Interactive BIOS simulator

HP ENVY x360 15-eu0xxx Convertible PC

Welcome to the interactive BIOS simulator for the
HP ENVY x360 15-eu0xxx 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.

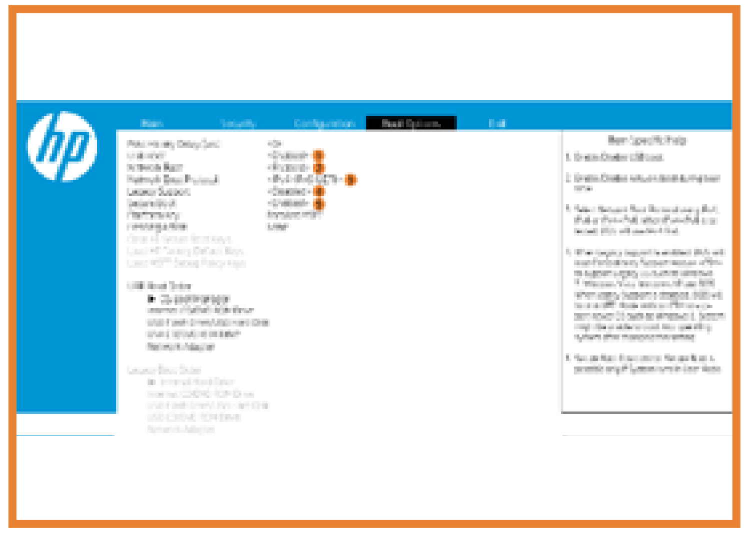
BIOS Utility Menus

Back to Welcome Page

Main

Security

Configuration

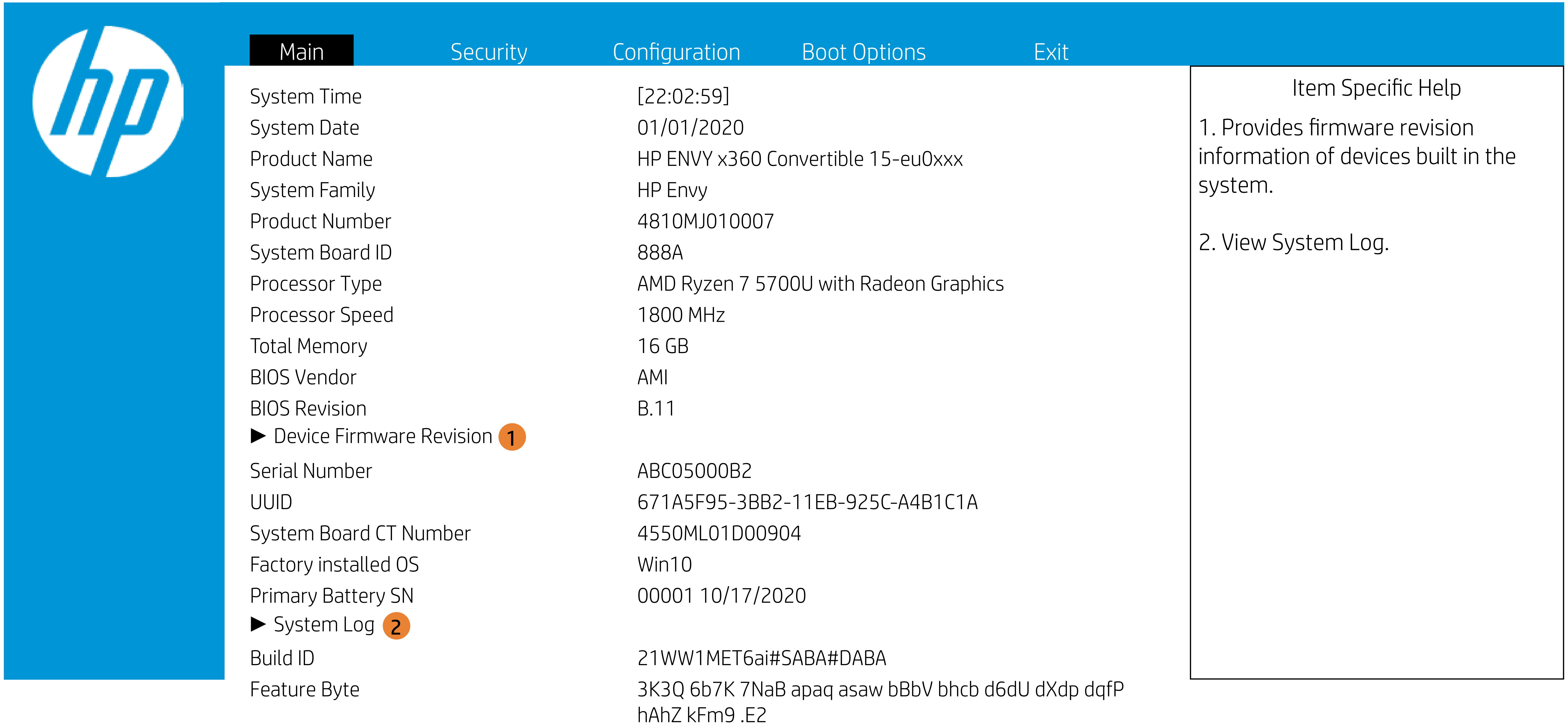


Boot Options

Exit

Main Menu

Back to BIOS Utility Menus



System Time	[22:02:59]
System Date	01/01/2020
Product Name	HP ENVY x360 Convertible 15-eu0xxx
System Family	HP Envy
Product Number	4810MJ010007
System Board ID	888A
Processor Type	AMD Ryzen 7 5700U with Radeon Graphics
Processor Speed	1800 MHz
Total Memory	16 GB
BIOS Vendor	AMI
BIOS Revision	B.11
▶ Device Firmware Revision 1	
Serial Number	ABC05000B2
UUID	671A5F95-3BB2-11EB-925C-A4B1C1A
System Board CT Number	4550ML01D00904
Factory installed OS	Win10
Primary Battery SN	00001 10/17/2020
▶ System Log 2	
Build ID	21WW1MET6ai#SABA#DABA
Feature Byte	3K3Q 6b7K 7NaB apaq asaw bBbV bhcb d6dU dXdp dqfP hAhZ kFm9 .E2

Item Specific Help

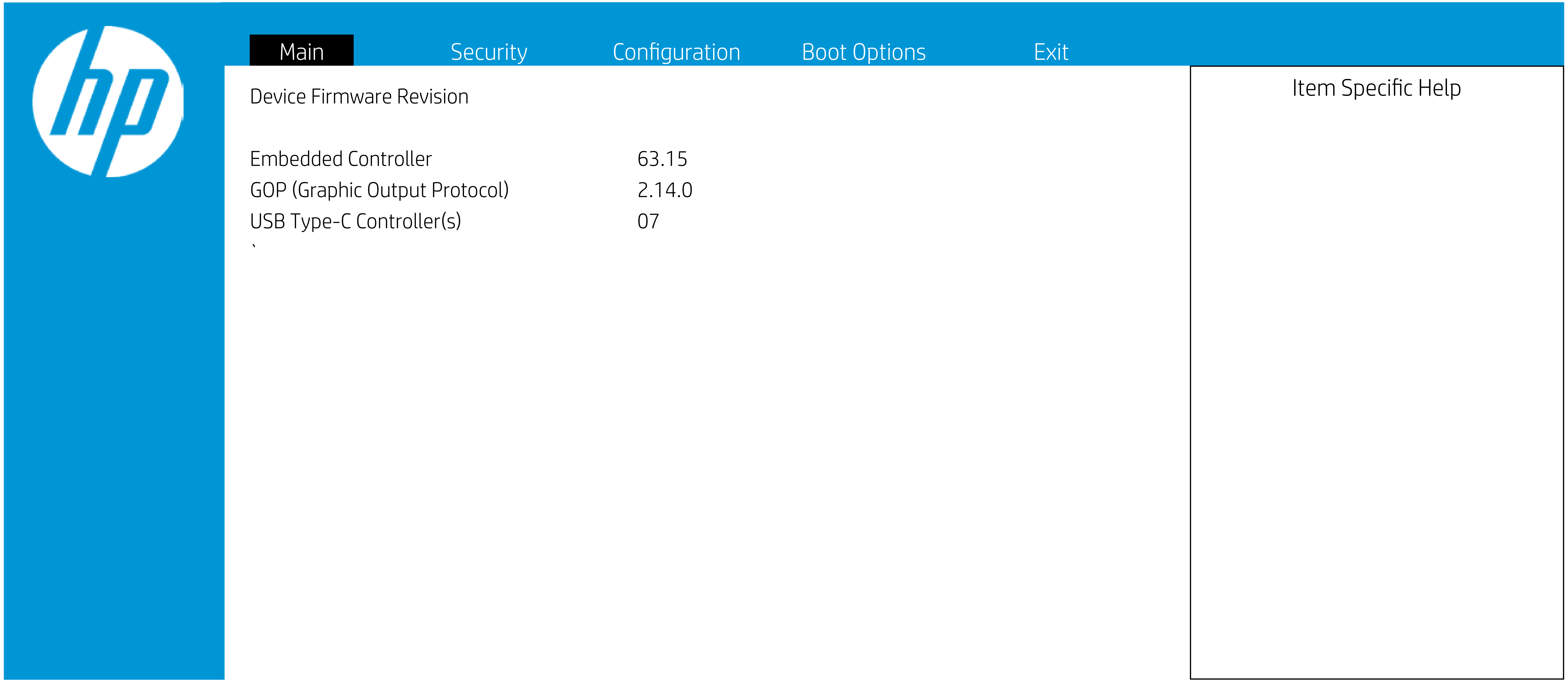
1. Provides firmware revision information of devices built in the system.

2. View System Log.

Back to Welcome Page

Main Menu

Back to BIOS Utility Menus



Device Firmware Revision

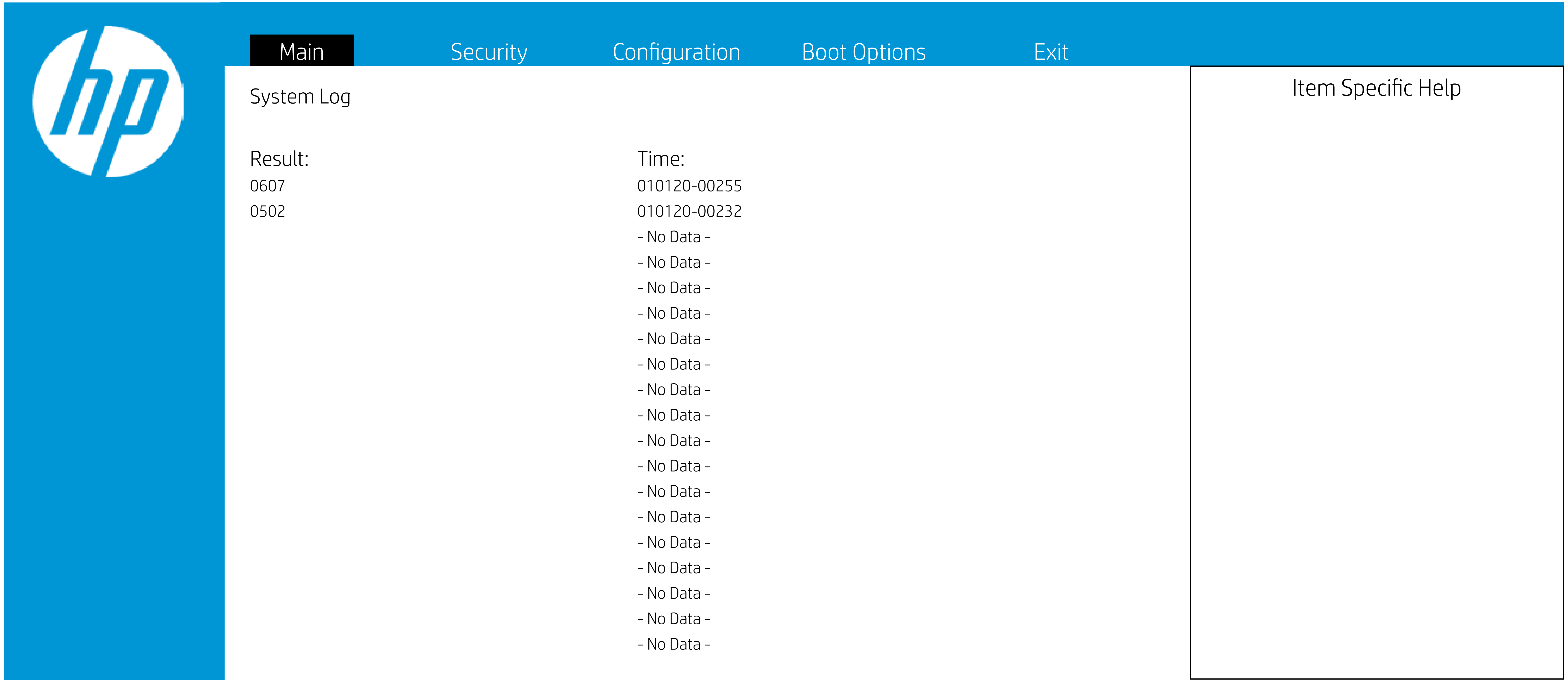
Embedded Controller	63.15
GOP (Graphic Output Protocol)	2.14.0
USB Type-C Controller(s)	07

`

Back to Welcome Page

Main Menu

Back to BIOS Utility Menus



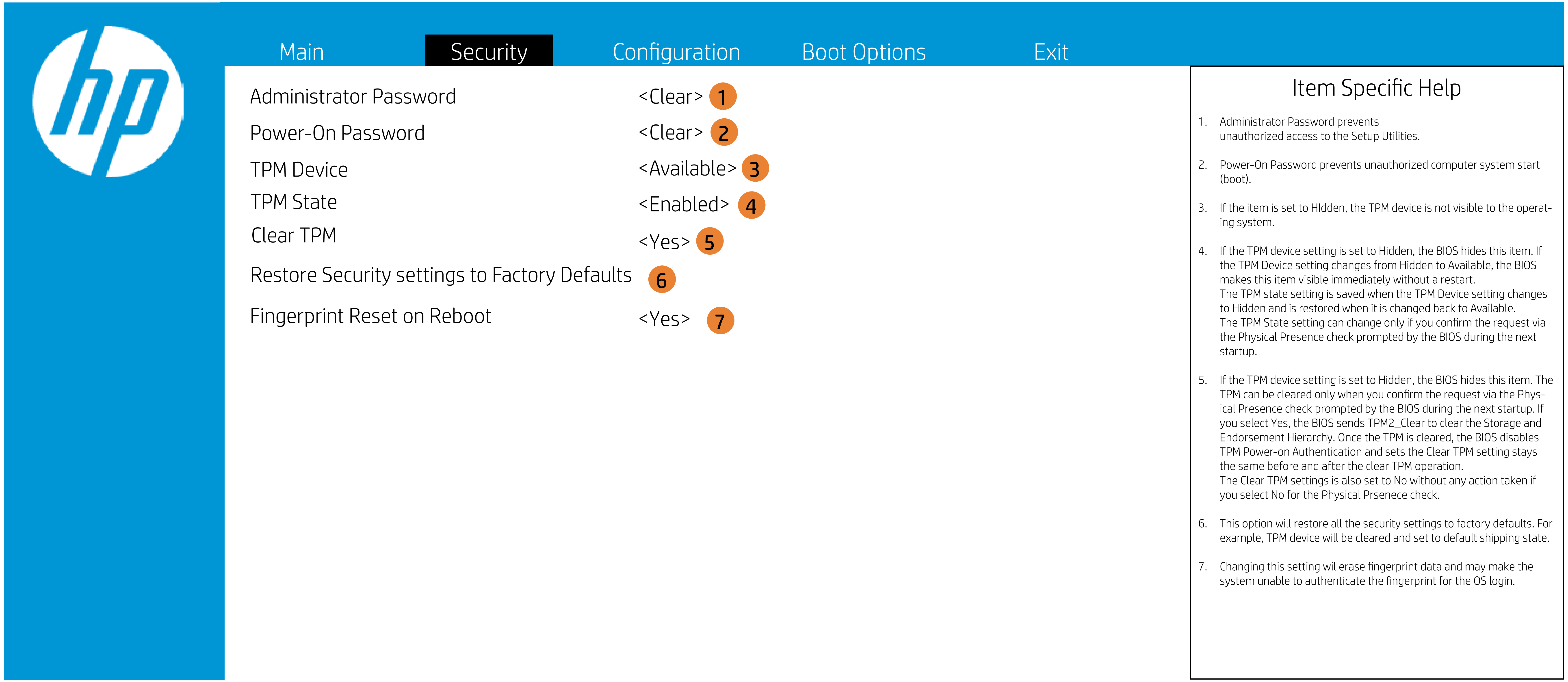
System Log

```
Result:                         Time:
0607                            010120-00255
0502                            010120-00232
                                - 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 -
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password	<Clear>	1
Power-On Password	<Clear>	2
TPM Device	<Available>	3
TPM State	<Enabled>	4
Clear TPM	<Yes>	5
Restore Security settings to Factory Defaults		6
Fingerprint Reset on Reboot	<Yes>	7

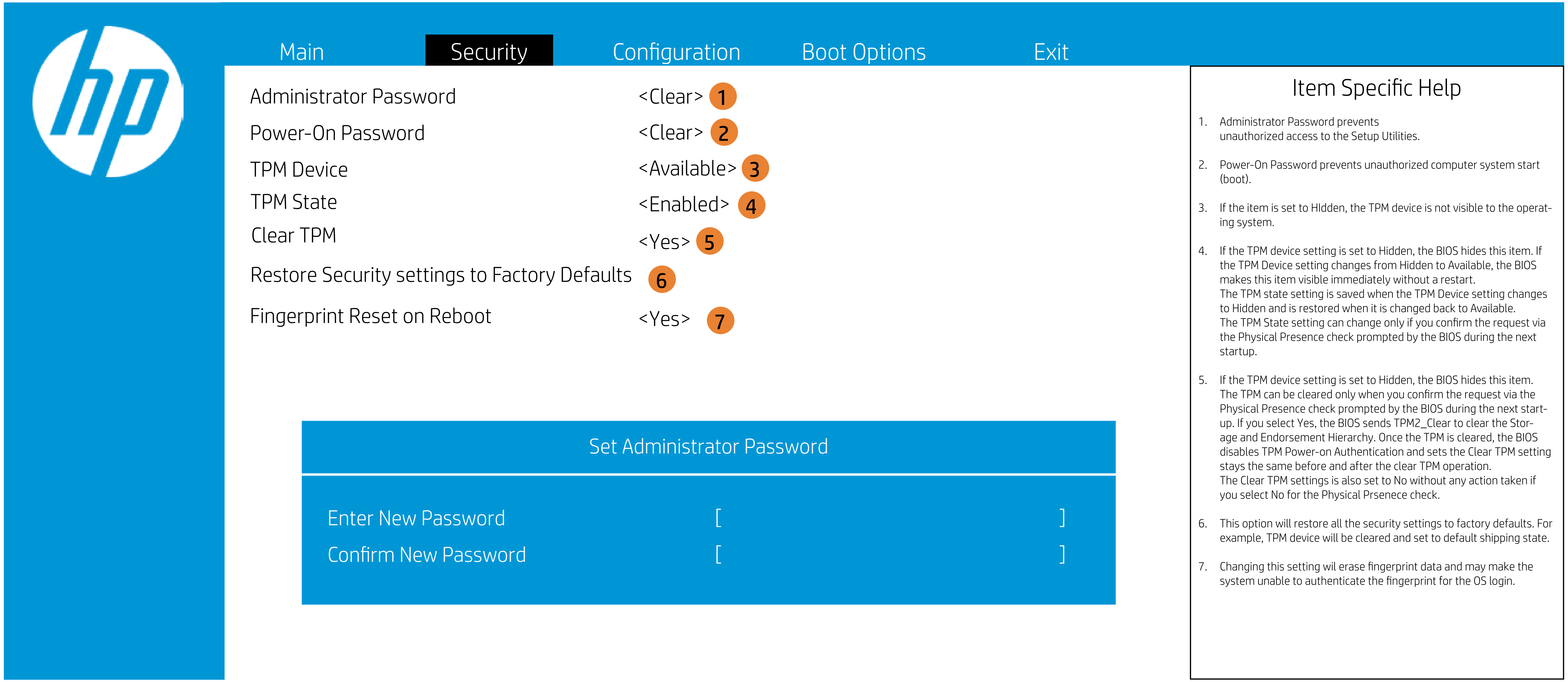
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password	<Clear>	1
Power-On Password	<Clear>	2
TPM Device	<Available>	3
TPM State	<Enabled>	4
Clear TPM	<Yes>	5
Restore Security settings to Factory Defaults		6
Fingerprint Reset on Reboot	<Yes>	7

Set Administrator Password

Enter New Password [ ]

Confirm New Password [ ]

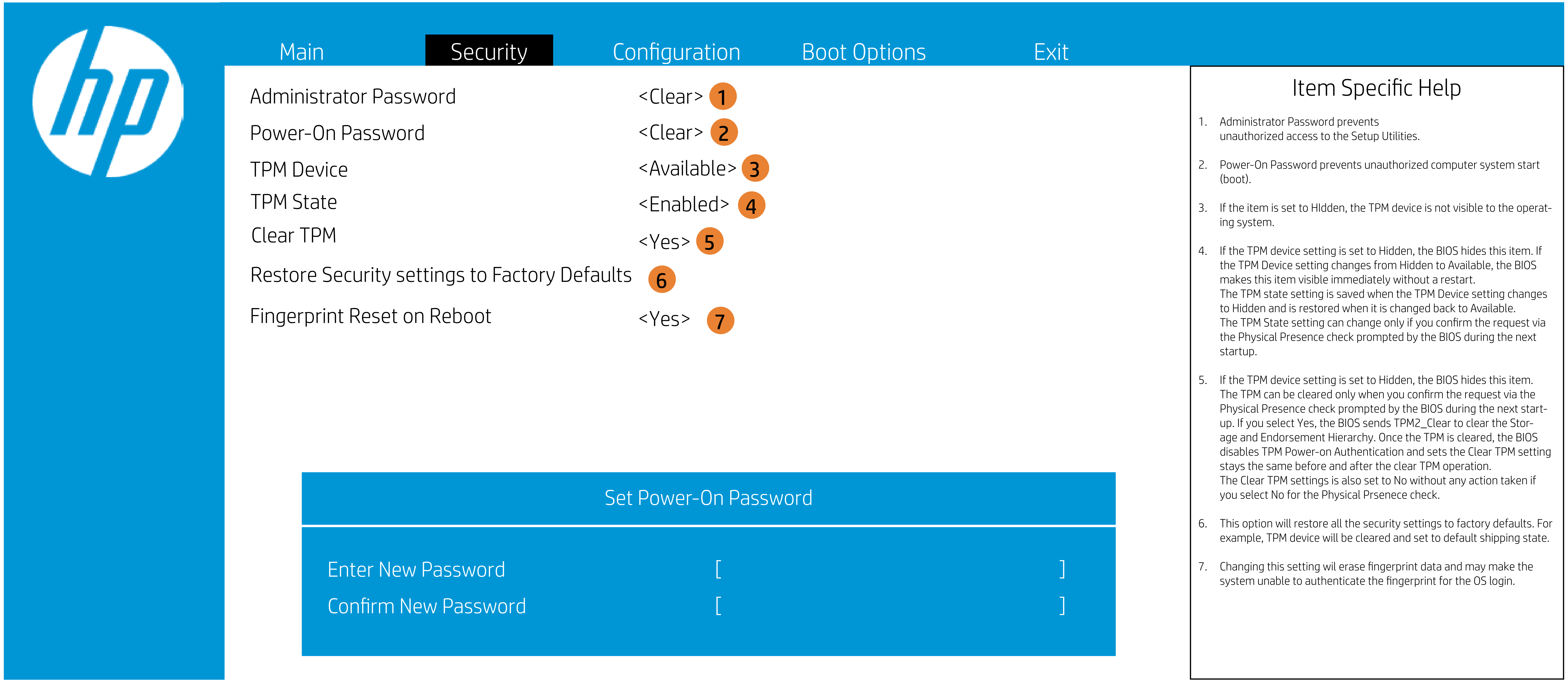
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <Yes> 5

Restore Security settings to Factory Defaults 6

Fingerprint Reset on Reboot <Yes> 7

Set Power-On Password

Enter New Password [ ]

Confirm New Password [ ]

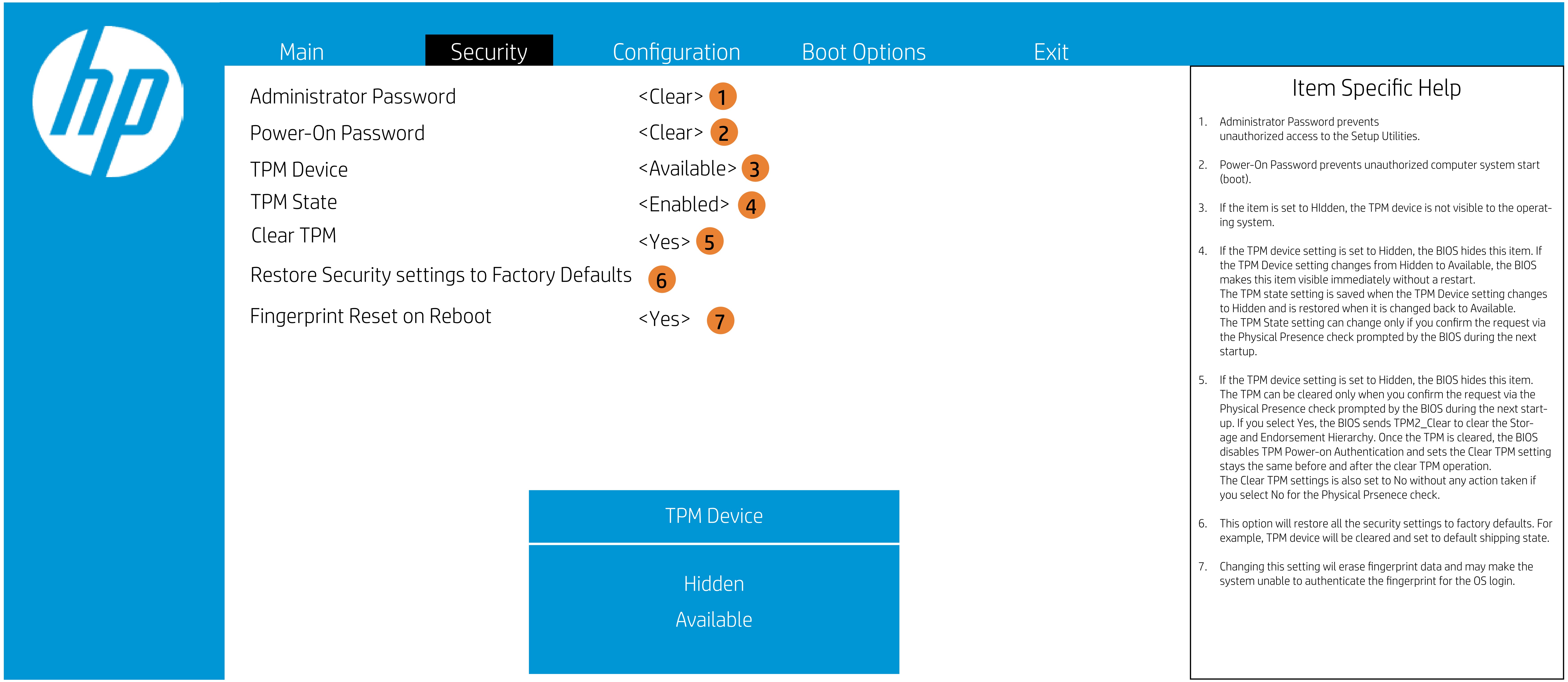
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <Yes> 5

Restore Security settings to Factory Defaults 6

Fingerprint Reset on Reboot <Yes> 7

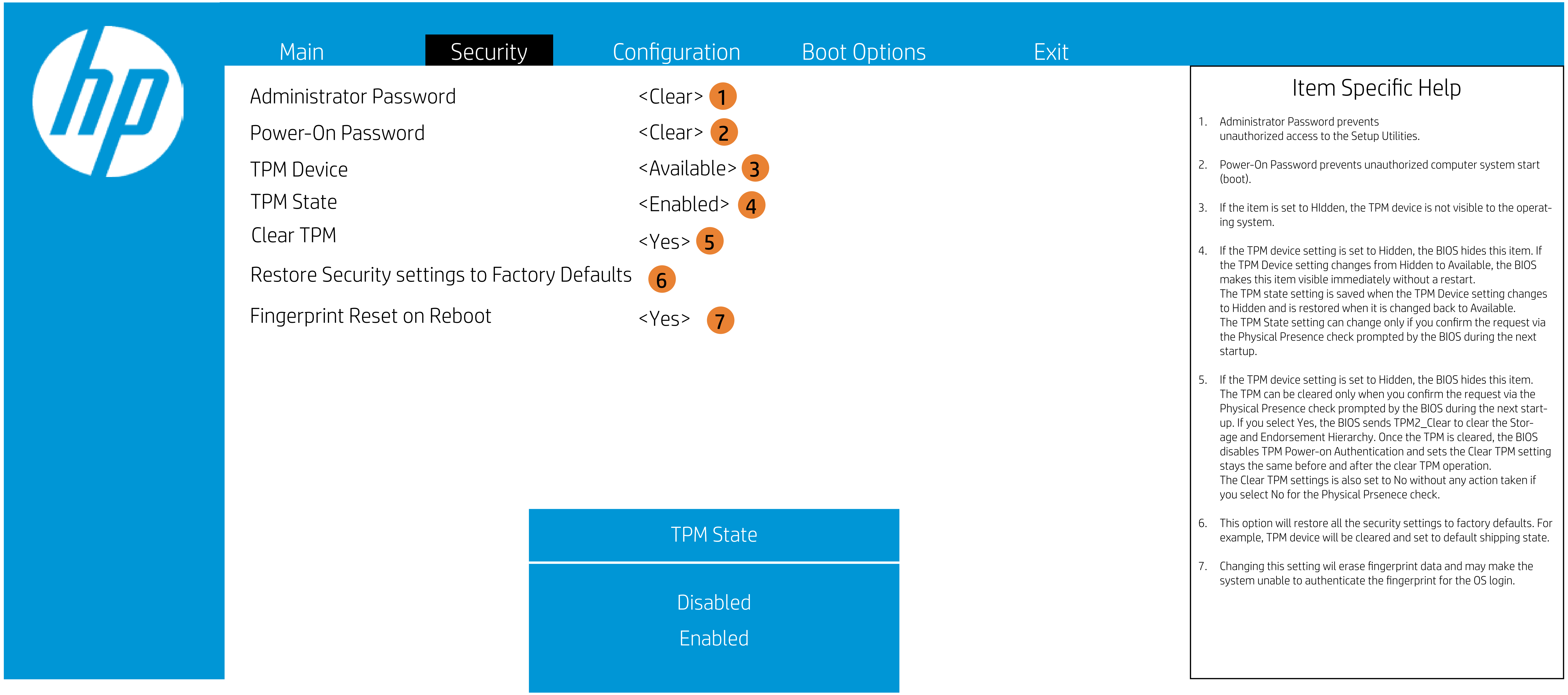
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <Yes> 5

Restore Security settings to Factory Defaults 6

Fingerprint Reset on Reboot <Yes> 7

TPM State

Disabled

Enabled

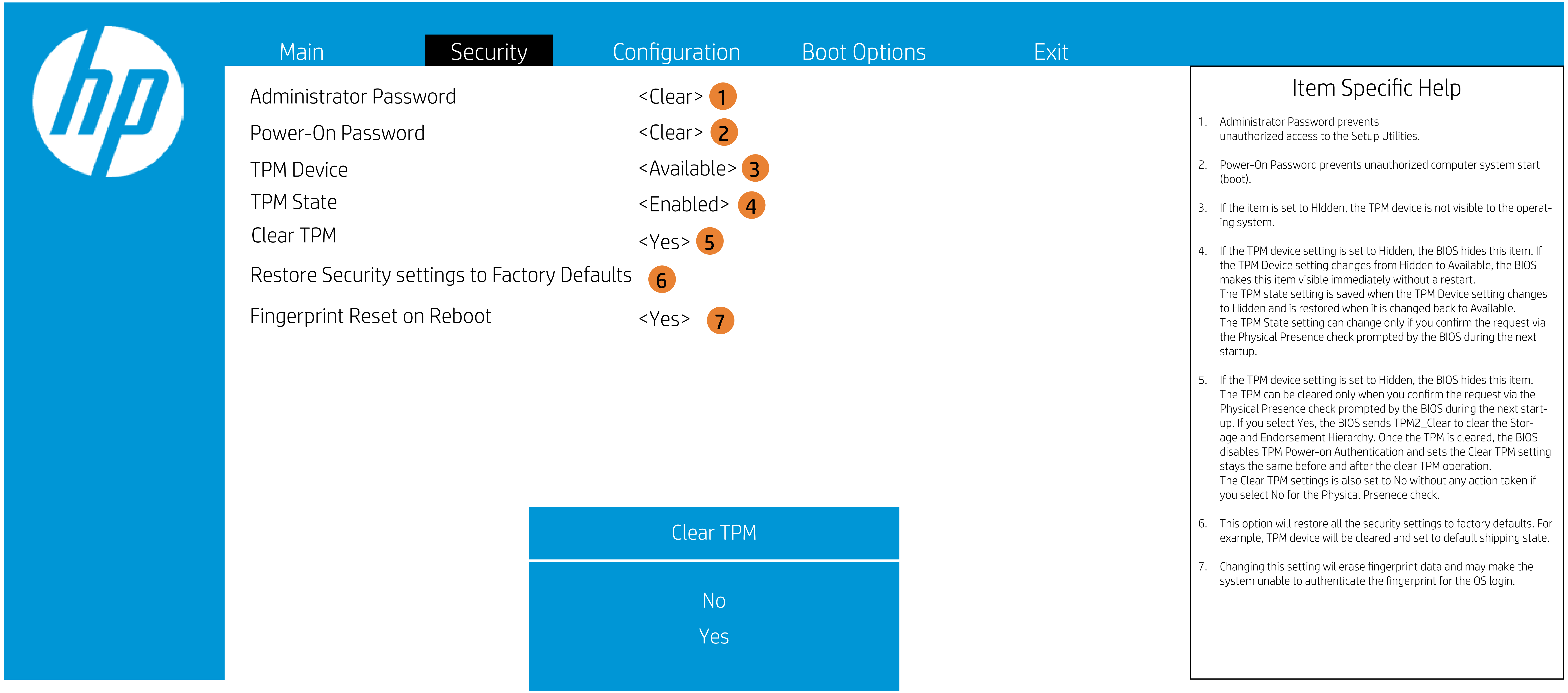
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password	<Clear>	1
Power-On Password	<Clear>	2
TPM Device	<Available>	3
TPM State	<Enabled>	4
Clear TPM	<Yes>	5
Restore Security settings to Factory Defaults		6
Fingerprint Reset on Reboot	<Yes>	7

Clear TPM

No

Yes

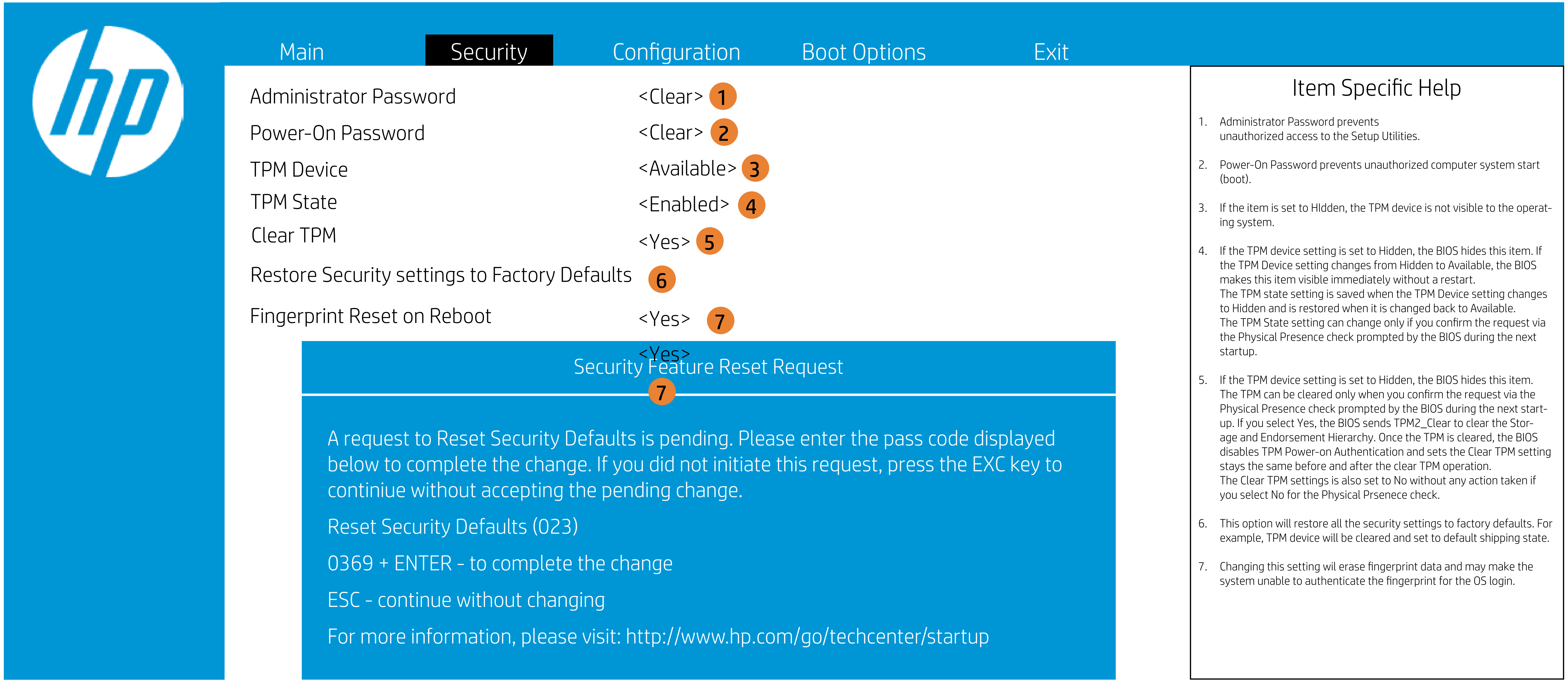
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to HIdden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart.
   The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available.
   The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next start-up. If you select Yes, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation.
   The Clear TPM settings is also set to No without any action taken if you select No for the Physical 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <Yes> 5

Restore Security settings to Factory Defaults 6

Fingerprint Reset on Reboot <Yes> 7

<Yes> 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

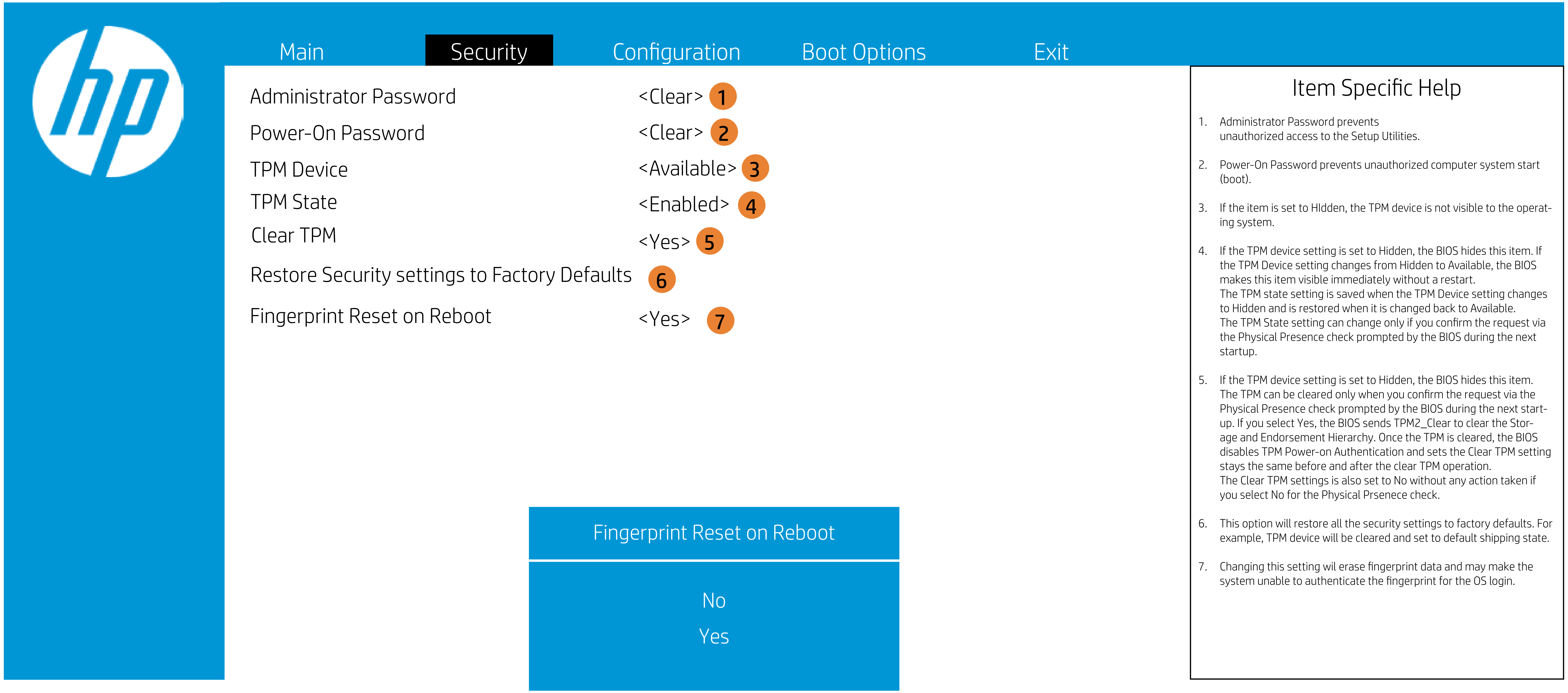
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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.
7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <Yes> 5

Restore Security settings to Factory Defaults 6

Fingerprint Reset on Reboot <Yes> 7

Fingerprint Reset on Reboot

No

Yes

Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.

2. Power-On Password prevents unauthorized computer system start (boot).

3. If the item is set to HIdden, the TPM device is not visible to the operating system.

4. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart.
   The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available.
   The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.

5. If the TPM device setting is set to Hidden, the BIOS hides this item.
   The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation.
   The Clear TPM settings is also set to No without any action taken if you select No for the Physical Prsenece check.

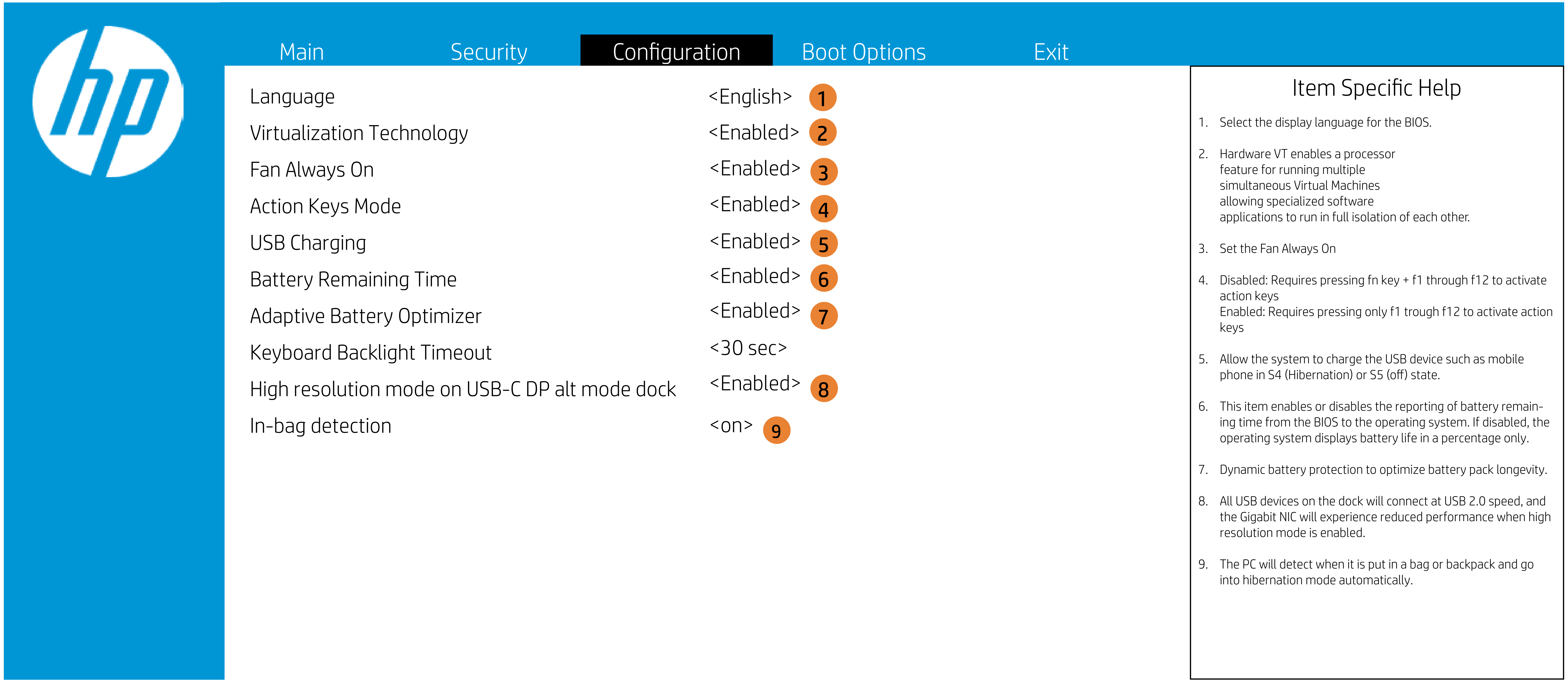
6. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

7. Changing this setting wil erase fingerprint data and may make the system unable to authenticate the fingerprint for the OS login.

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language	<English>	1
Virtualization Technology	<Enabled>	2
Fan Always On	<Enabled>	3
Action Keys Mode	<Enabled>	4
USB Charging	<Enabled>	5
Battery Remaining Time	<Enabled>	6
Adaptive Battery Optimizer	<Enabled>	7
Keyboard Backlight Timeout	<30 sec>	
High resolution mode on USB-C DP alt mode dock	<Enabled>	8
In-bag detection	<on>	9

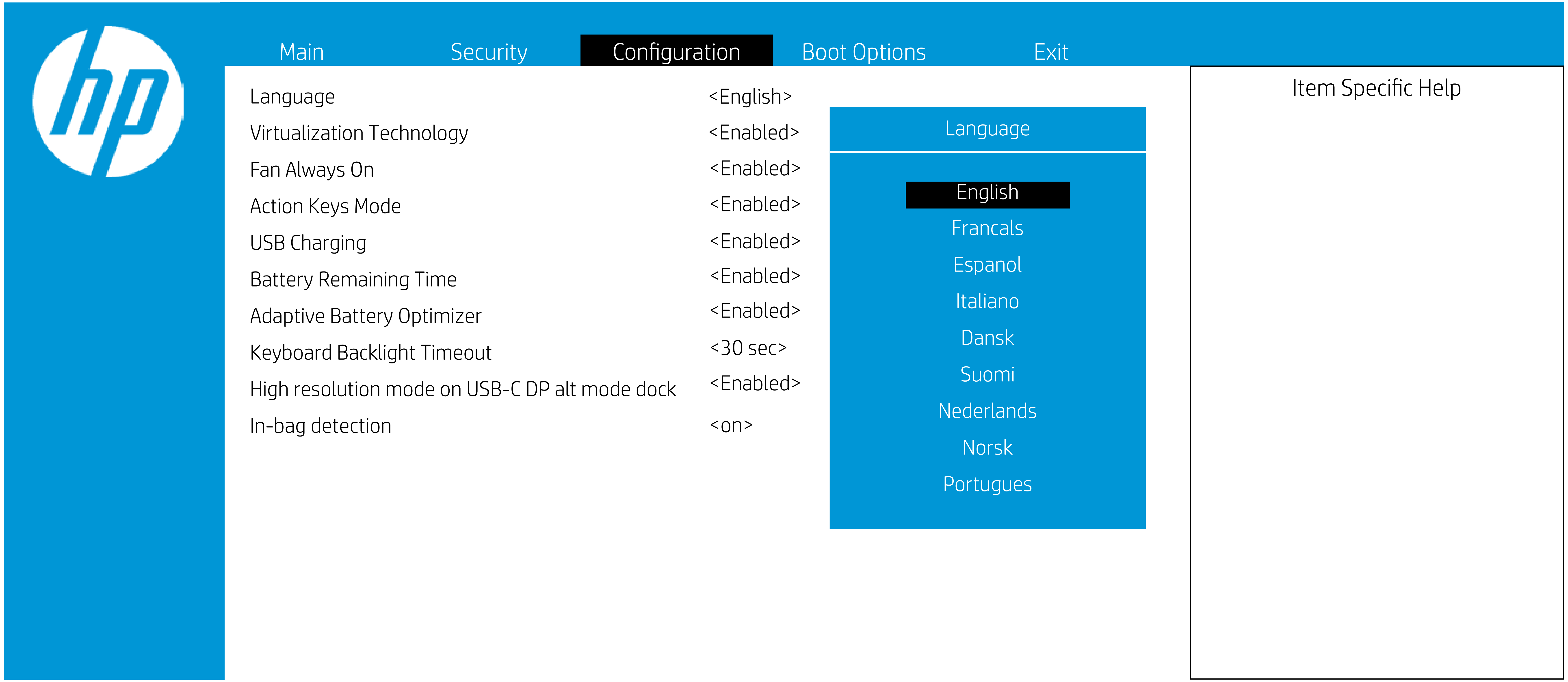
Item Specific Help

1. Select the display language for the BIOS.
2. Hardware VT enables a processor feature for running multiple simultaneous Virtual Machines allowing specialized software applications to run in full isolation of each other.
3. Set the Fan Always On
4. Disabled: Requires pressing fn key + f1 through f12 to activate action keys
   Enabled: Requires pressing only f1 trough 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. Dynamic battery protection to optimize battery pack longevity.
8. 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.
9. The PC will detect when it is put in a bag or backpack and go into hibernation mode automatically.

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

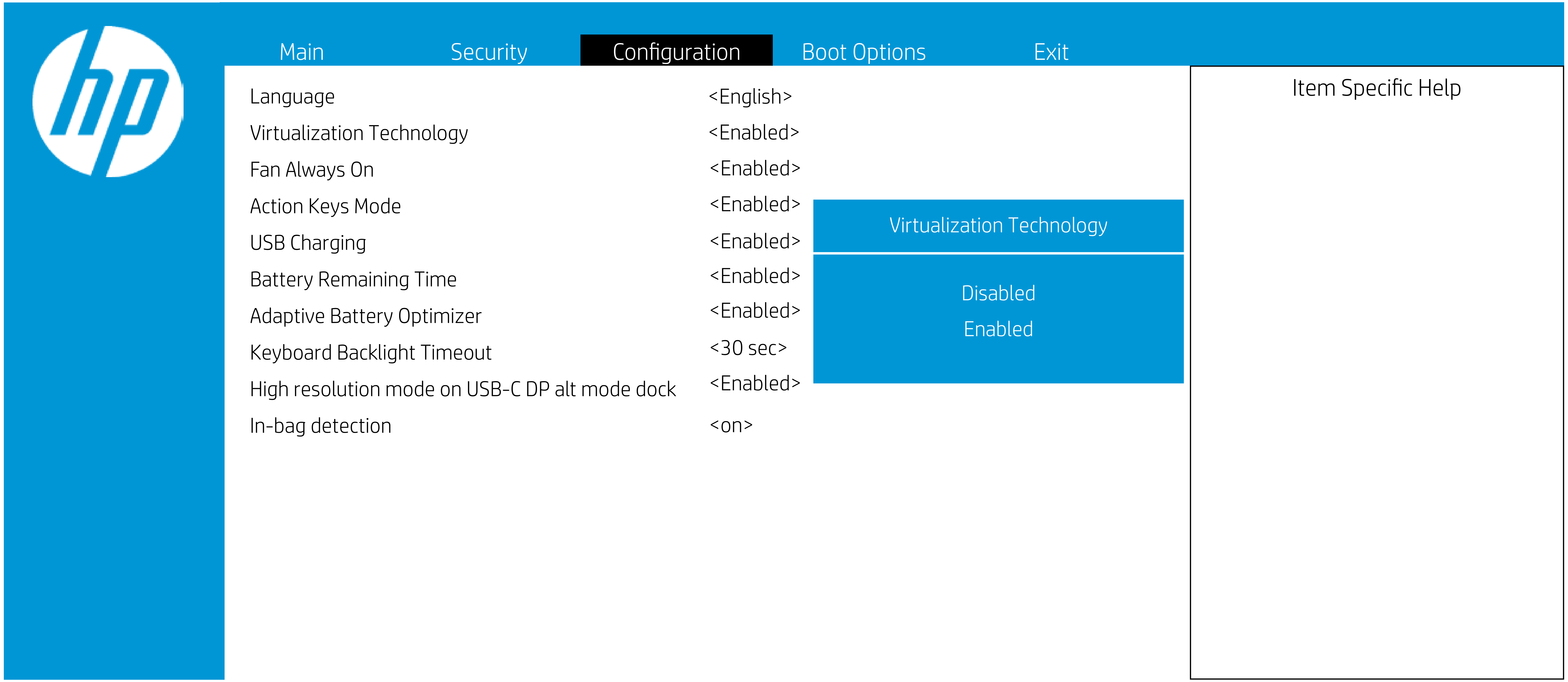


Language	<English>
Virtualization Technology	<Enabled>
Fan Always On	<Enabled>
Action Keys Mode	<Enabled>
USB Charging	<Enabled>
Battery Remaining Time	<Enabled>
Adaptive Battery Optimizer	<Enabled>
Keyboard Backlight Timeout	<30 sec>
High resolution mode on USB-C DP alt mode dock	<Enabled>
In-bag detection	<on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

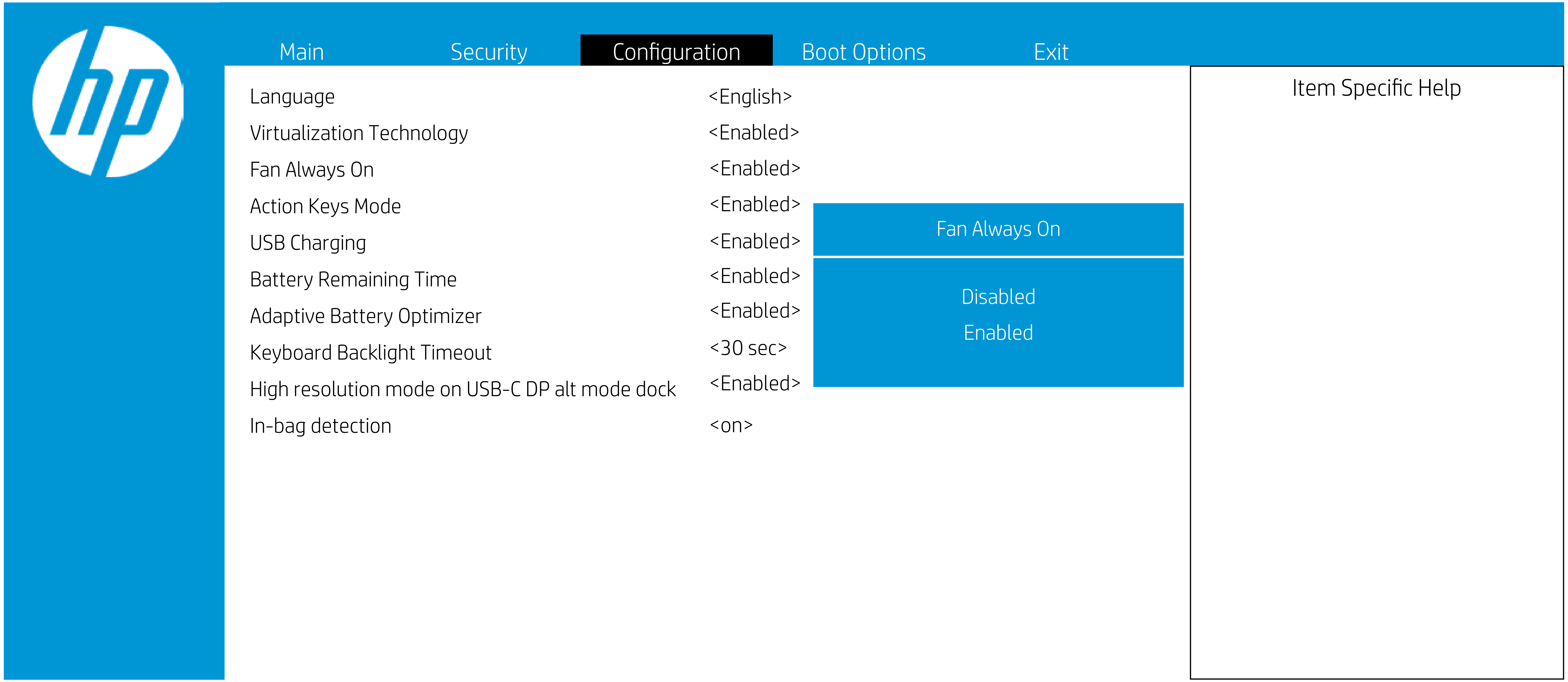


Language <English>
Virtualization Technology <Enabled>
Fan Always On <Enabled>
Action Keys Mode <Enabled>
USB Charging <Enabled>
Battery Remaining Time <Enabled>
Adaptive Battery Optimizer <Enabled>
Keyboard Backlight Timeout <30 sec>
High resolution mode on USB-C DP alt mode dock <Enabled>
In-bag detection <on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

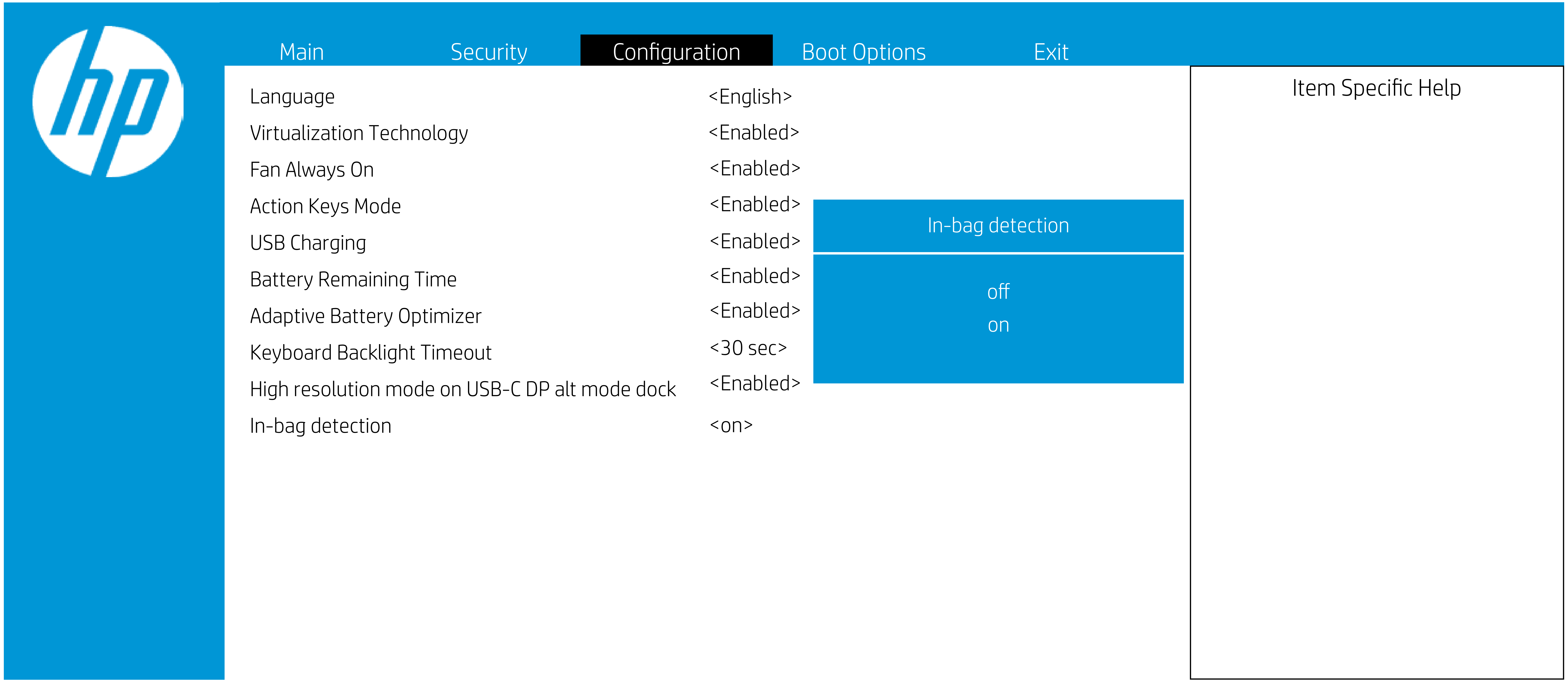


Language	<English>
Virtualization Technology	<Enabled>
Fan Always On	<Enabled>
Action Keys Mode	<Enabled>
USB Charging	<Enabled>
Battery Remaining Time	<Enabled>
Adaptive Battery Optimizer	<Enabled>
Keyboard Backlight Timeout	<30 sec>
High resolution mode on USB-C DP alt mode dock	<Enabled>
In-bag detection	<on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language	<English>
Virtualization Technology	<Enabled>
Fan Always On	<Enabled>
Action Keys Mode	<Enabled>
USB Charging	<Enabled>
Battery Remaining Time	<Enabled>
Adaptive Battery Optimizer	<Enabled>
Keyboard Backlight Timeout	<30 sec>
High resolution mode on USB-C DP alt mode dock	<Enabled>
In-bag detection	<on>

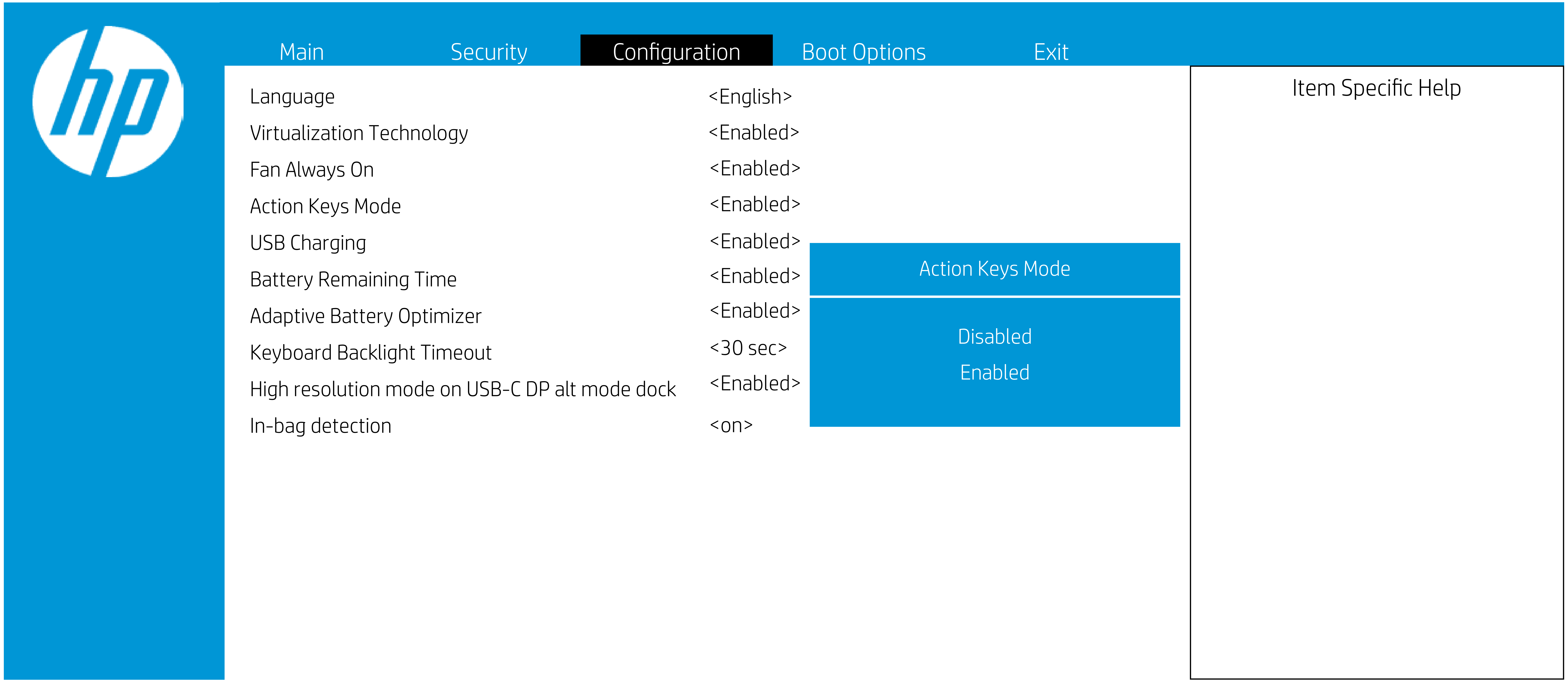
In-bag detection

off
on

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language <English>
Virtualization Technology <Enabled>
Fan Always On <Enabled>
Action Keys Mode <Enabled>
USB Charging <Enabled>
Battery Remaining Time <Enabled>
Adaptive Battery Optimizer <Enabled>
Keyboard Backlight Timeout <30 sec>
High resolution mode on USB-C DP alt mode dock <Enabled>
In-bag detection <on>

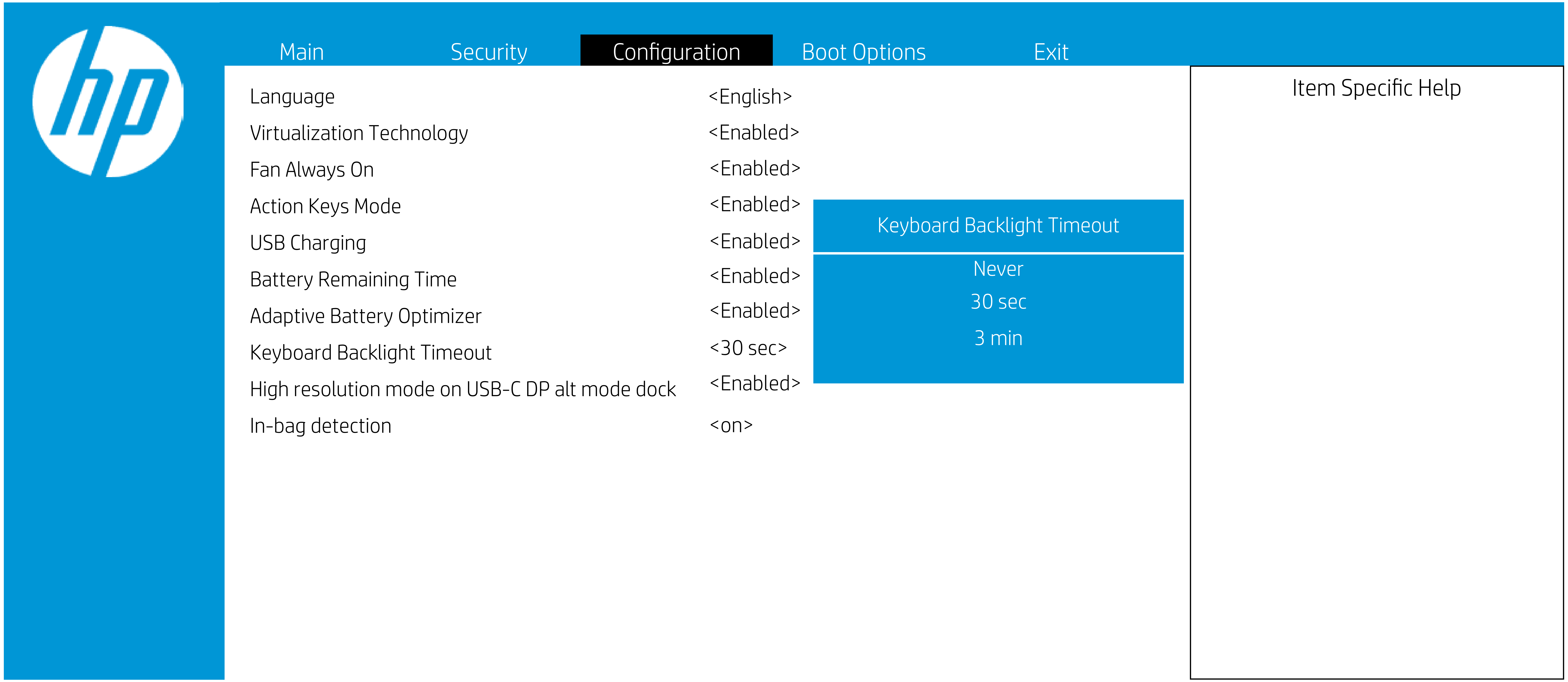
Action Keys Mode

Disabled
Enabled

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language <English>

Virtualization Technology <Enabled>

Fan Always On <Enabled>

Action Keys Mode <Enabled>

USB Charging <Enabled>

Battery Remaining Time <Enabled>

Adaptive Battery Optimizer <Enabled>

Keyboard Backlight Timeout <30 sec>

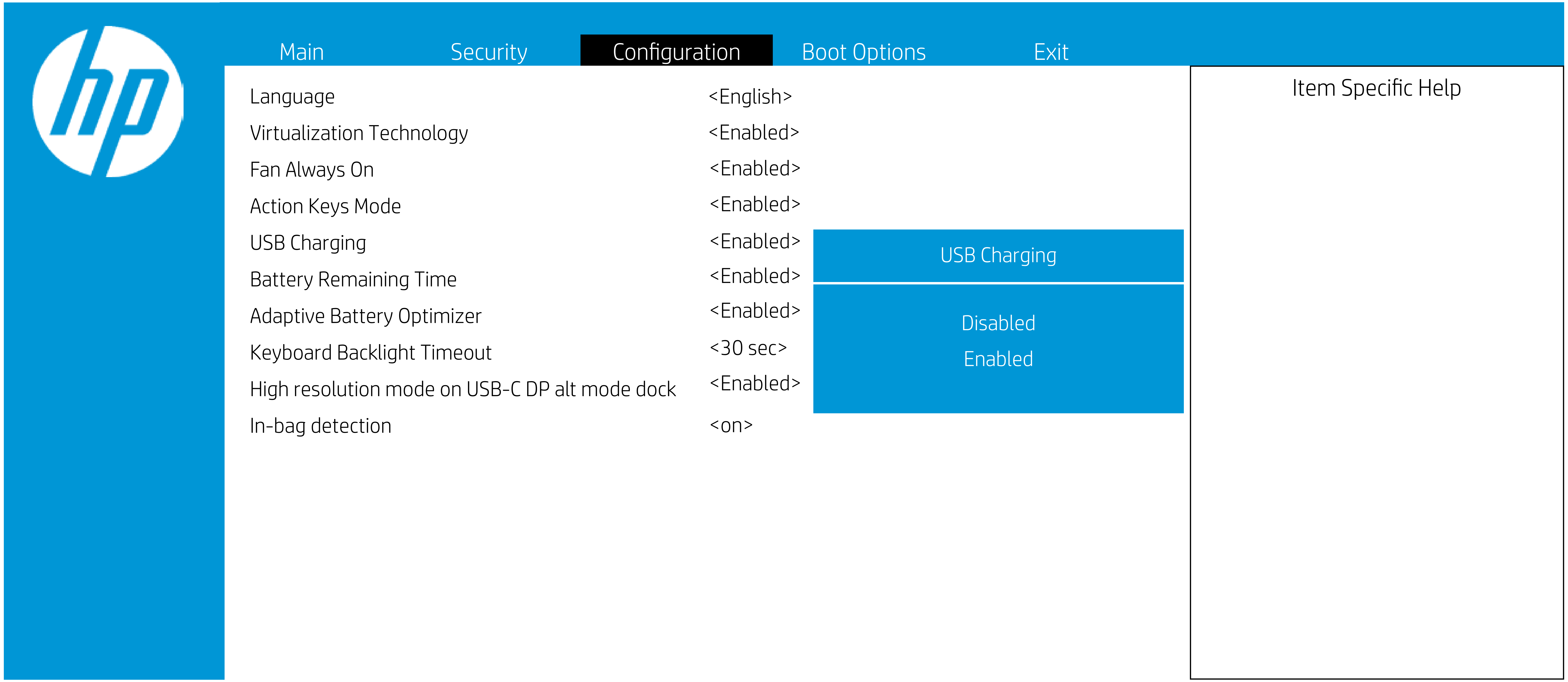
High resolution mode on USB-C DP alt mode dock <Enabled>

In-bag detection <on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



```
Language                                       <English>
Virtualization Technology                      <Enabled>
Fan Always On                                  <Enabled>
Action Keys Mode                               <Enabled>
USB Charging                                   <Enabled>
Battery Remaining Time                         <Enabled>
Adaptive Battery Optimizer                     <Enabled>
Keyboard Backlight Timeout                     <30 sec>
High resolution mode on USB-C DP alt mode dock <Enabled>
In-bag detection                               <on>
```

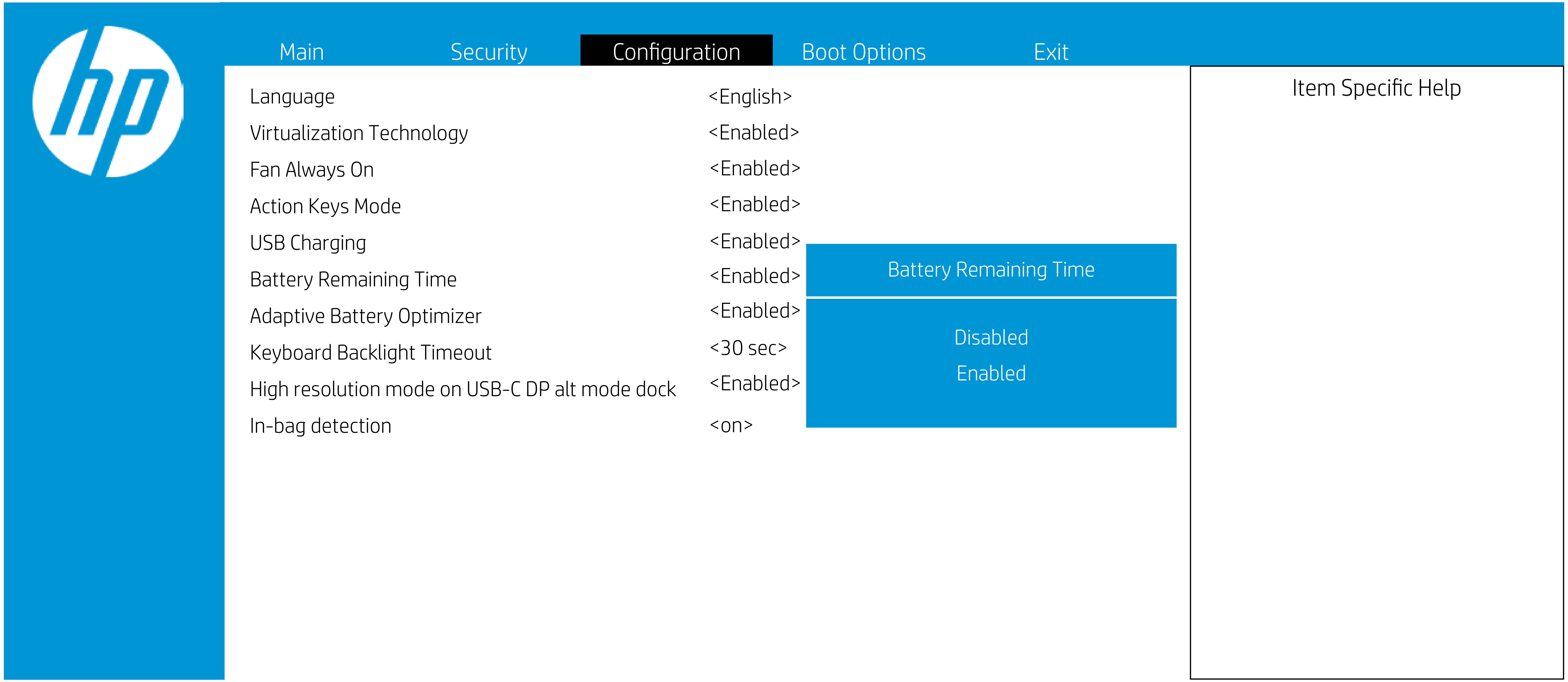
USB Charging

Disabled
Enabled

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

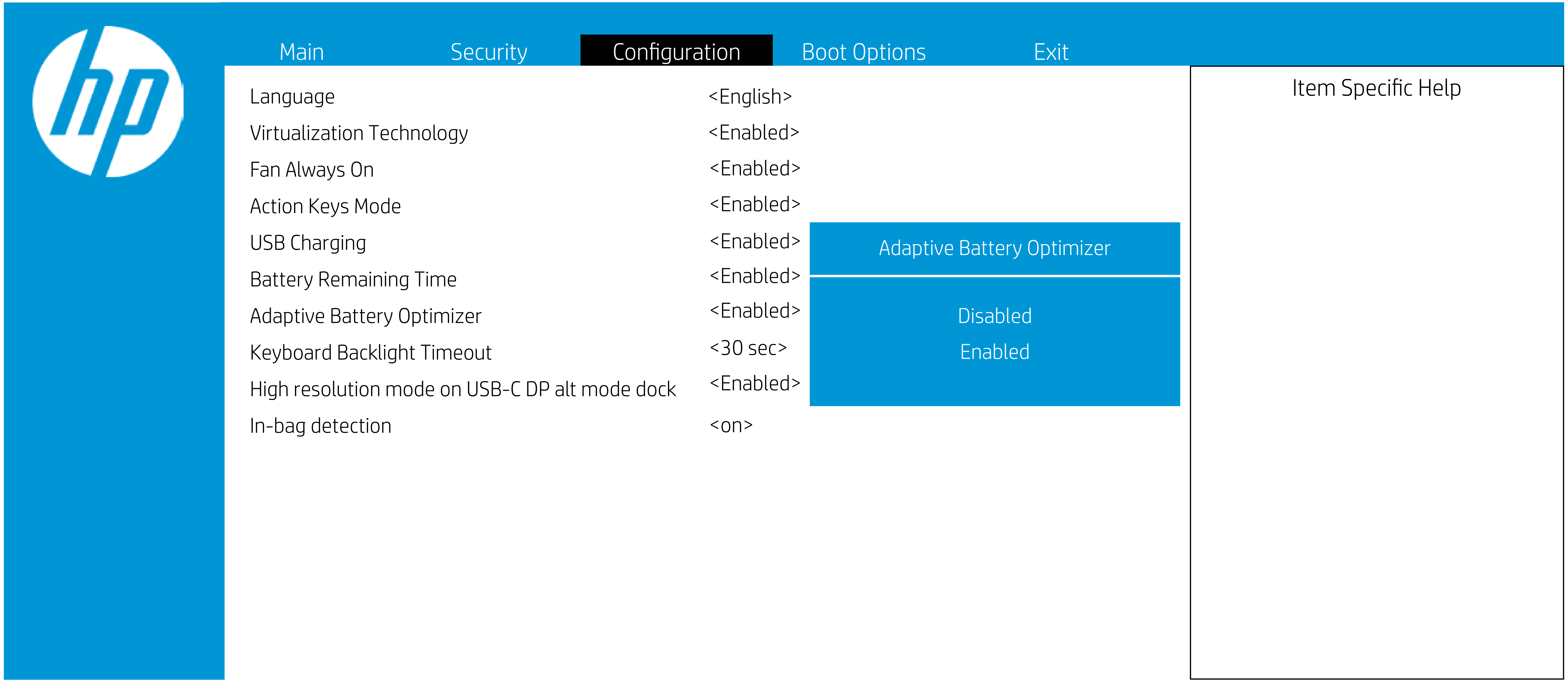


Language	<English>
Virtualization Technology	<Enabled>
Fan Always On	<Enabled>
Action Keys Mode	<Enabled>
USB Charging	<Enabled>
Battery Remaining Time	<Enabled>
Adaptive Battery Optimizer	<Enabled>
Keyboard Backlight Timeout	<30 sec>
High resolution mode on USB-C DP alt mode dock	<Enabled>
In-bag detection	<on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language <English>

Virtualization Technology <Enabled>

Fan Always On <Enabled>

Action Keys Mode <Enabled>

USB Charging <Enabled>

Battery Remaining Time <Enabled>

Adaptive Battery Optimizer <Enabled>

Keyboard Backlight Timeout <30 sec>

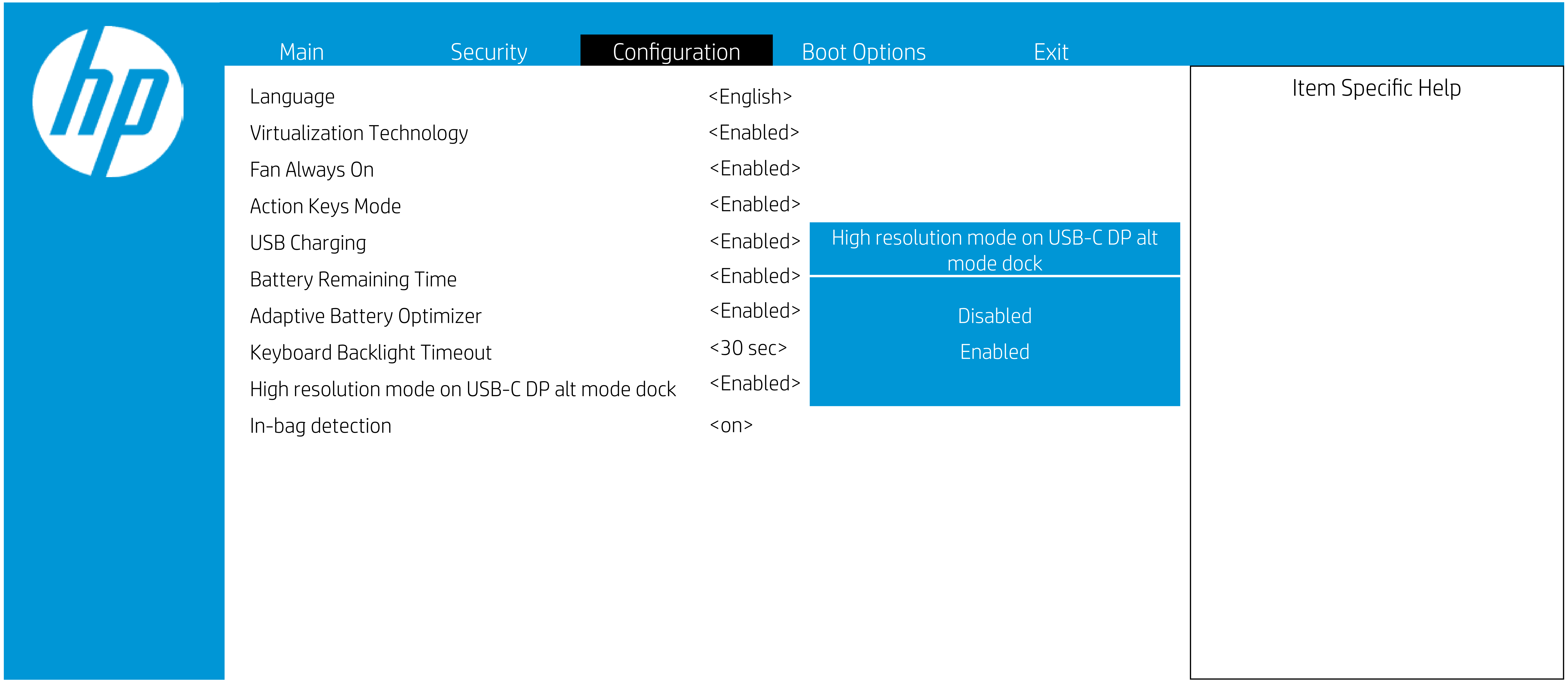
High resolution mode on USB-C DP alt mode dock <Enabled>

In-bag detection <on>

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

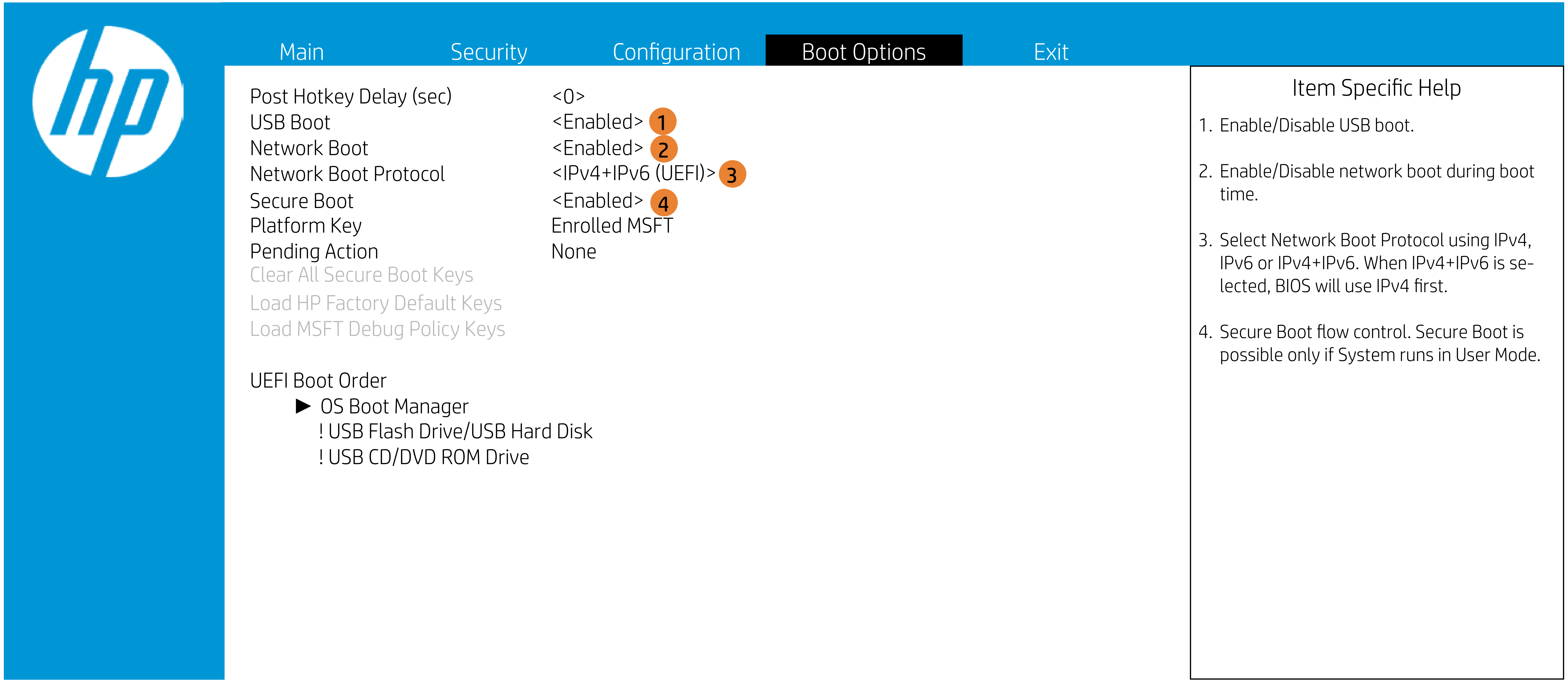


Language	<English>
Virtualization Technology	<Enabled>
Fan Always On	<Enabled>
Action Keys Mode	<Enabled>
USB Charging	<Enabled>
Battery Remaining Time	<Enabled>
Adaptive Battery Optimizer	<Enabled>
Keyboard Backlight Timeout	<30 sec>
High resolution mode on USB-C DP alt mode dock	<Enabled>
In-bag detection	<on>

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec) <0>
USB Boot <Enabled> 1
Network Boot <Enabled> 2
Network Boot Protocol <IPv4+IPv6 (UEFI)> 3
Secure Boot <Enabled> 4
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
! USB Flash Drive/USB Hard Disk
! USB CD/DVD ROM Drive

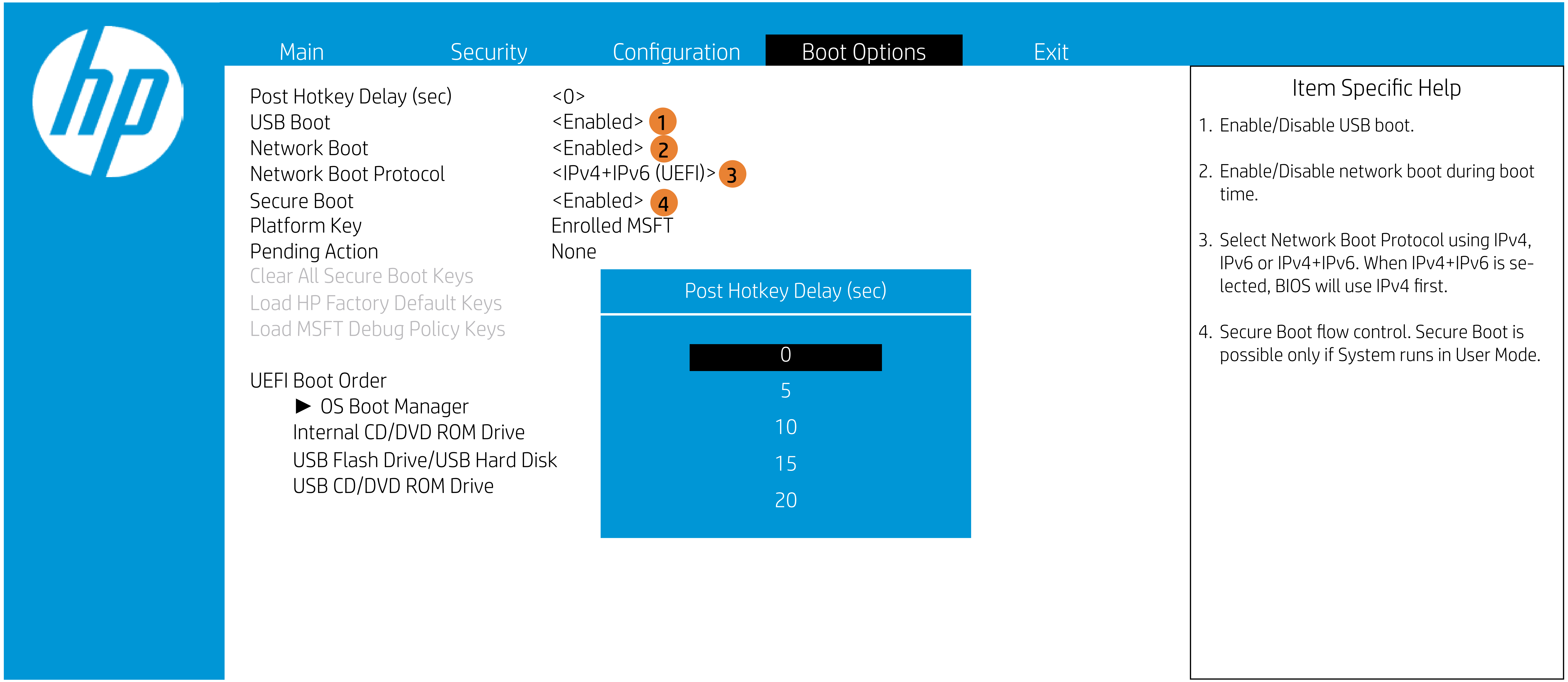
Item Specific Help

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. 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



```
Post Hotkey Delay (sec)      <0>
USB Boot                     <Enabled> 1
Network Boot                 <Enabled> 2
Network Boot Protocol        <IPv4+IPv6 (UEFI)> 3
Secure Boot                  <Enabled> 4
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
```

Post Hotkey Delay (sec)

0
5
10
15
20

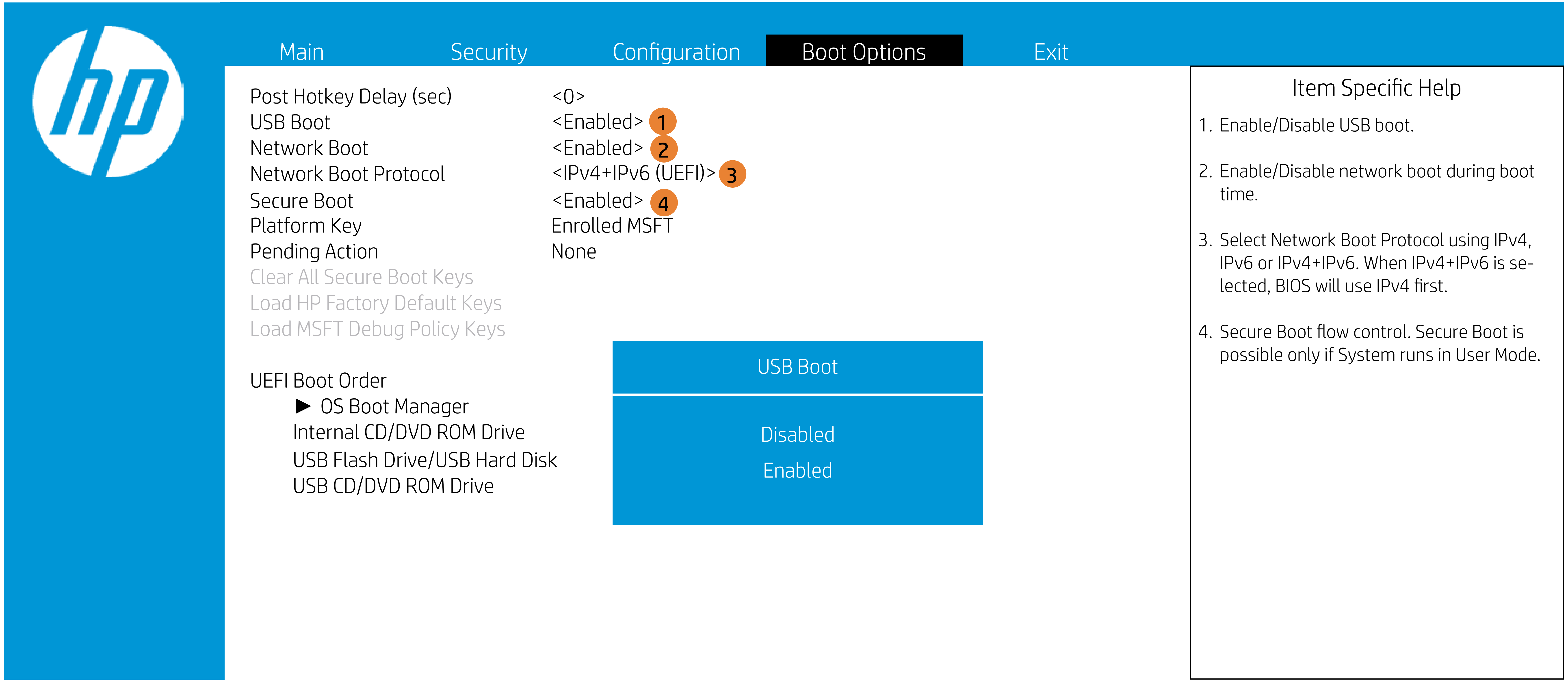
Item Specific Help

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. 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



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Secure Boot	<Enabled> 4
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

USB Boot

Disabled

Enabled

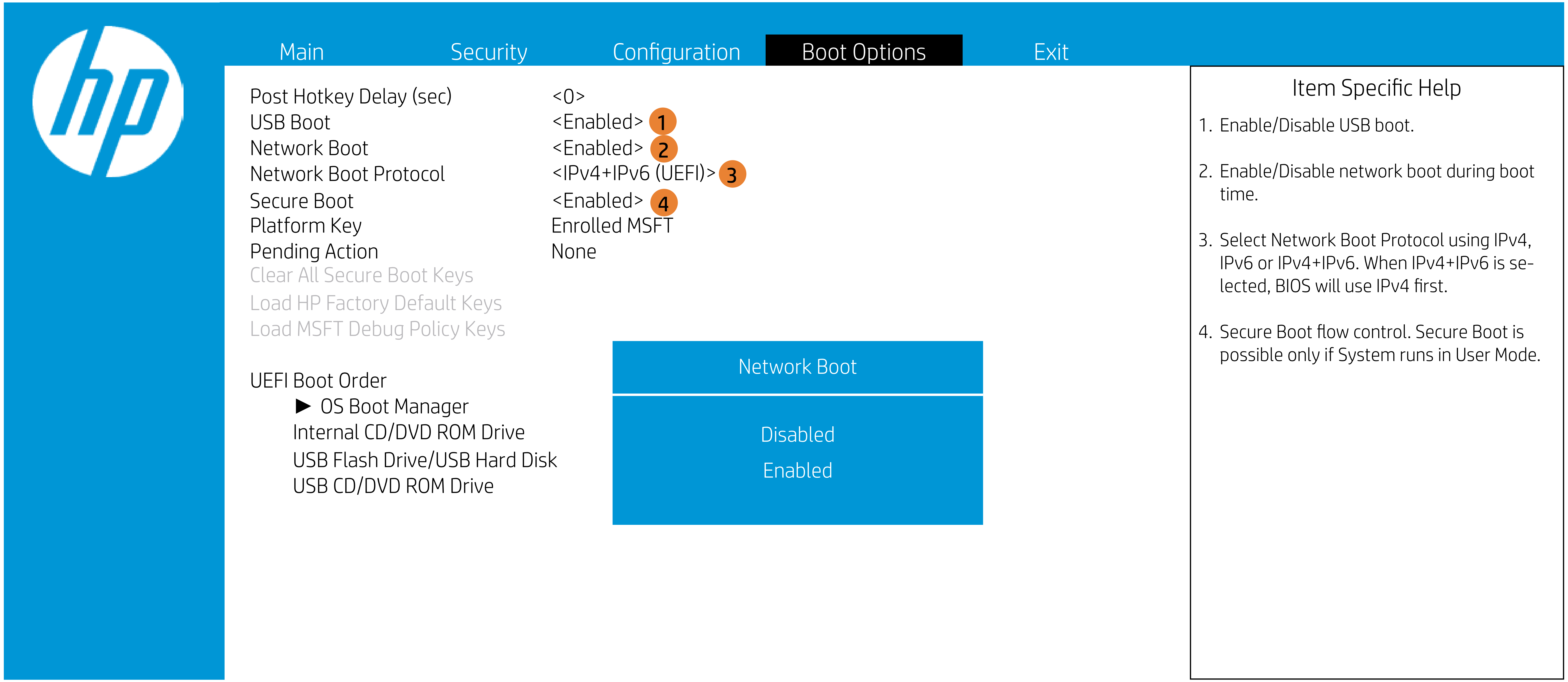
Item Specific Help

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. 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



Post Hotkey Delay (sec) <0>
USB Boot <Enabled> 1
Network Boot <Enabled> 2
Network Boot Protocol <IPv4+IPv6 (UEFI)> 3
Secure Boot <Enabled> 4
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

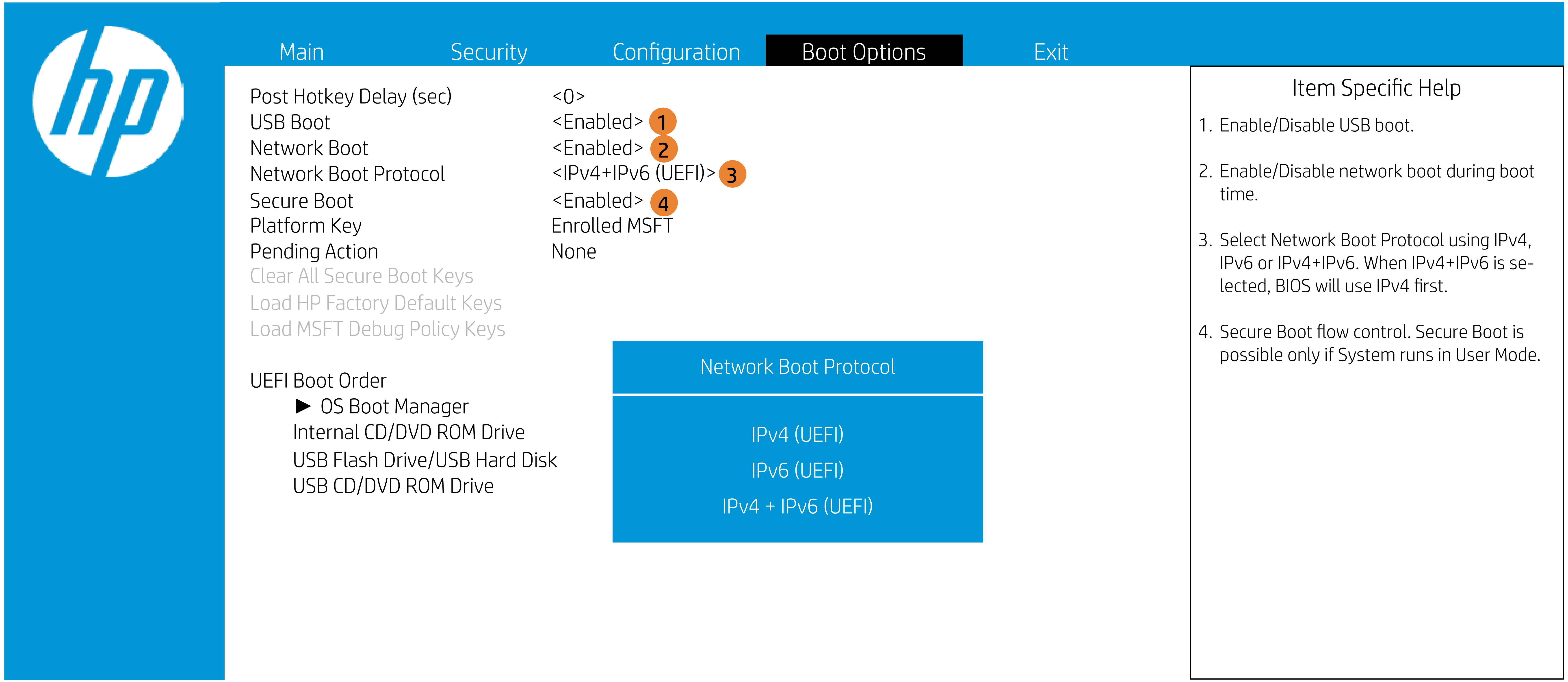
Item Specific Help

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

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Secure Boot	<Enabled> 4
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

Network Boot Protocol

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

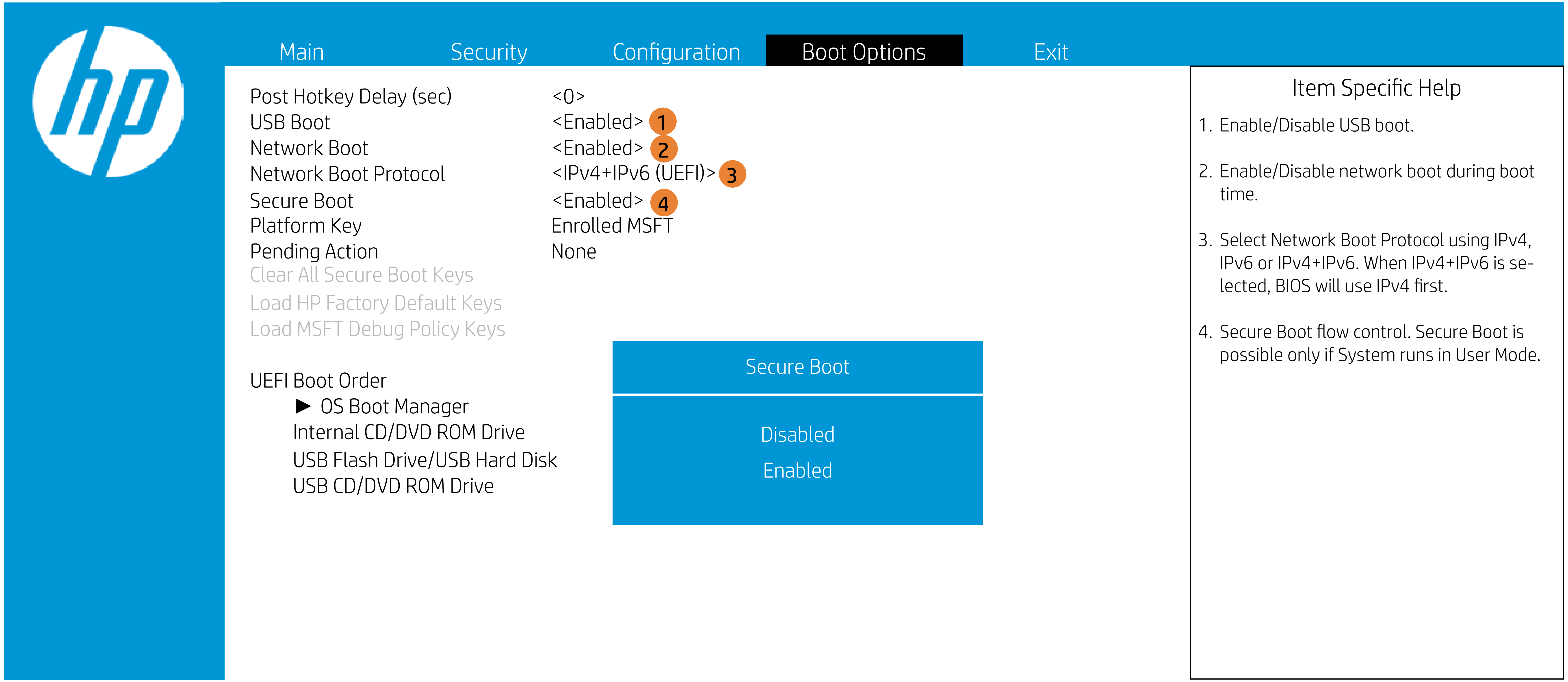
Item Specific Help

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. 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



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Enabled> 2
Network Boot Protocol	<IPv4+IPv6 (UEFI)> 3
Secure Boot	<Enabled> 4
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

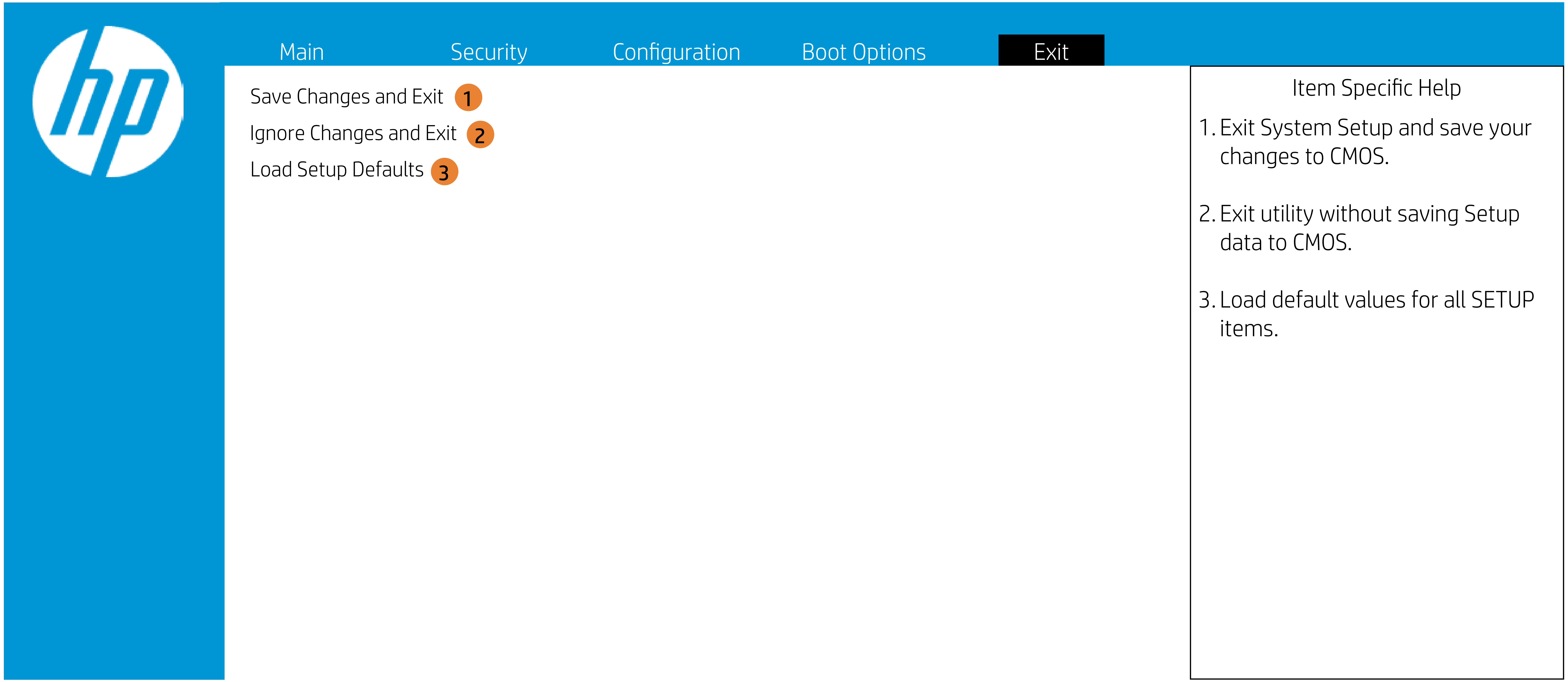
Item Specific Help

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

Back to Welcome Page

Exit Menu

Back to BIOS Utility Menus



Item Specific Help

1. Exit System Setup and save your changes to CMOS.

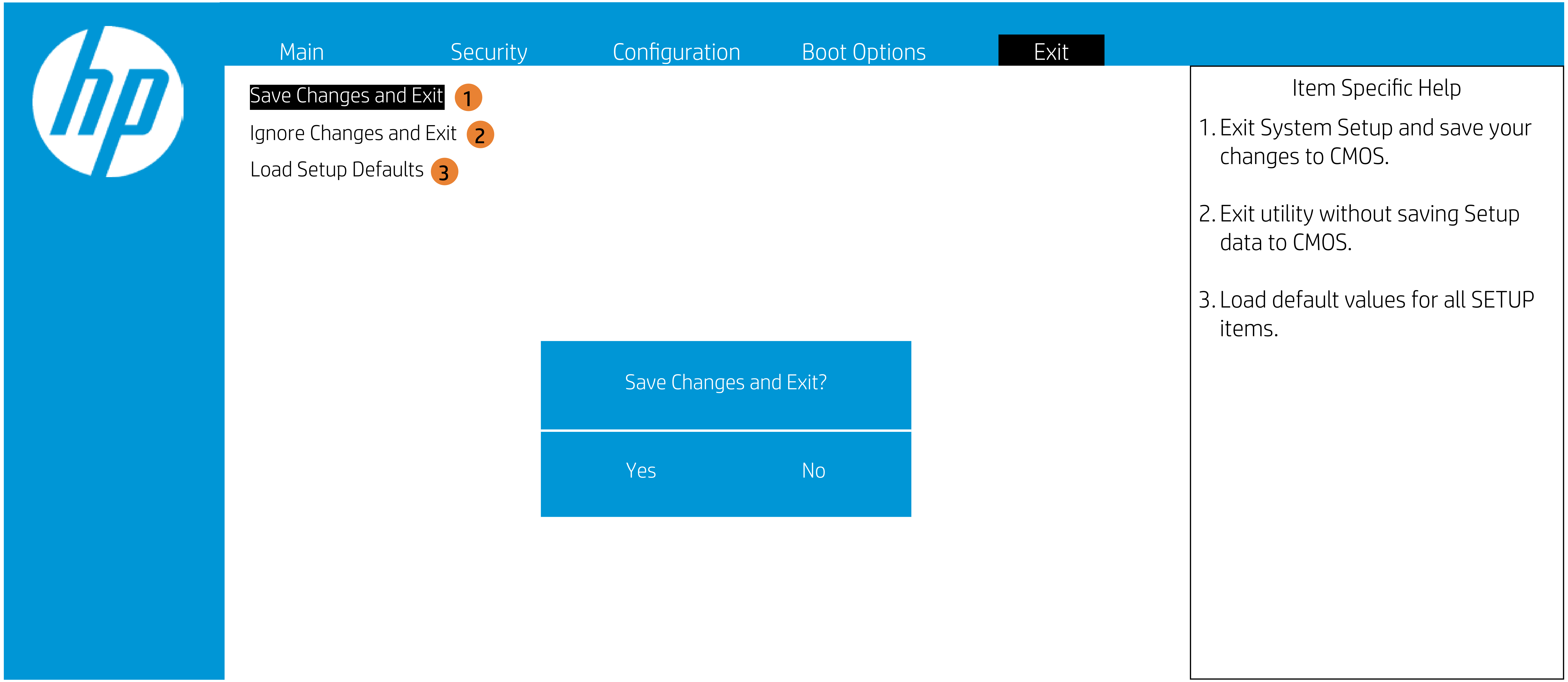
2. Exit utility without saving Setup data to CMOS.

3. Load default values for all SETUP items.

Back to Welcome Page

Exit Menu

Back to BIOS Utility Menus



Save Changes and Exit?

Item Specific Help

1. Exit System Setup and save your changes to CMOS.

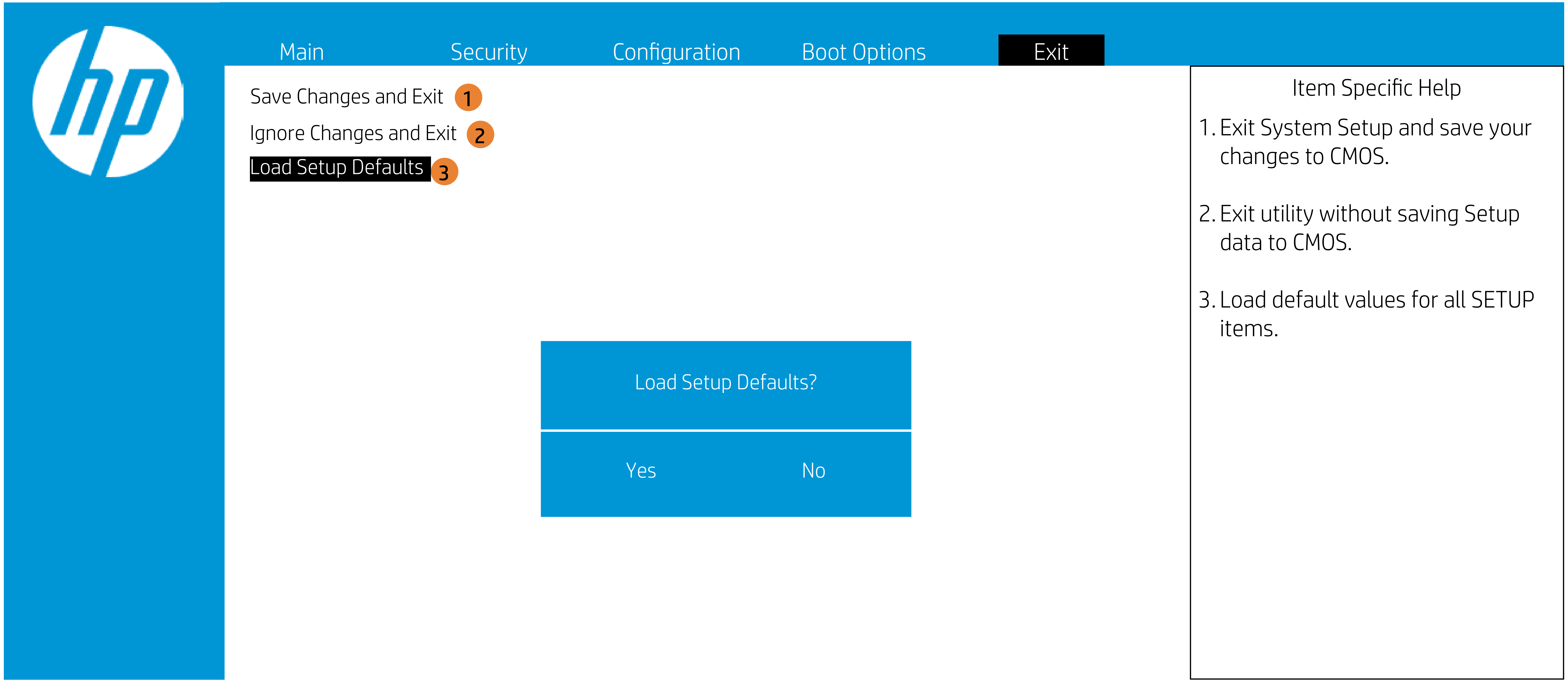
2. Exit utility without saving Setup data to CMOS.

3. Load default values for all SETUP items.

Back to Welcome Page

Exit Menu

Back to BIOS Utility Menus



Save Changes and Exit 1

Ignore Changes and Exit 2

Load Setup Defaults 3

Load Setup Defaults?

Yes No

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.

Back to Welcome Page