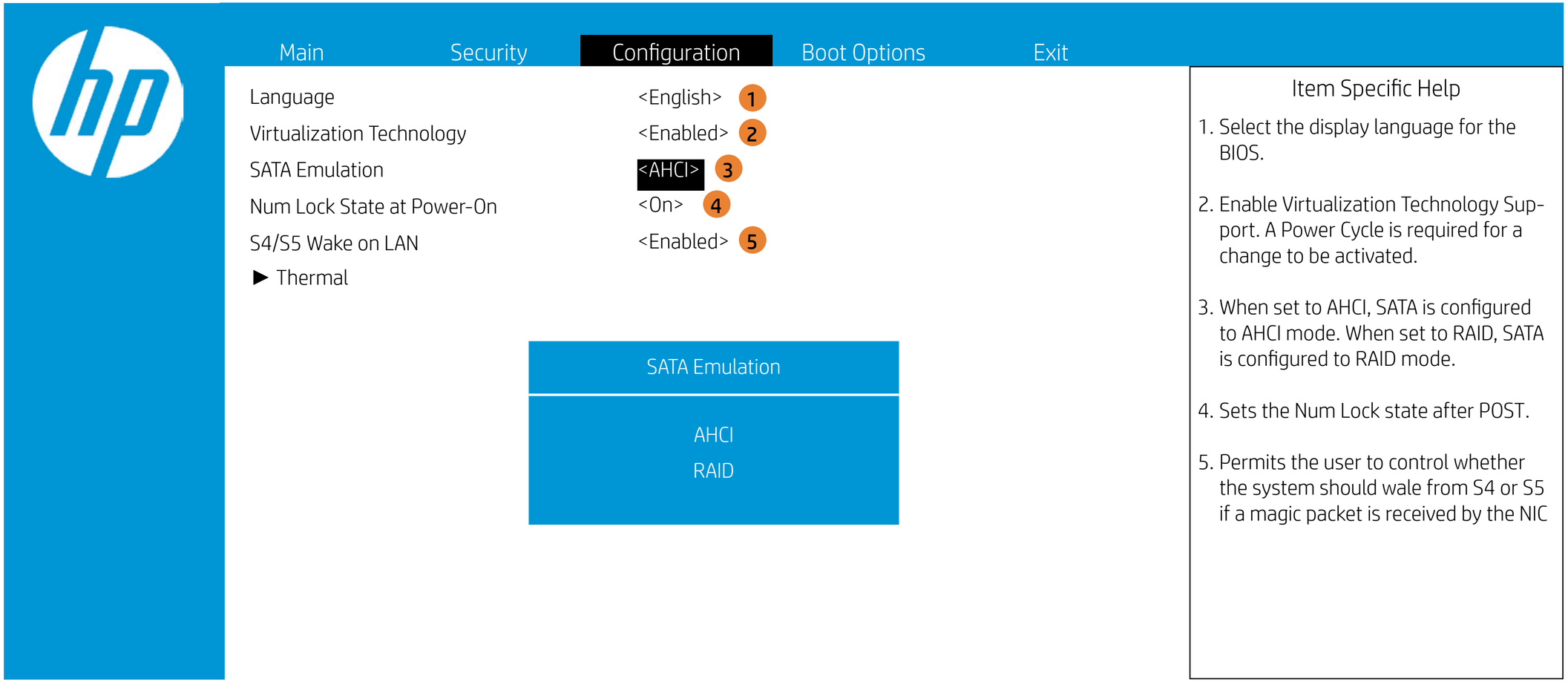
Back to BIOS Utility Menus



Back to Welcome Page

Configuration Menu

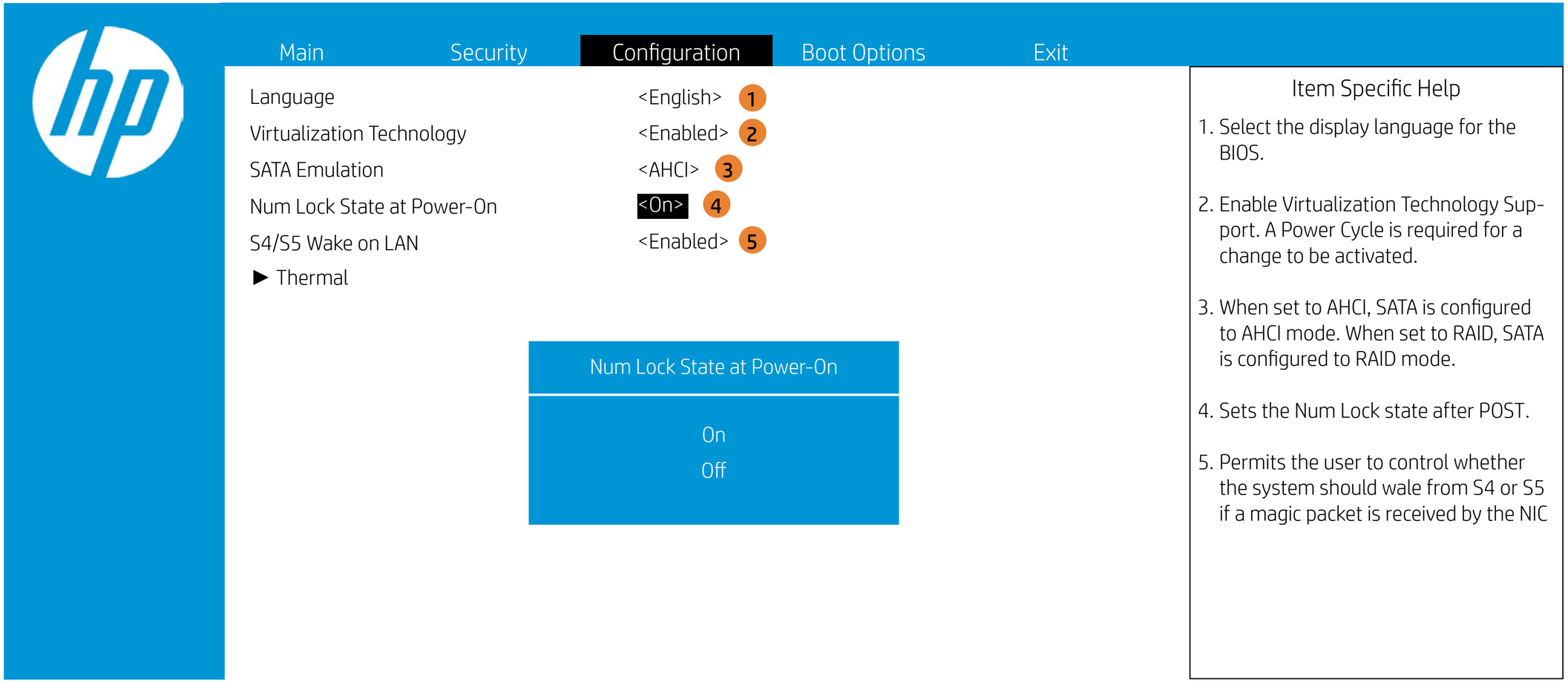
Back to BIOS Utility Menus



Back to Welcome Page

Configuration Menu

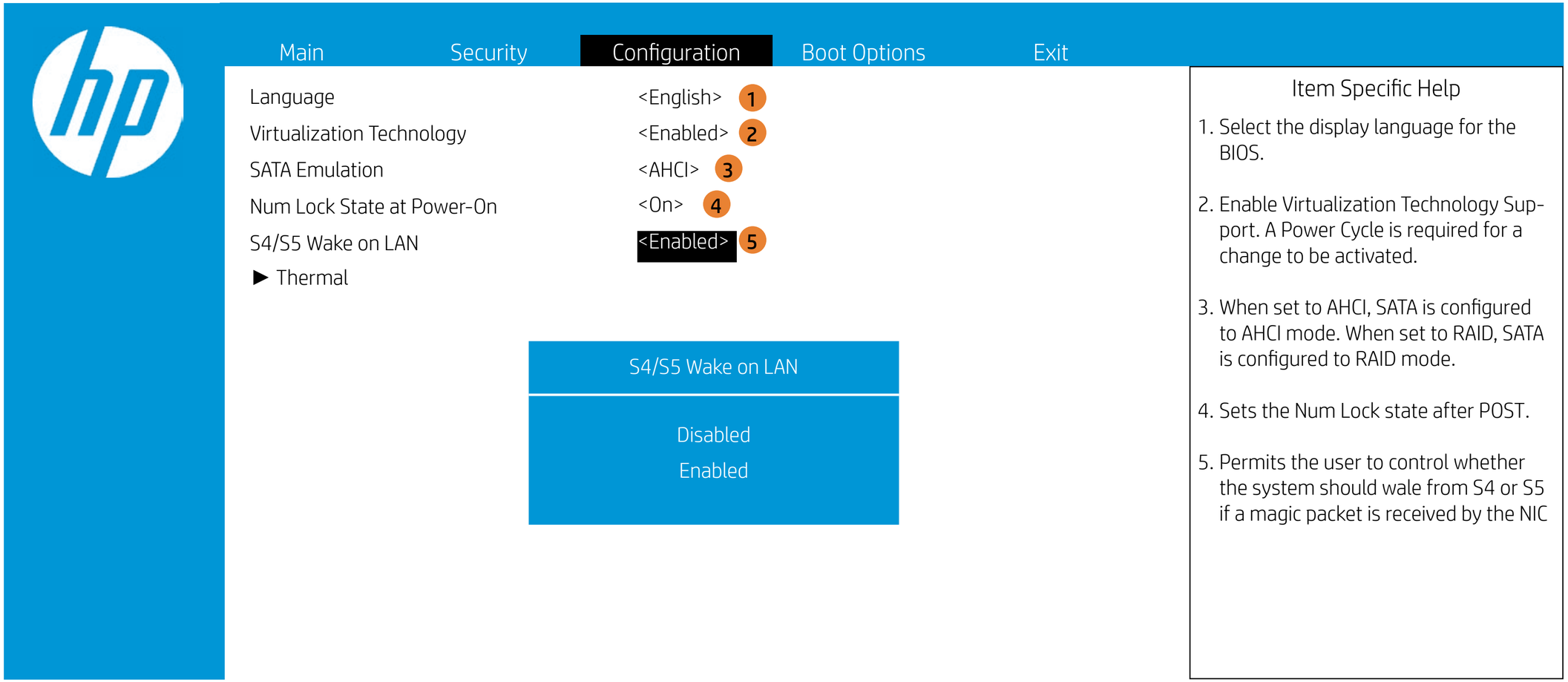
Back to BIOS Utility Menus



Back to Welcome Page

Configuration Menu

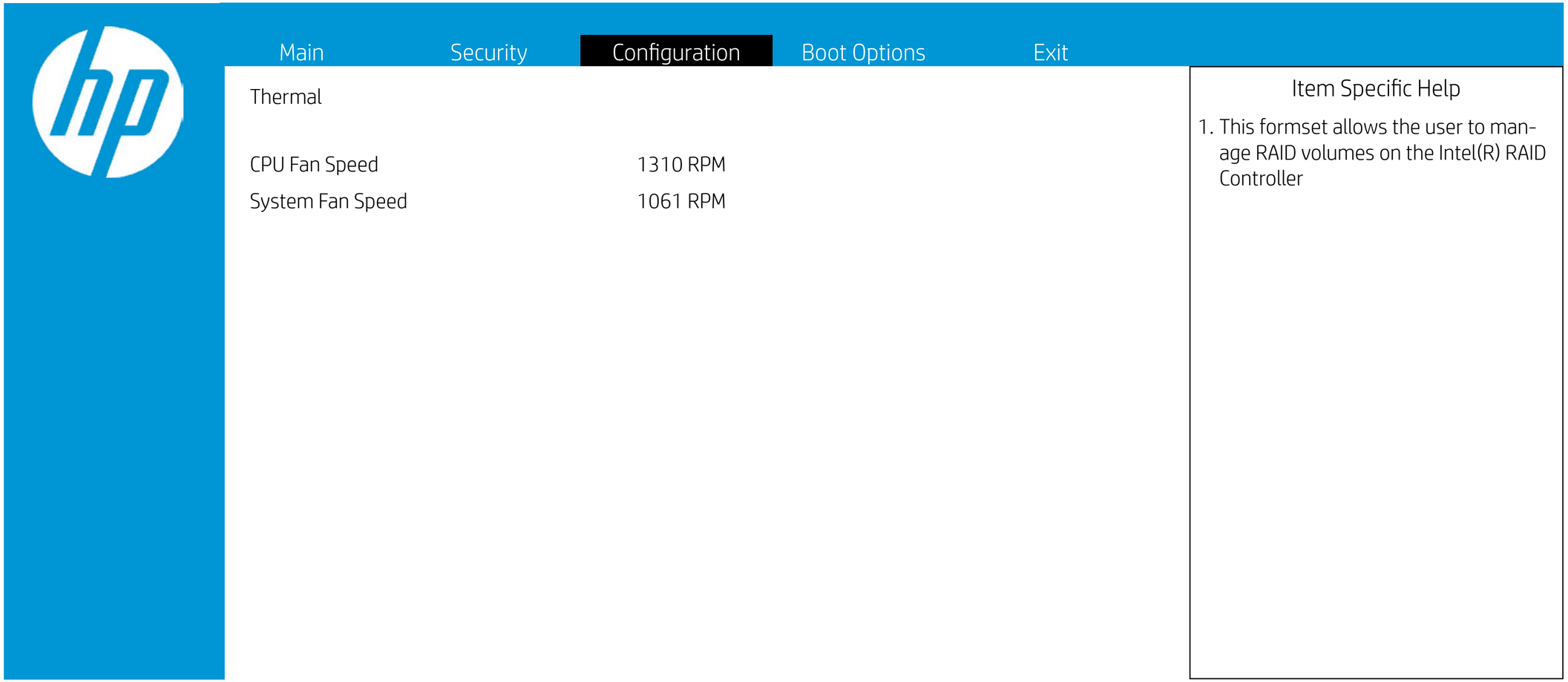
Back to BIOS Utility Menus



Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB 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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Post Hotkey Delay (sec)

- 0
- 5
- 10
- 15
- 20

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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

USB Boot

Disabled

Enabled

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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Network Boot

Disabled

Enabled

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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Network Boot Protocol

IPv4 (UEFI)

IPv6 (UEFI)

IPv4 + IPv6 (UEFI)

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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None
Clear All Secure Boot Keys	
Load HP Factory Default Keys	
Load MSFT Debug Policy Keys	

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Support

Disabled

Enabled

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.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus

Main | Security | Configuration | **Boot Options** | Exit

Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Legacy Support	<Disabled> 4
Secure Boot	<Enabled> 5
Platform Key	Enrolled MSFT
Pending Action	None

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

UEFI Boot Order
- ► OS Boot Manager
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Legacy Boot Order
- ► Internal Hard Drive
- Internal CD/DVD ROM Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive

Secure Boot

Disabled

Enabled

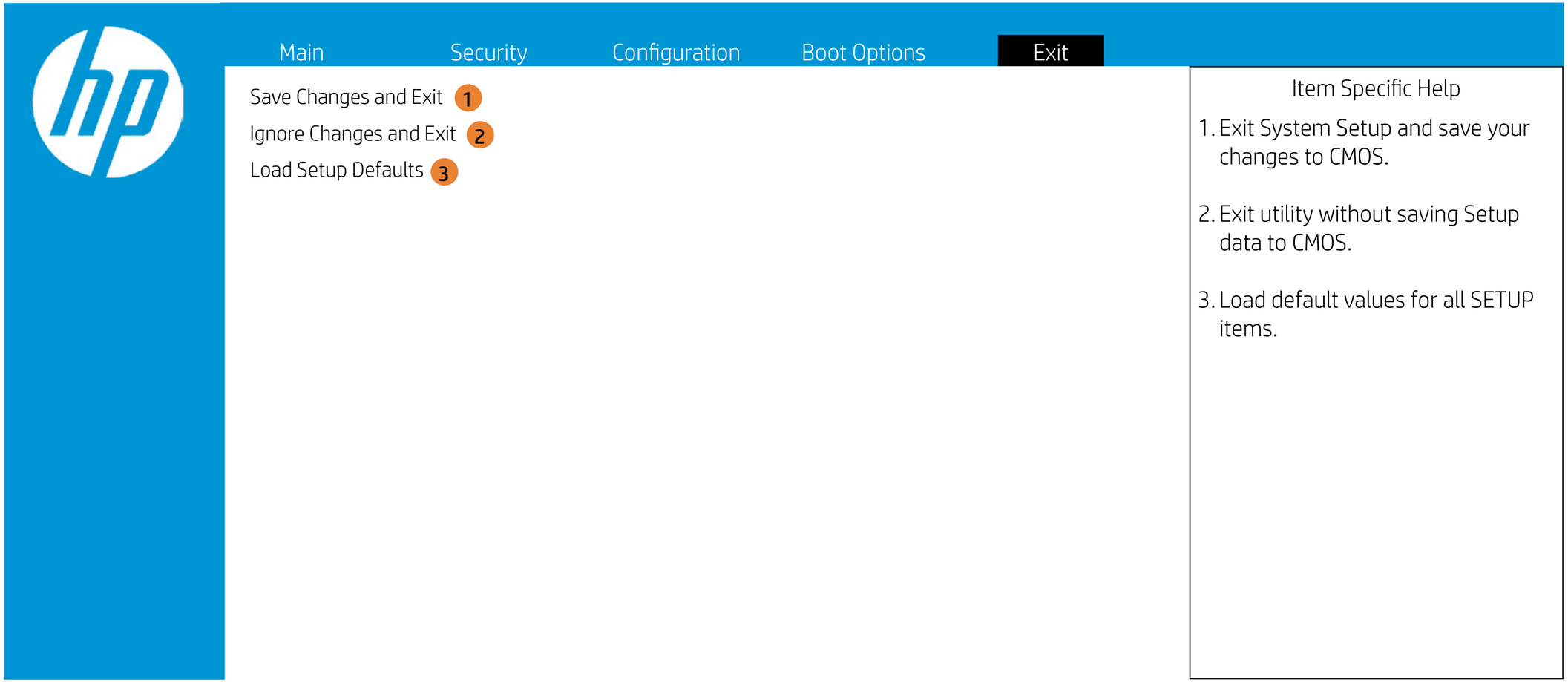
Item Specific Help

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.

Back to Welcome Page

Exit Menu

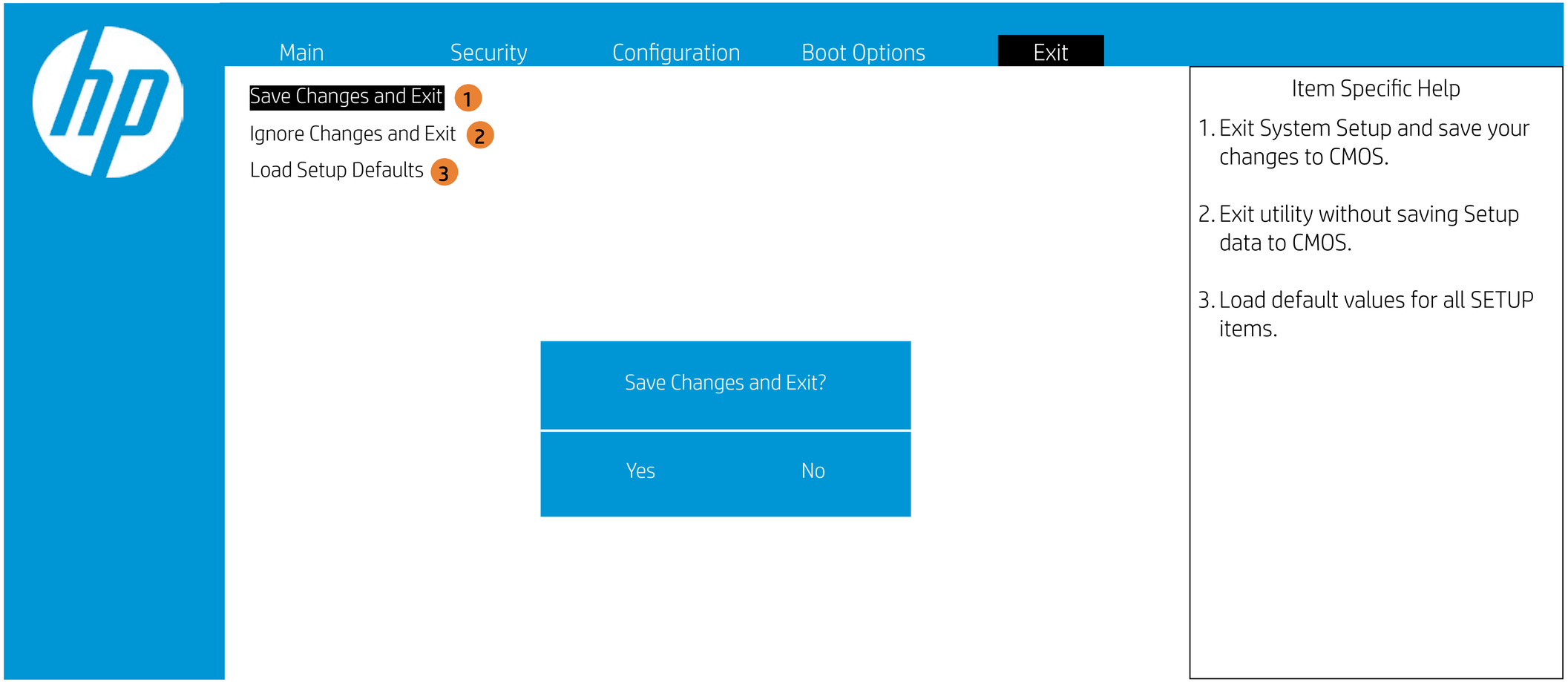
Back to BIOS Utility Menus



Back to Welcome Page

Exit Menu

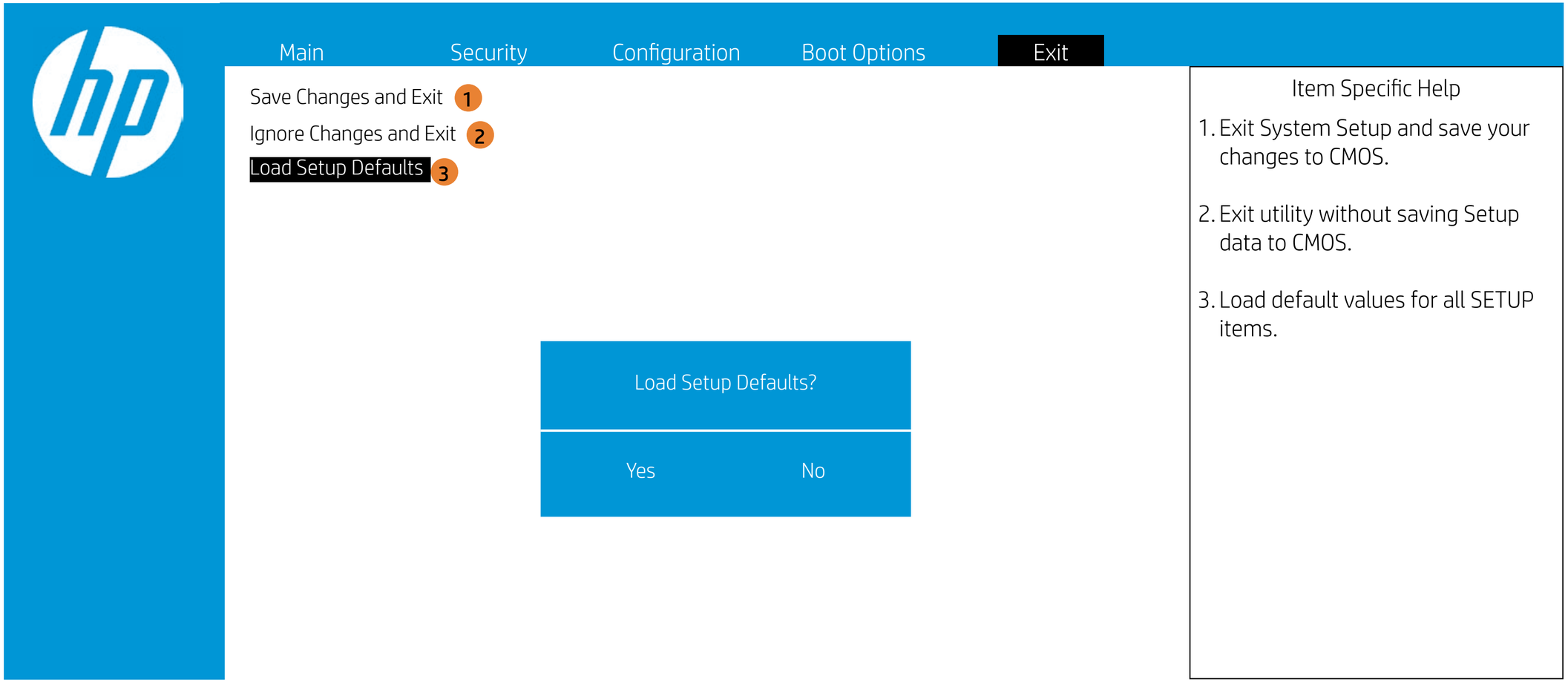
Back to BIOS Utility Menus



Back to Welcome Page

Exit Menu

Back to BIOS Utility Menus



Back to Welcome Page