Interactive BIOS simulator

HP ENVY 34in AiO Desktop PC

Welcome to the interactive BIOS simulator for the
HP ENVY 34in AiO Desktop 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.

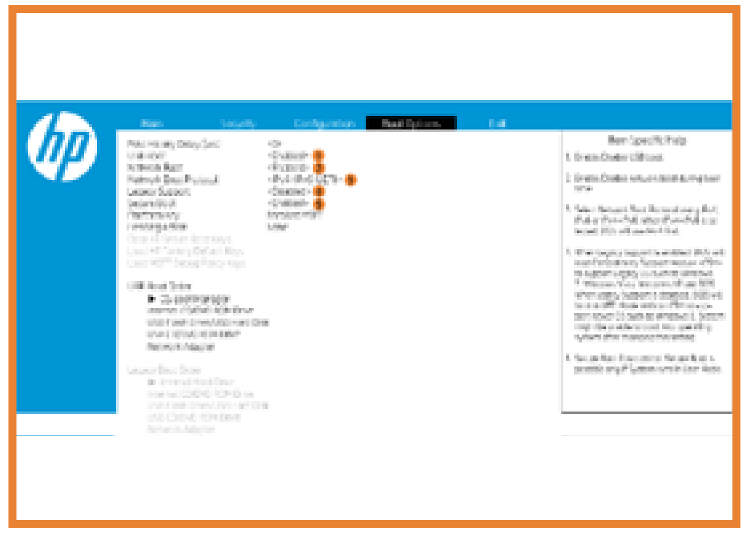
BIOS Utility Menus

Back to Welcome Page

Main

Security

Configuration

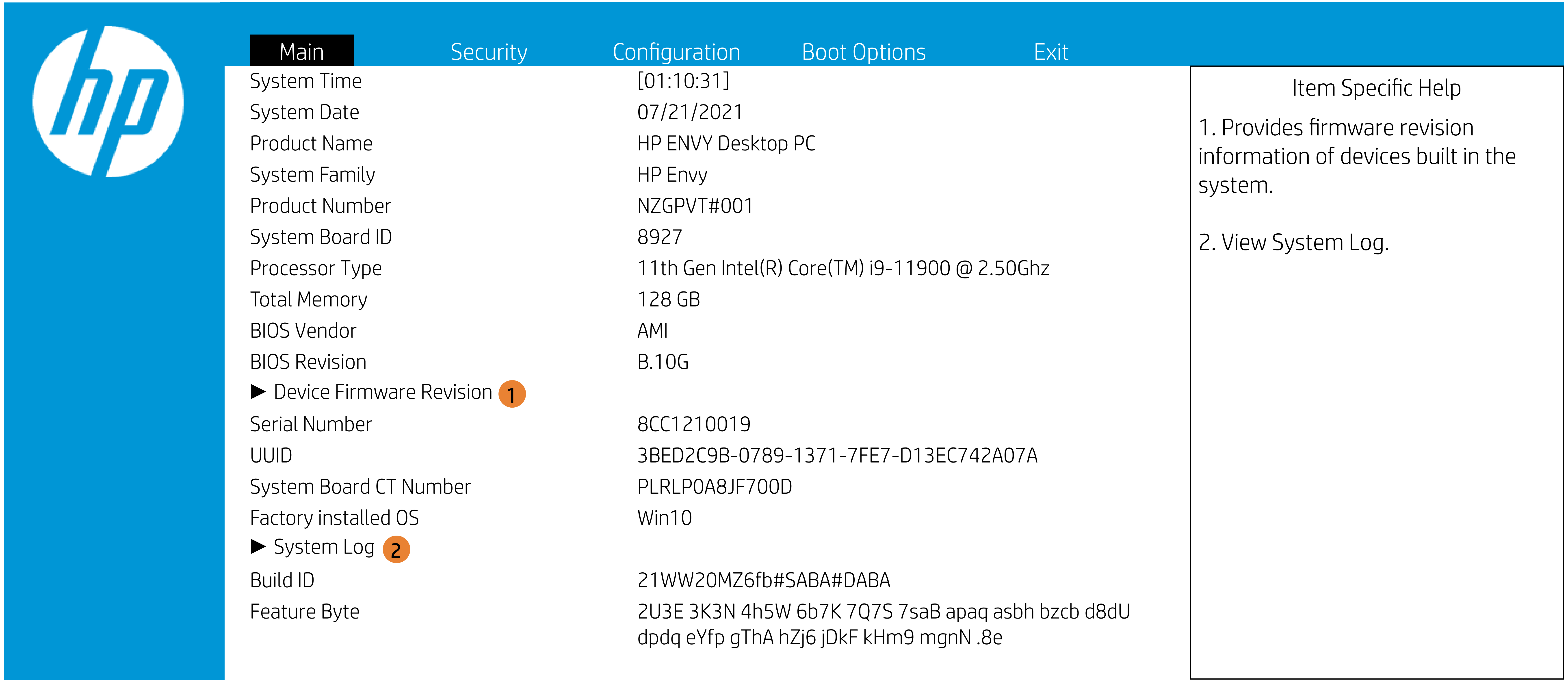


Boot Options

Exit

Main Menu

Back to BIOS Utility Menus



System Time	[01:10:31]
System Date	07/21/2021
Product Name	HP ENVY Desktop PC
System Family	HP Envy
Product Number	NZGPVT#001
System Board ID	8927
Processor Type	11th Gen Intel(R) Core(TM) i9-11900 @ 2.50Ghz
Total Memory	128 GB
BIOS Vendor	AMI
BIOS Revision	B.10G
▶ Device Firmware Revision 1	
Serial Number	8CC1210019
UUID	3BED2C9B-0789-1371-7FE7-D13EC742A07A
System Board CT Number	PLRLP0A8JF700D
Factory installed OS	Win10
▶ System Log 2	
Build ID	21WW20MZ6fb#SABA#DABA
Feature Byte	2U3E 3K3N 4h5W 6b7K 7Q7S 7saB apaq asbh bzcb d8dU dpdq eYfp gThA hZj6 jDkF kHm9 mgnN .8e

Item Specific Help

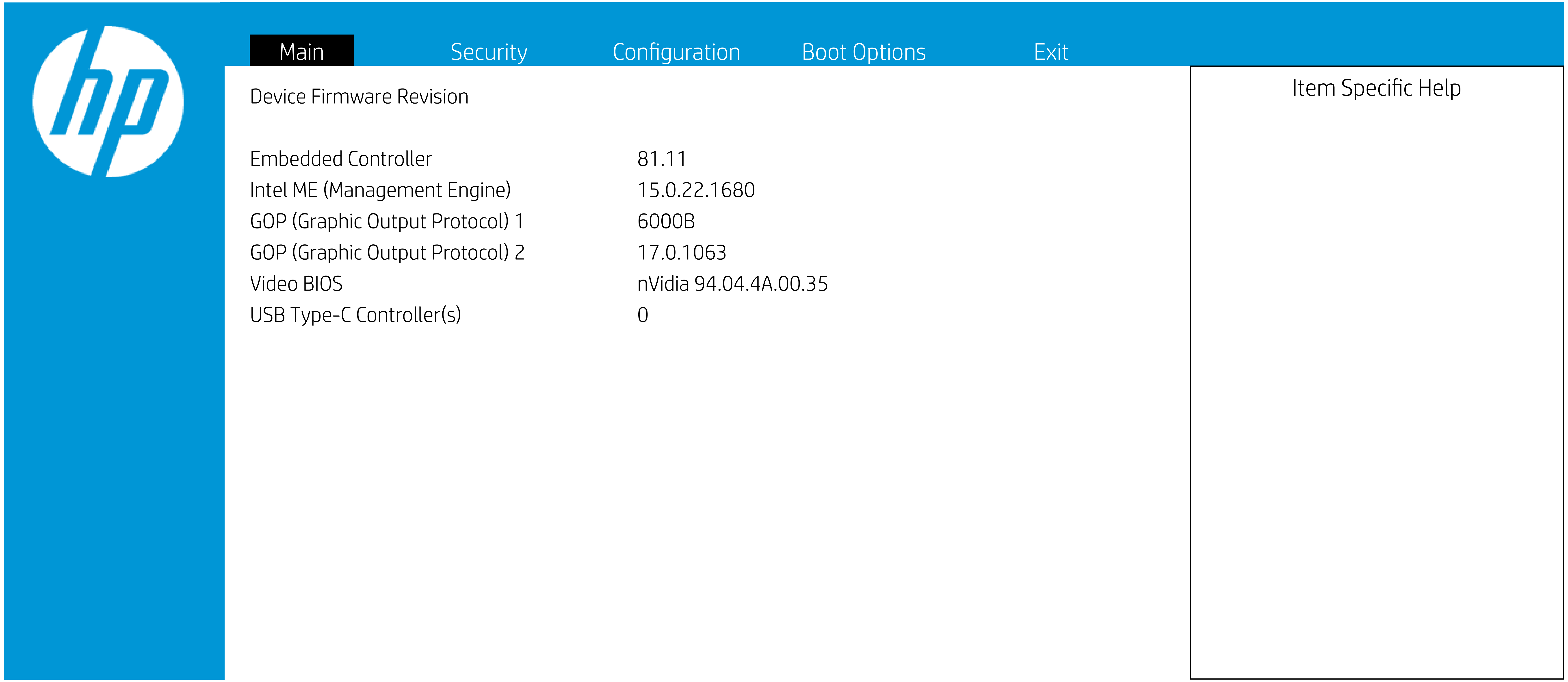
1. Provides firmware revision information of devices built in the system.

2. View System Log.

Back to Welcome Page

Main Menu

Back to BIOS Utility Menus



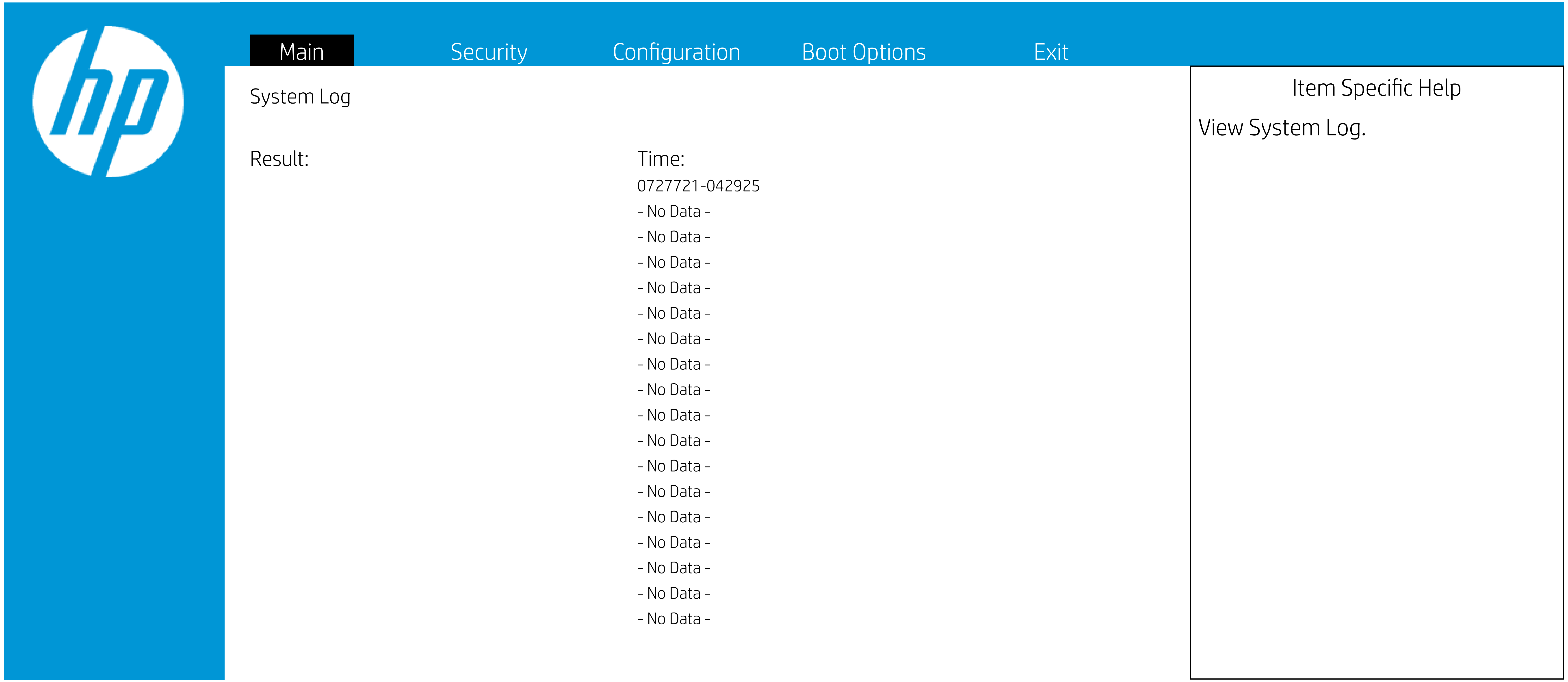
Device Firmware Revision

Embedded Controller	81.11
Intel ME (Management Engine)	15.0.22.1680
GOP (Graphic Output Protocol) 1	6000B
GOP (Graphic Output Protocol) 2	17.0.1063
Video BIOS	nVidia 94.04.4A.00.35
USB Type-C Controller(s)	0

Back to Welcome Page

Main Menu

Back to BIOS Utility Menus



System Log

```
Result:                                   Time:
                                          0727721-042925
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
                                          - No Data -
```

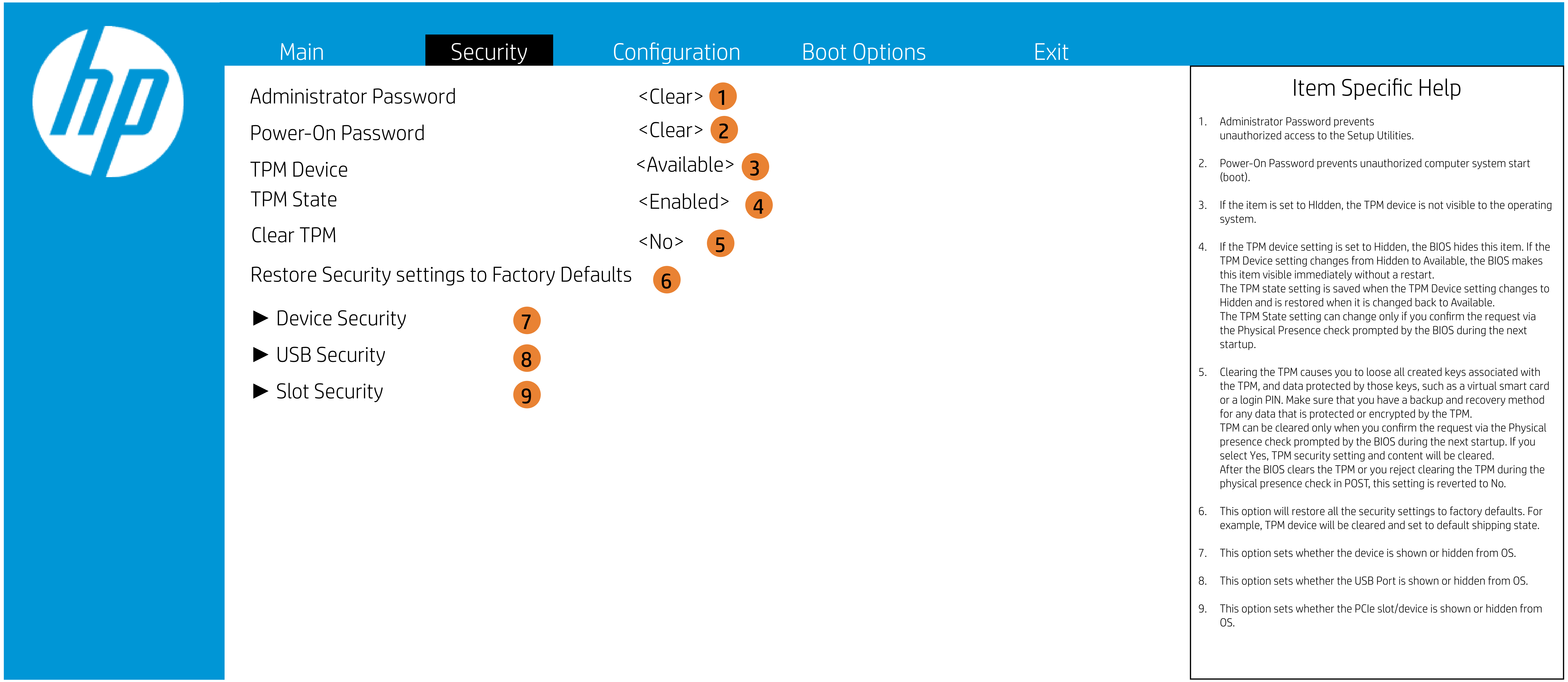
Item Specific Help

View System Log.

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 <No> 5

Restore Security settings to Factory Defaults 6

▶ Device Security 7

▶ USB Security 8

▶ Slot Security 9

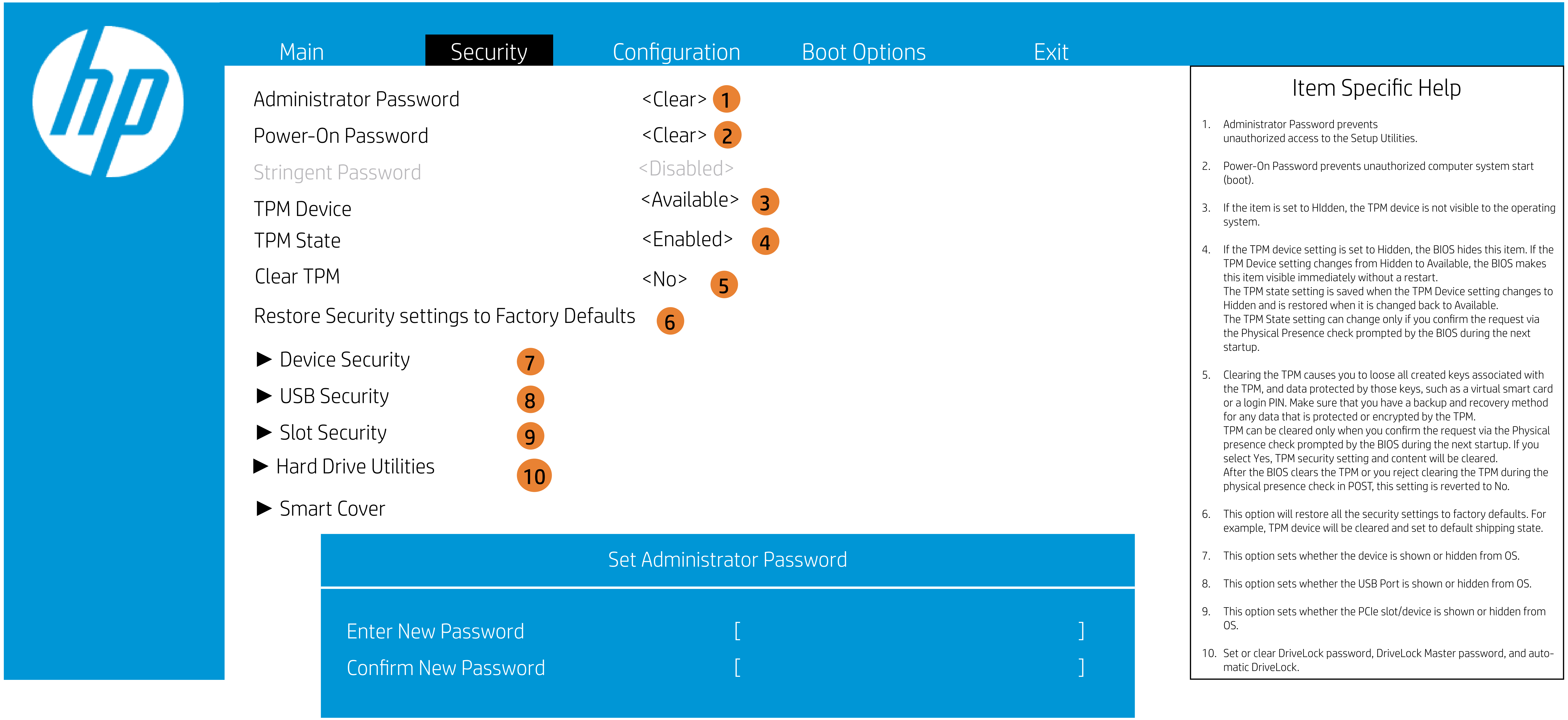
Item Specific Help

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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
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. This option sets whether the device is shown or hidden from OS.
8. This option sets whether the USB Port is shown or hidden from OS.
9. This option sets whether the PCIe slot/device is shown or hidden from OS.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear>

Power-On Password <Clear>

Stringent Password <Disabled>

TPM Device <Available>

TPM State <Enabled>

Clear TPM <No>

Restore Security settings to Factory Defaults

▶ Device Security

▶ USB Security

▶ Slot Security

▶ Hard Drive Utilities

▶ Smart Cover

Set Administrator Password

Enter New Password [ ]

Confirm New Password [ ]

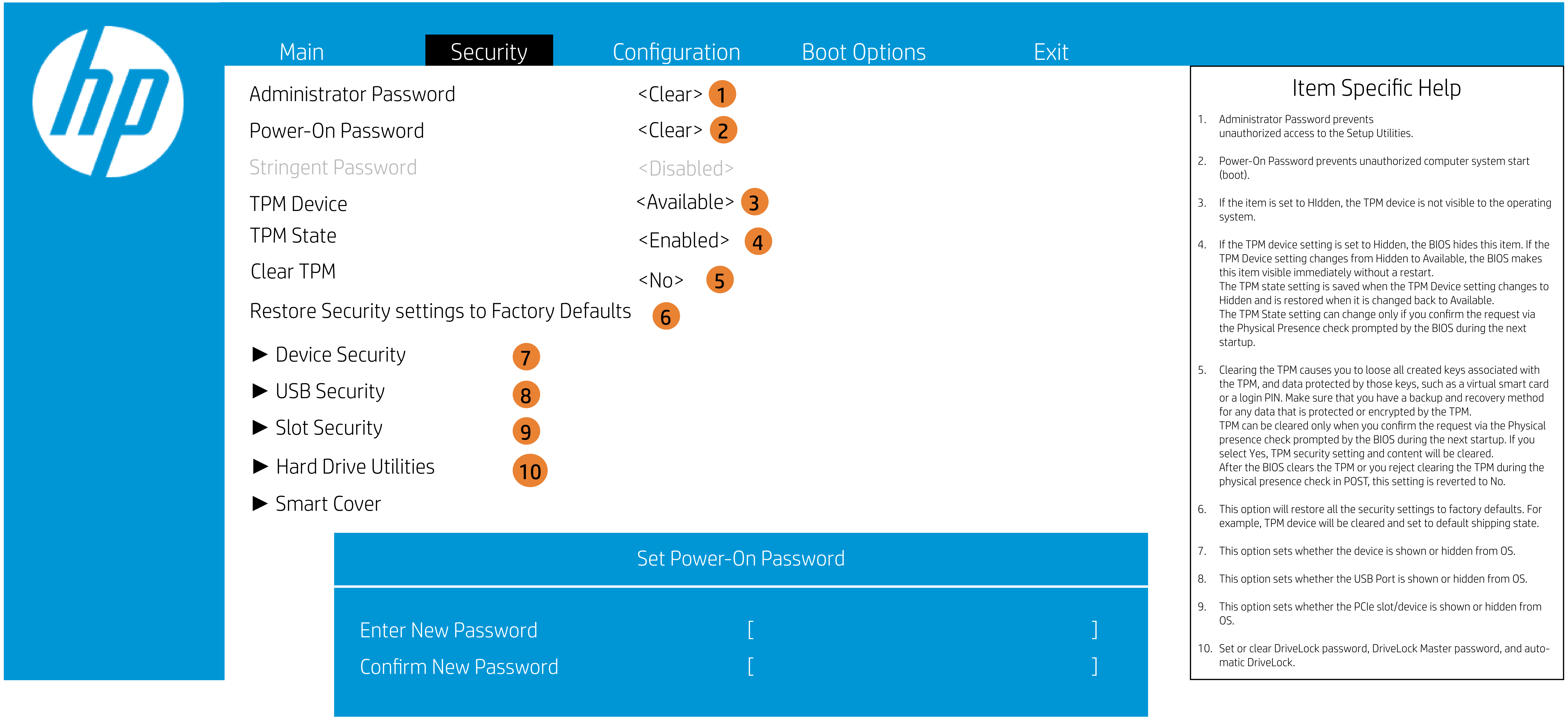
Item Specific Help

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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
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. This option sets whether the device is shown or hidden from OS.
8. This option sets whether the USB Port is shown or hidden from OS.
9. This option sets whether the PCIe slot/device is shown or hidden from OS.
10. Set or clear DriveLock password, DriveLock Master password, and automatic DriveLock.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear>

Power-On Password <Clear>

Stringent Password <Disabled>

TPM Device <Available>

TPM State <Enabled>

Clear TPM <No>

Restore Security settings to Factory Defaults

▶ Device Security

▶ USB Security

▶ Slot Security

▶ Hard Drive Utilities

▶ Smart Cover

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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.

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. This option sets whether the device is shown or hidden from OS.

8. This option sets whether the USB Port is shown or hidden from OS.

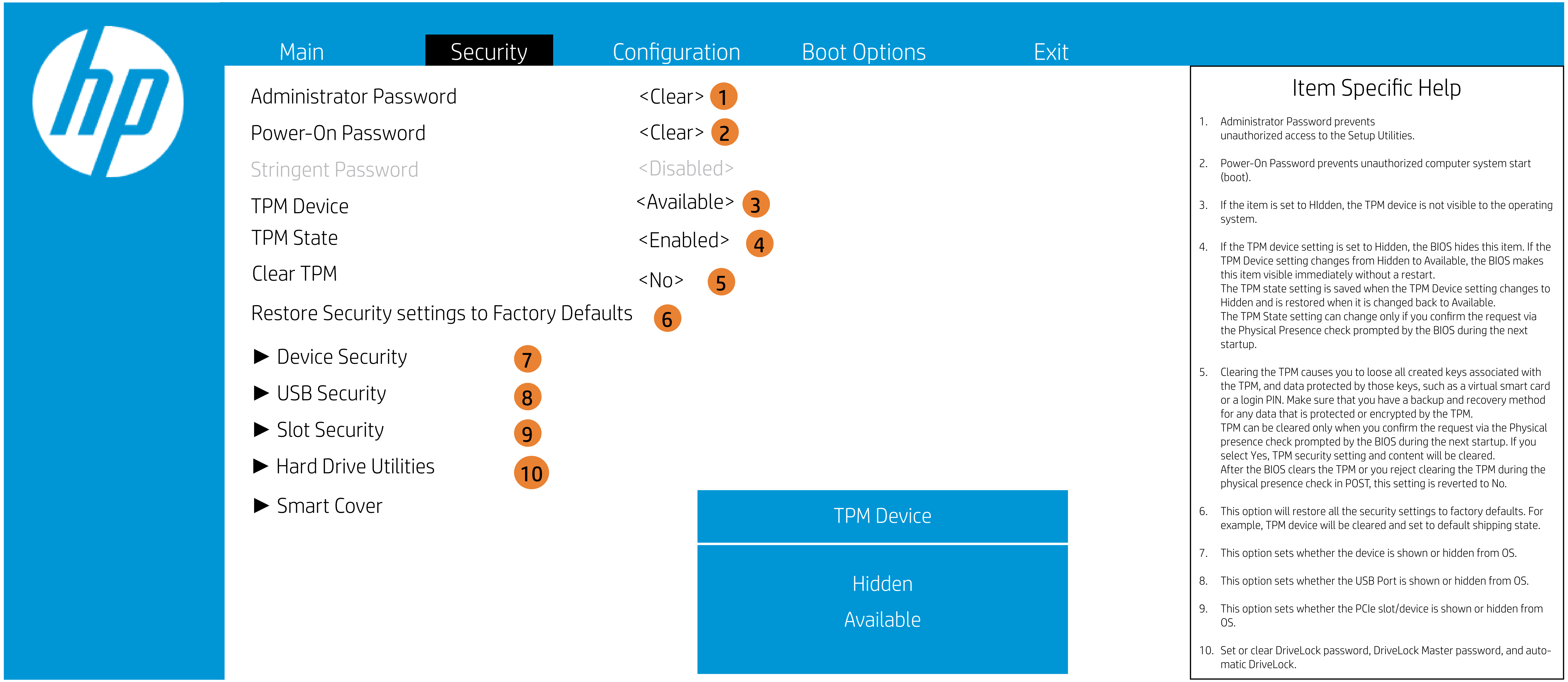
9. This option sets whether the PCIe slot/device is shown or hidden from OS.

10. Set or clear DriveLock password, DriveLock Master password, and automatic DriveLock.

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

Stringent Password <Disabled>

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <No> 5

Restore Security settings to Factory Defaults 6

▶ Device Security 7

▶ USB Security 8

▶ Slot Security 9

▶ Hard Drive Utilities 10

▶ Smart Cover

TPM Device

Hidden

Available

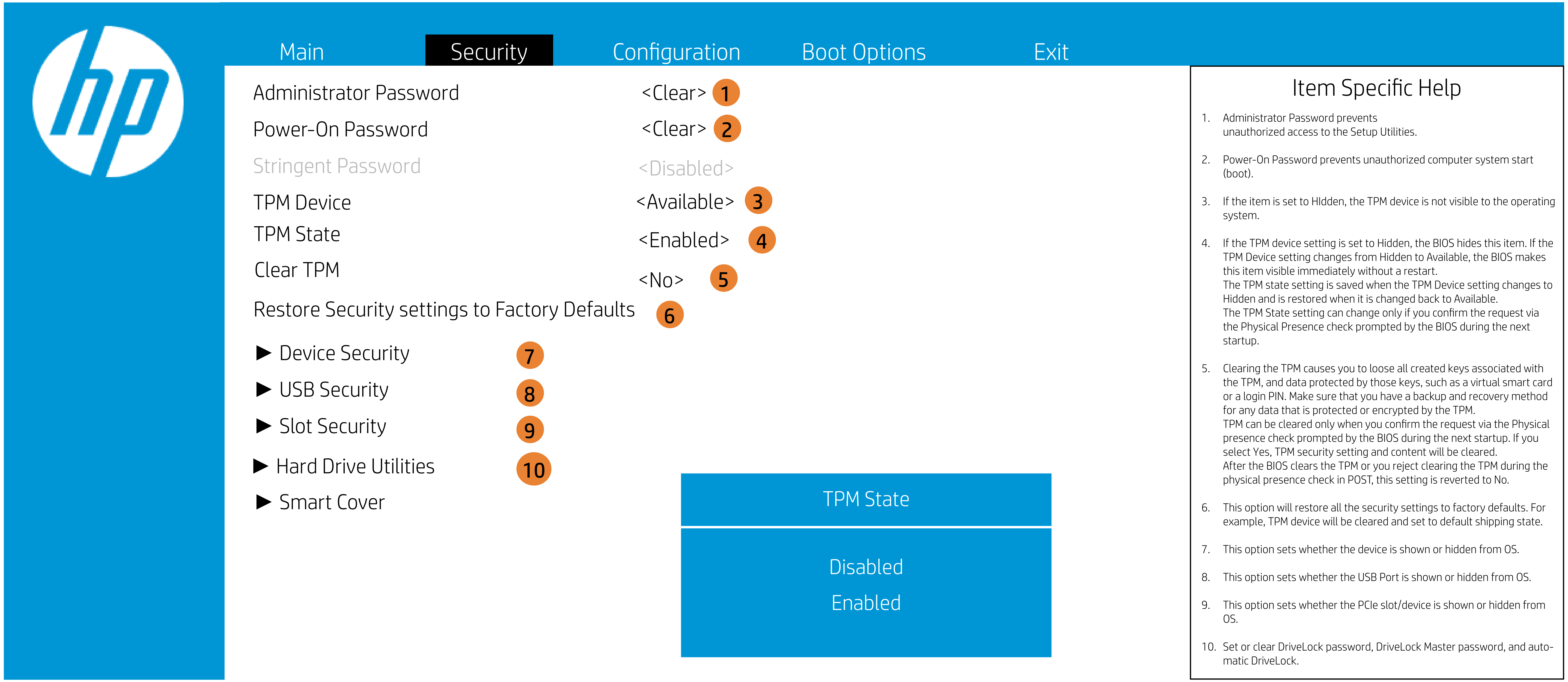
Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. 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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
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. This option sets whether the device is shown or hidden from OS.
8. This option sets whether the USB Port is shown or hidden from OS.
9. This option sets whether the PCIe slot/device is shown or hidden from OS.
10. Set or clear DriveLock password, DriveLock Master password, and automatic DriveLock.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

Stringent Password <Disabled>

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <No> 5

Restore Security settings to Factory Defaults 6

▶ Device Security 7

▶ USB Security 8

▶ Slot Security 9

▶ Hard Drive Utilities 10

▶ Smart Cover

TPM State

Disabled

Enabled

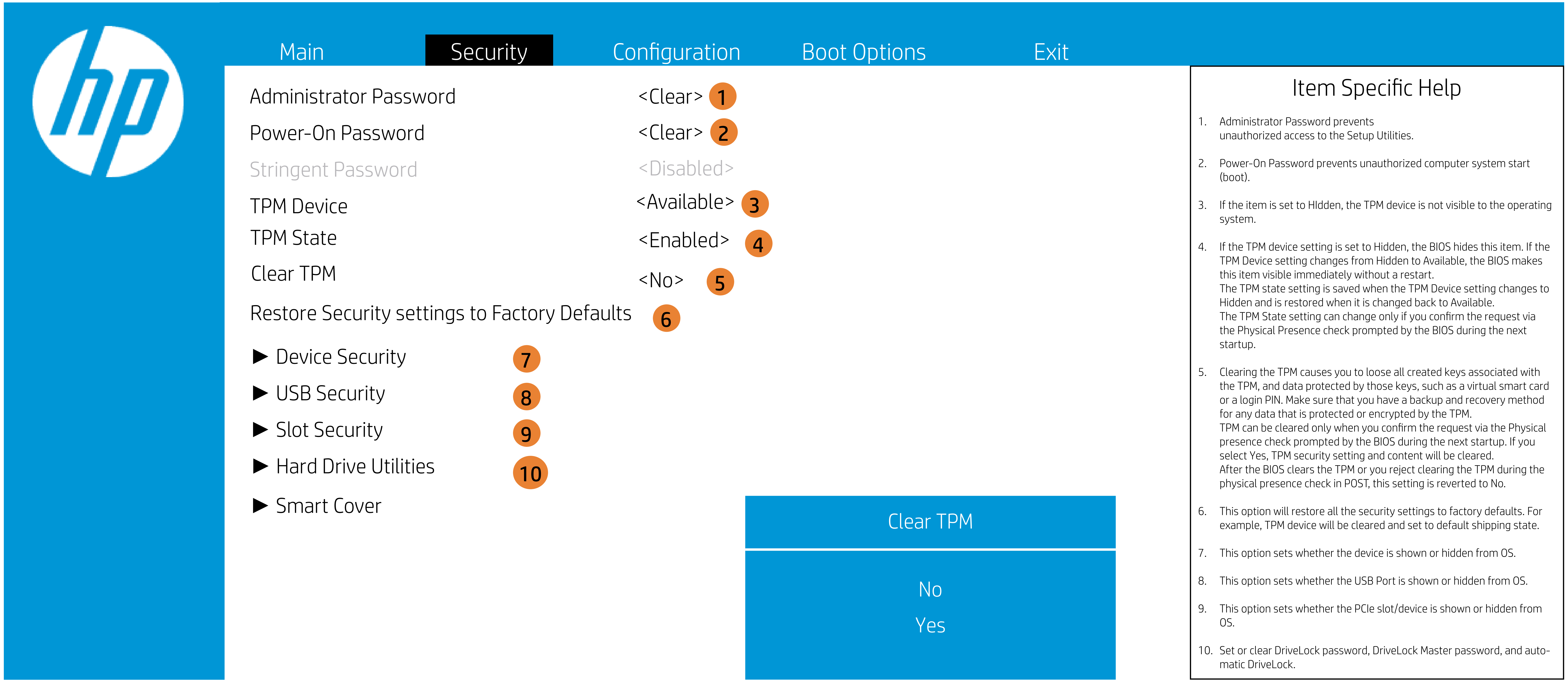
Item Specific Help

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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
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. This option sets whether the device is shown or hidden from OS.
8. This option sets whether the USB Port is shown or hidden from OS.
9. This option sets whether the PCIe slot/device is shown or hidden from OS.
10. Set or clear DriveLock password, DriveLock Master password, and automatic DriveLock.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Administrator Password <Clear> 1

Power-On Password <Clear> 2

Stringent Password <Disabled>

TPM Device <Available> 3

TPM State <Enabled> 4

Clear TPM <No> 5

Restore Security settings to Factory Defaults 6

▶ Device Security 7

▶ USB Security 8

▶ Slot Security 9

▶ Hard Drive Utilities 10

▶ Smart Cover

Clear TPM

No

Yes

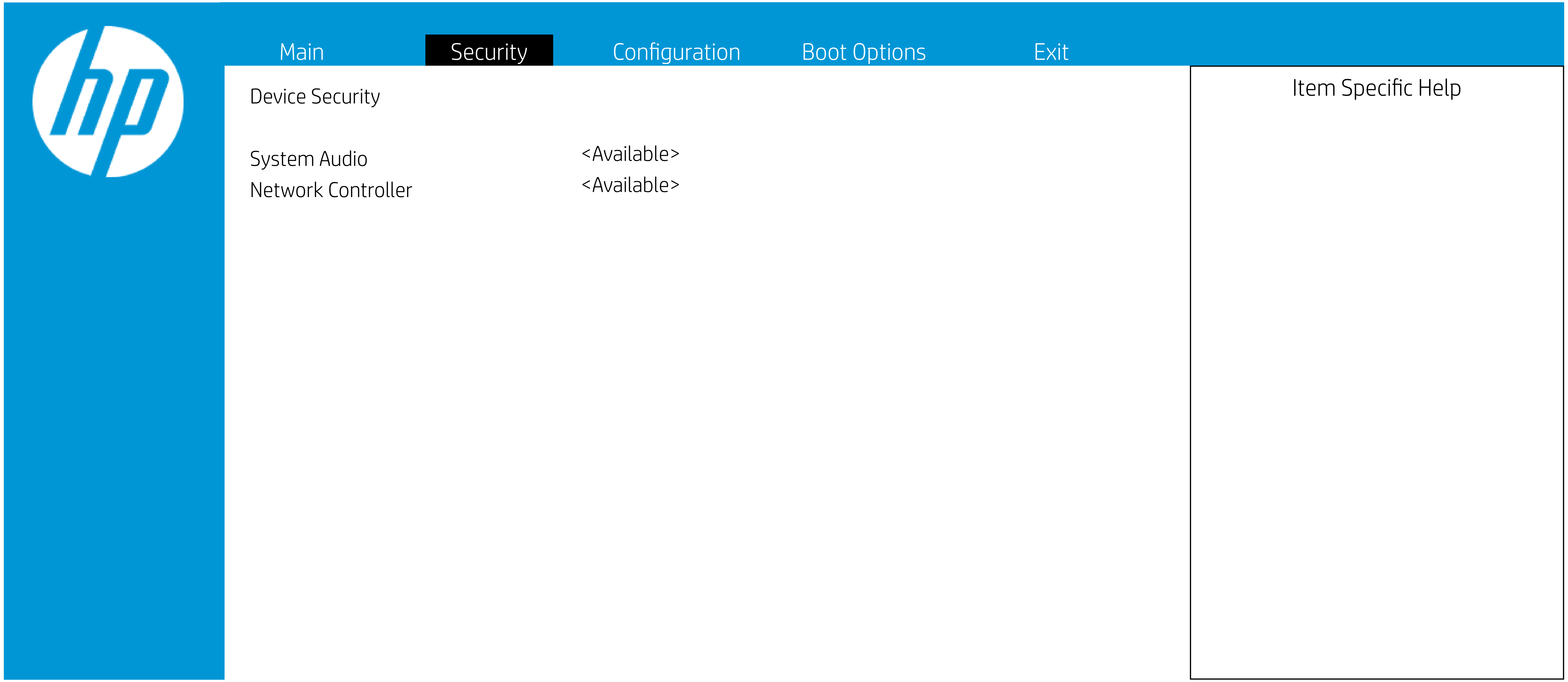
Item Specific Help

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. Clearing the TPM causes you to loose all created keys associated with the TPM, and data protected by those keys, such as a virtual smart card or a login PIN. Make sure that you have a backup and recovery method for any data that is protected or encrypted by the TPM.
   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, TPM security setting and content will be cleared.
   After the BIOS clears the TPM or you reject clearing the TPM during the physical presence check in POST, this setting is reverted to No.
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. This option sets whether the device is shown or hidden from OS.
8. This option sets whether the USB Port is shown or hidden from OS.
9. This option sets whether the PCIe slot/device is shown or hidden from OS.
10. Set or clear DriveLock password, DriveLock Master password, and automatic DriveLock.

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Device Security

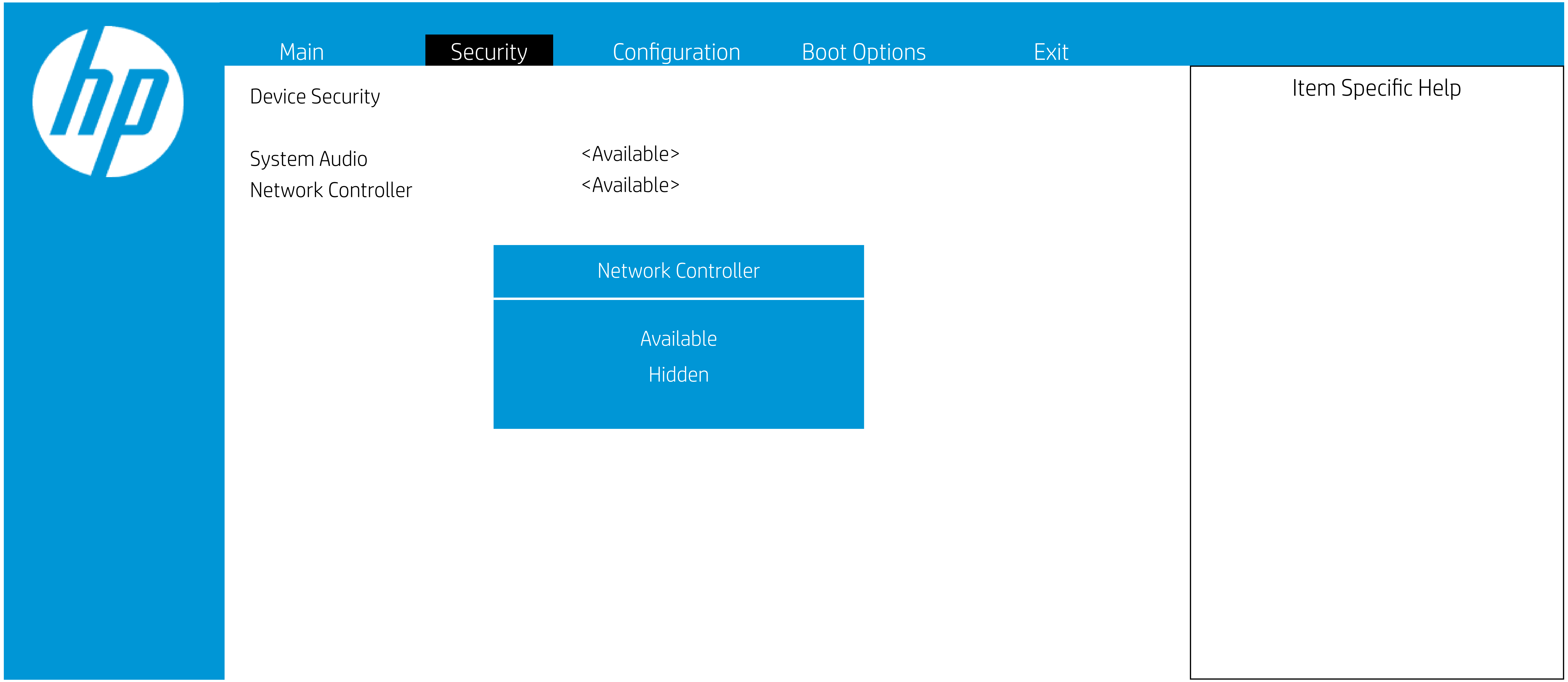
System Audio <Available>

Network Controller <Available>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Device Security

System Audio <Available>

Network Controller <Available>

Network Controller

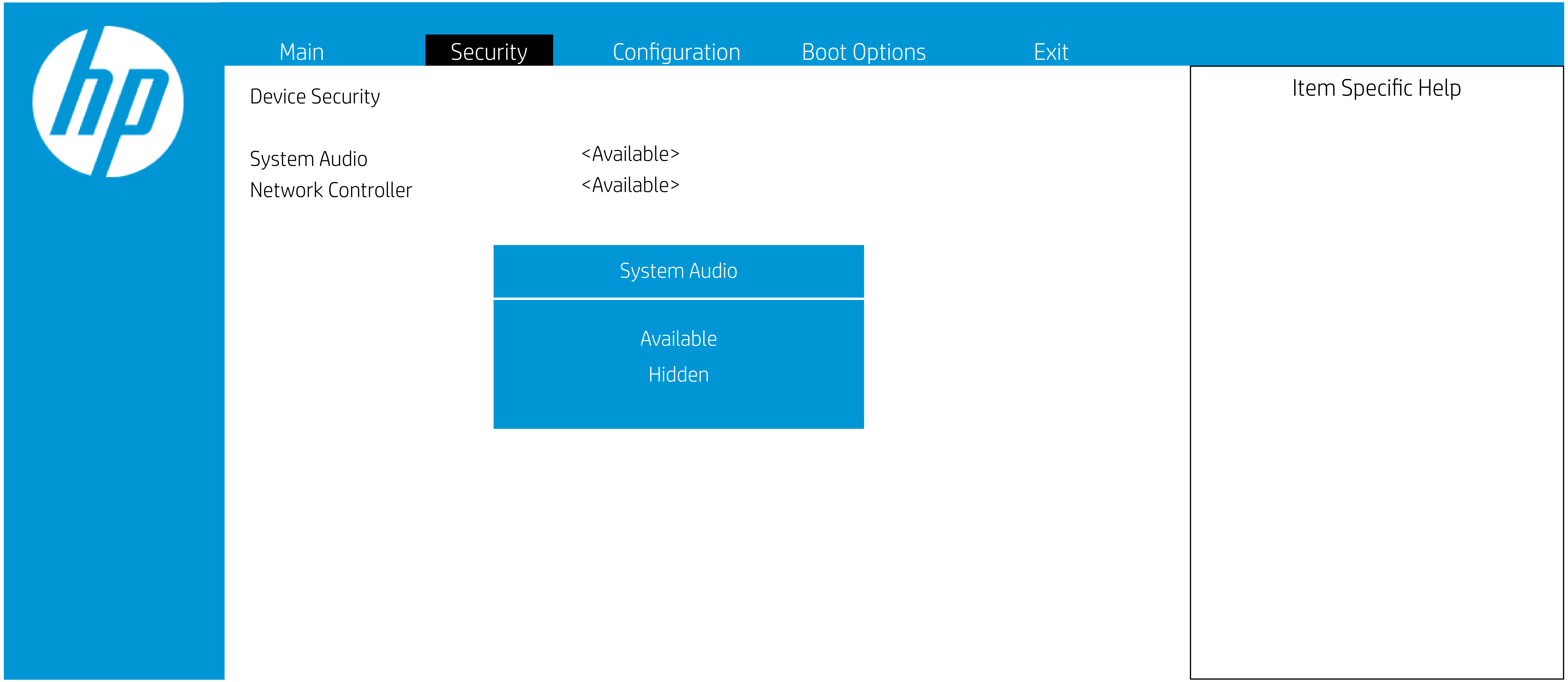
Available

Hidden

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Device Security

System Audio <Available>
Network Controller <Available>

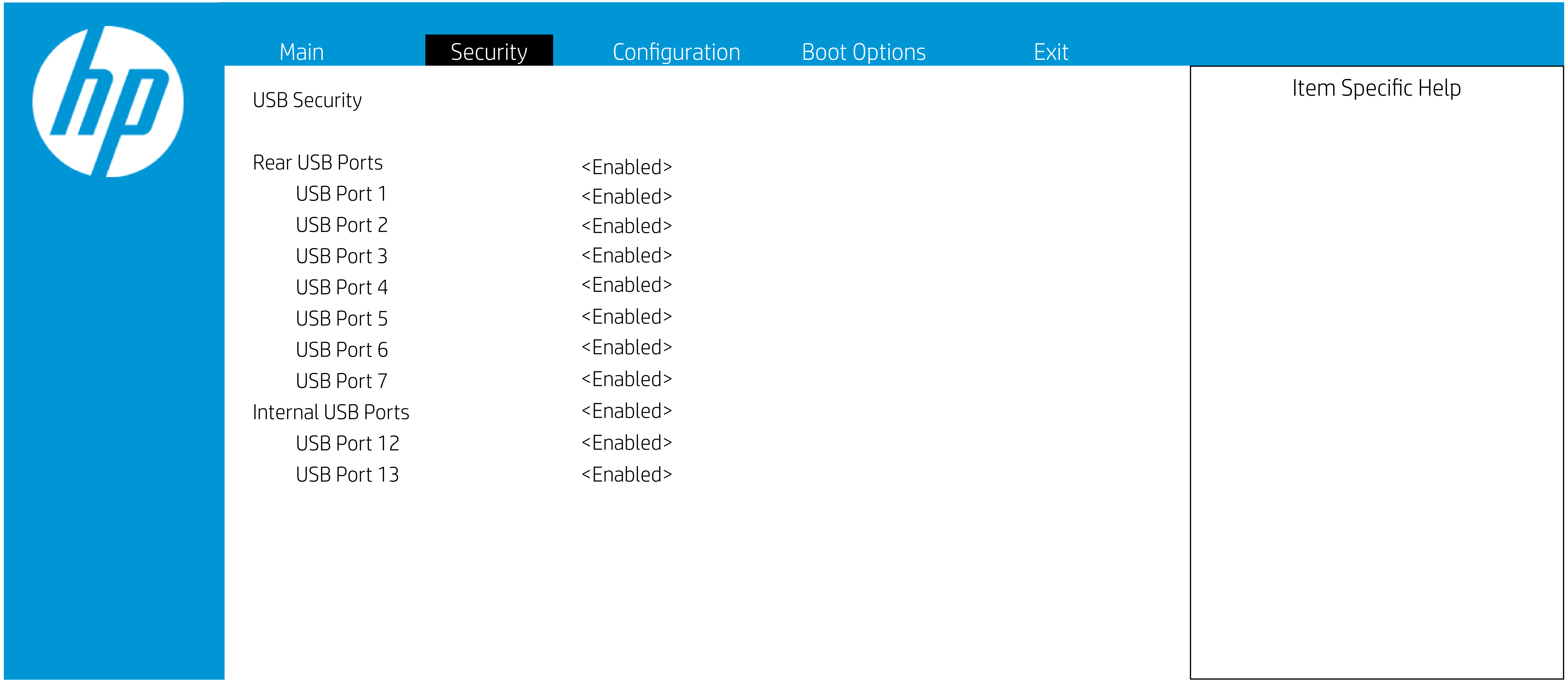
System Audio

Available
Hidden

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



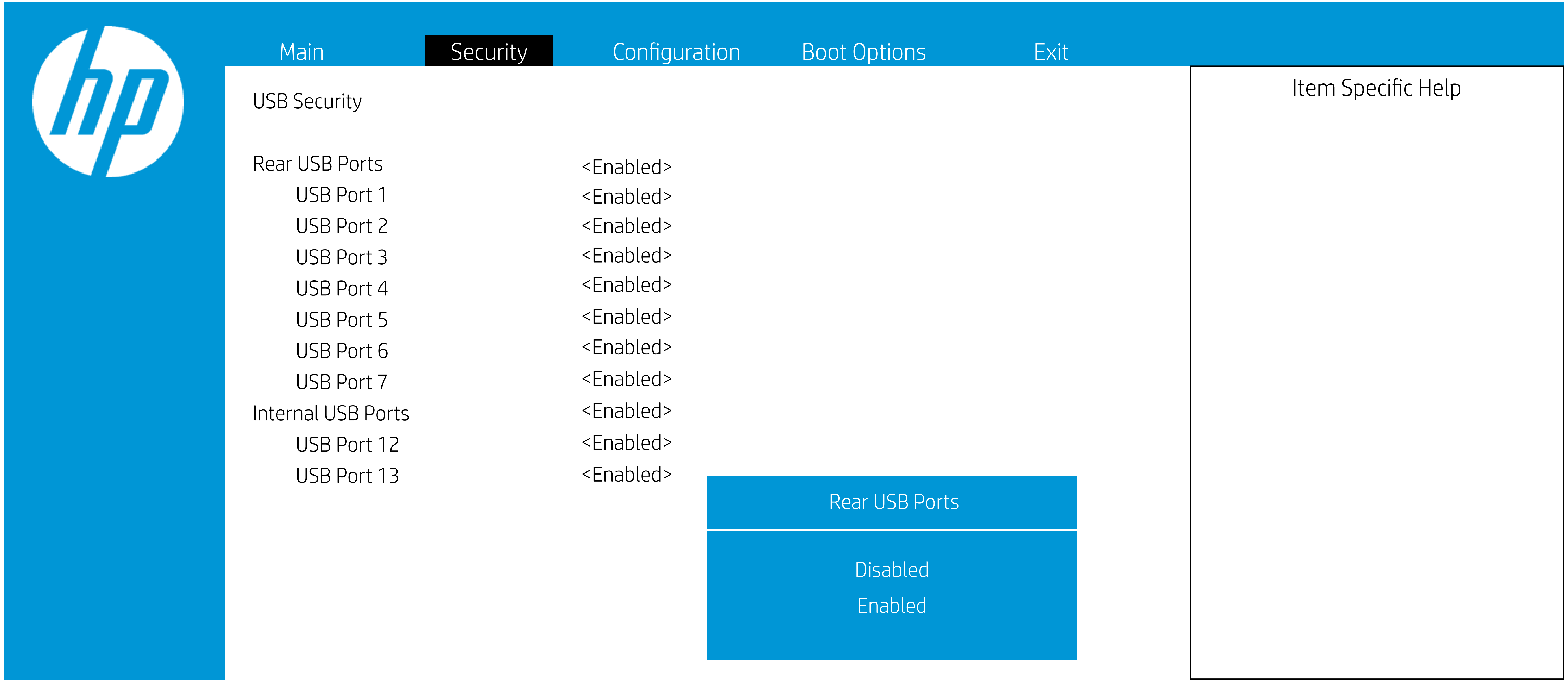
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



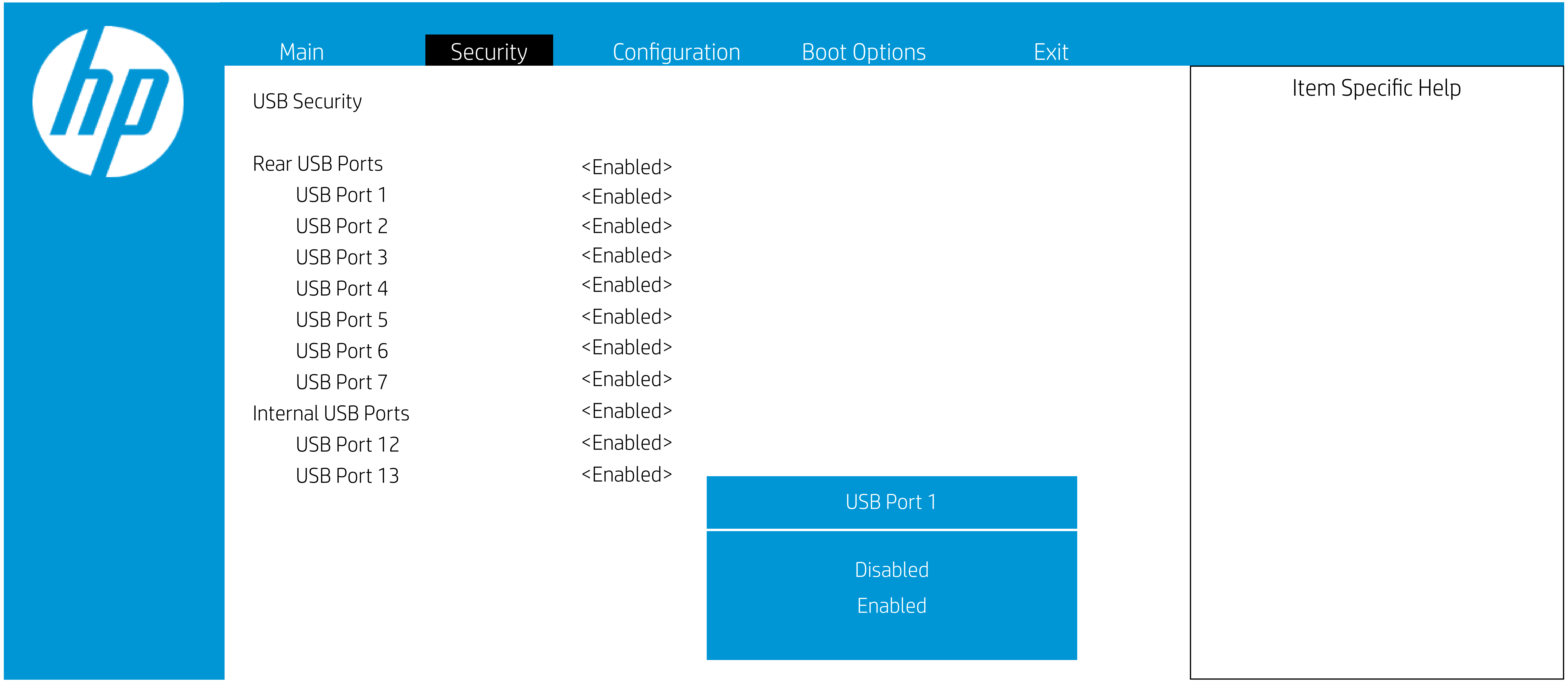
USB Security

```
Rear USB Ports          <Enabled>
    USB Port 1          <Enabled>
    USB Port 2          <Enabled>
    USB Port 3          <Enabled>
    USB Port 4          <Enabled>
    USB Port 5          <Enabled>
    USB Port 6          <Enabled>
    USB Port 7          <Enabled>
Internal USB Ports      <Enabled>
    USB Port 12         <Enabled>
    USB Port 13         <Enabled>
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



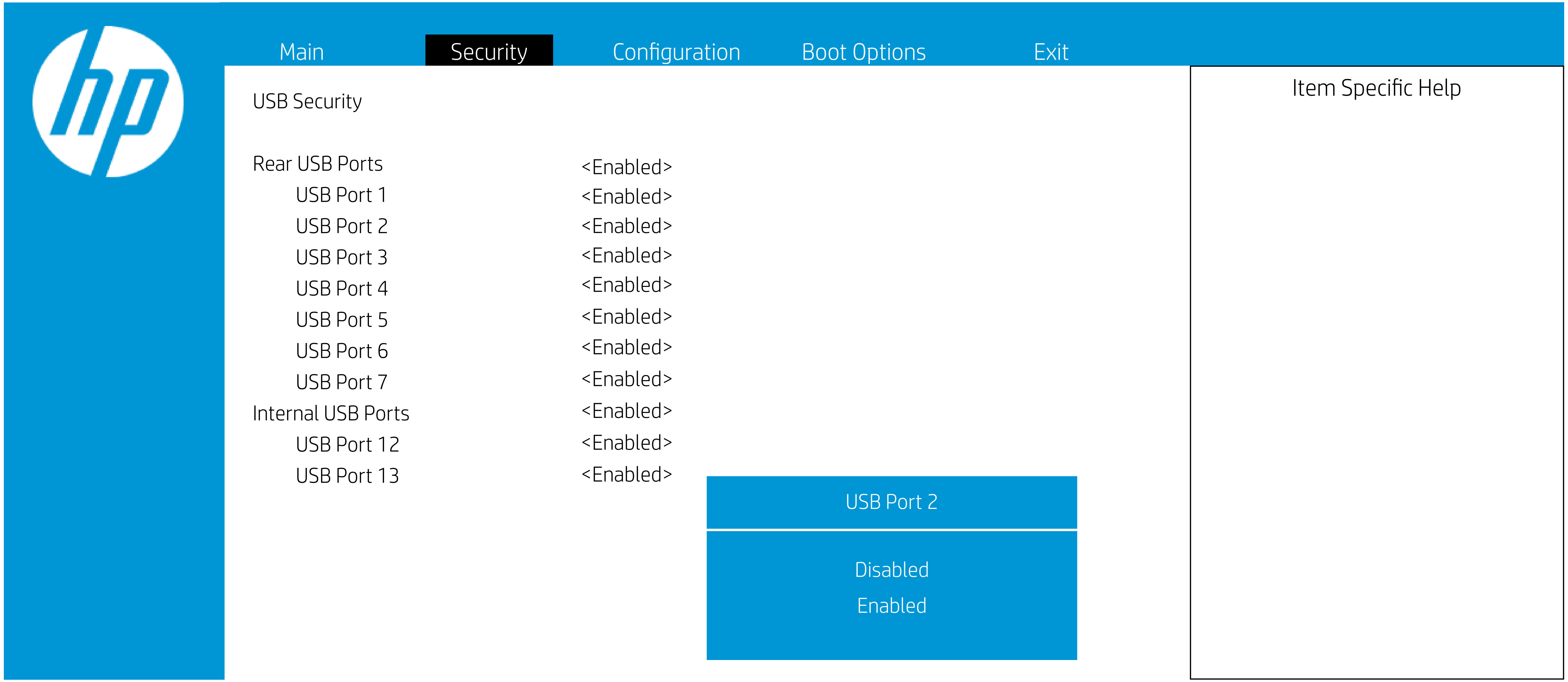
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

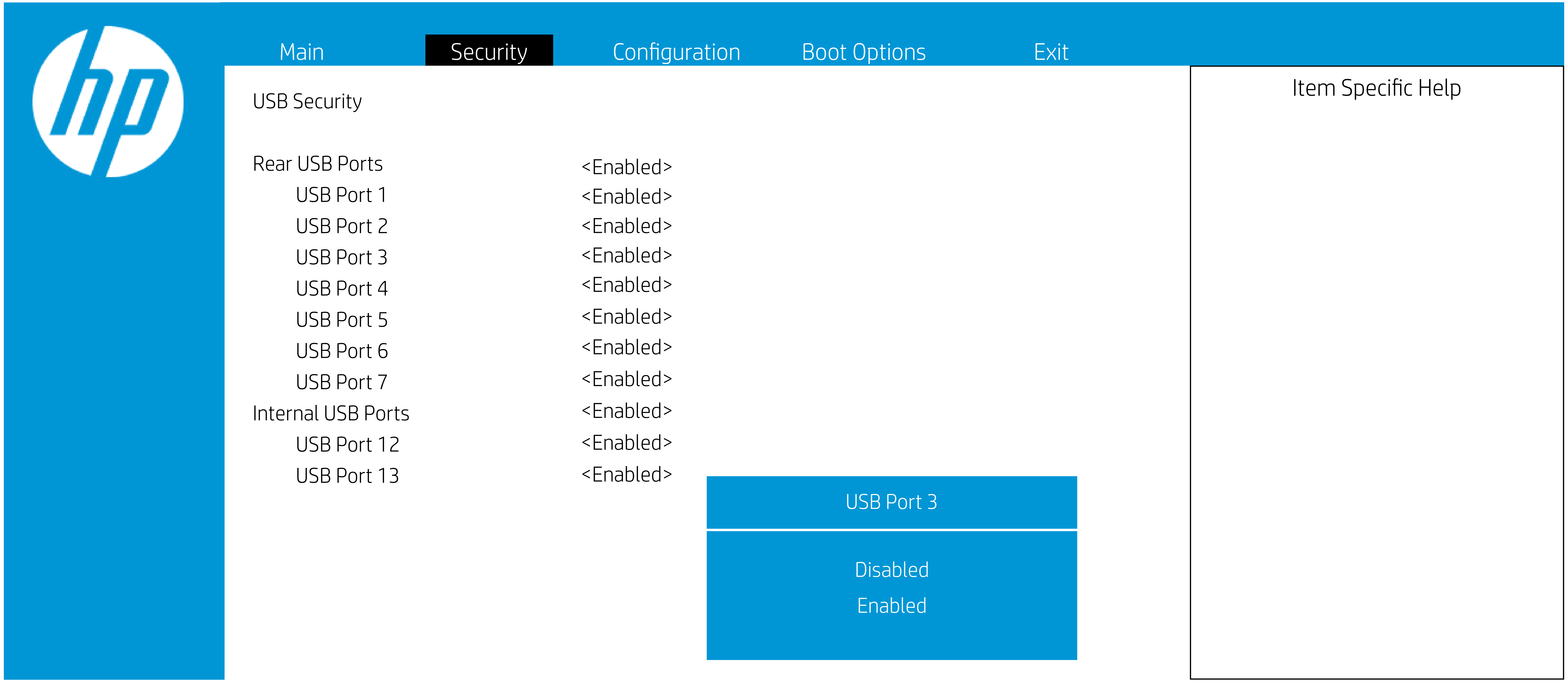
USB Port 2

Disabled
Enabled

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



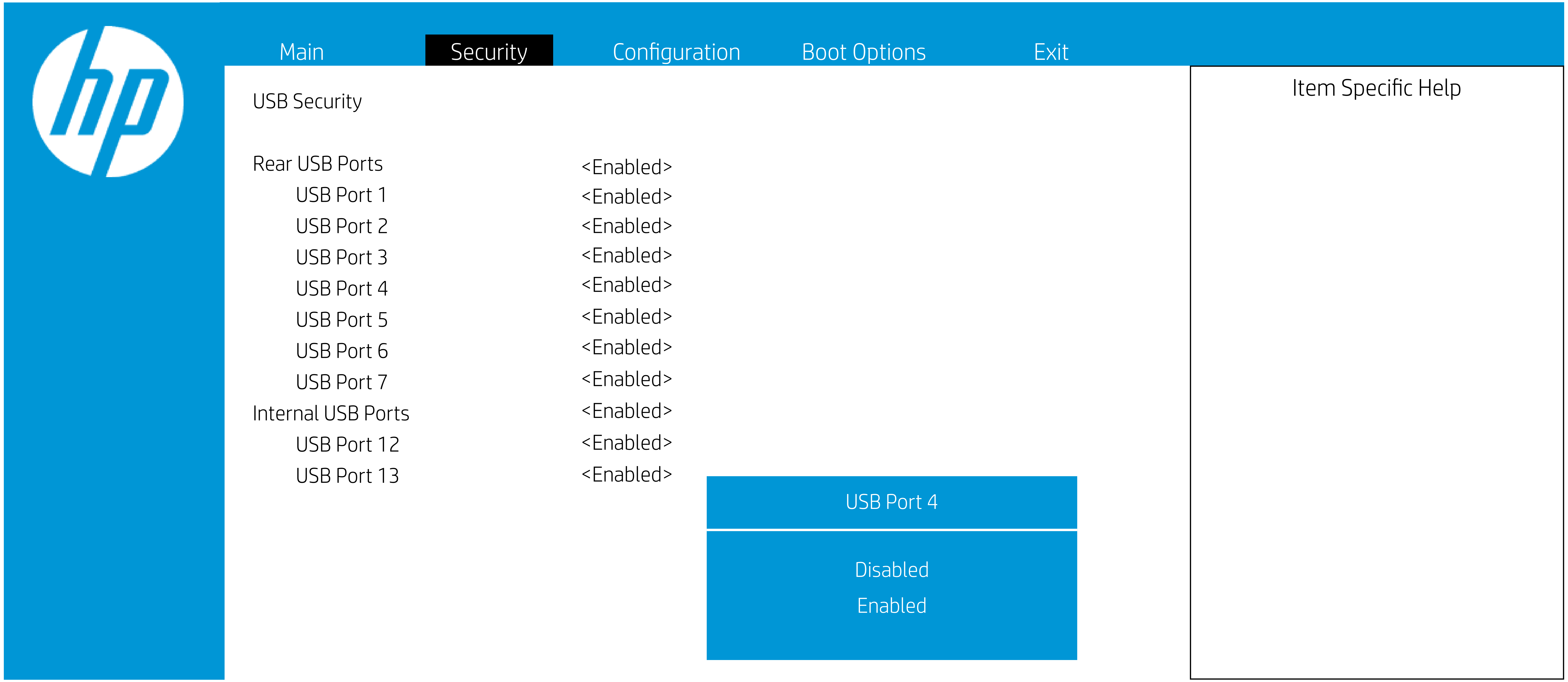
```
USB Security

Rear USB Ports             <Enabled>
      USB Port 1           <Enabled>
      USB Port 2           <Enabled>
      USB Port 3           <Enabled>
      USB Port 4           <Enabled>
      USB Port 5           <Enabled>
      USB Port 6           <Enabled>
      USB Port 7           <Enabled>
Internal USB Ports         <Enabled>
      USB Port 12          <Enabled>
      USB Port 13          <Enabled>
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



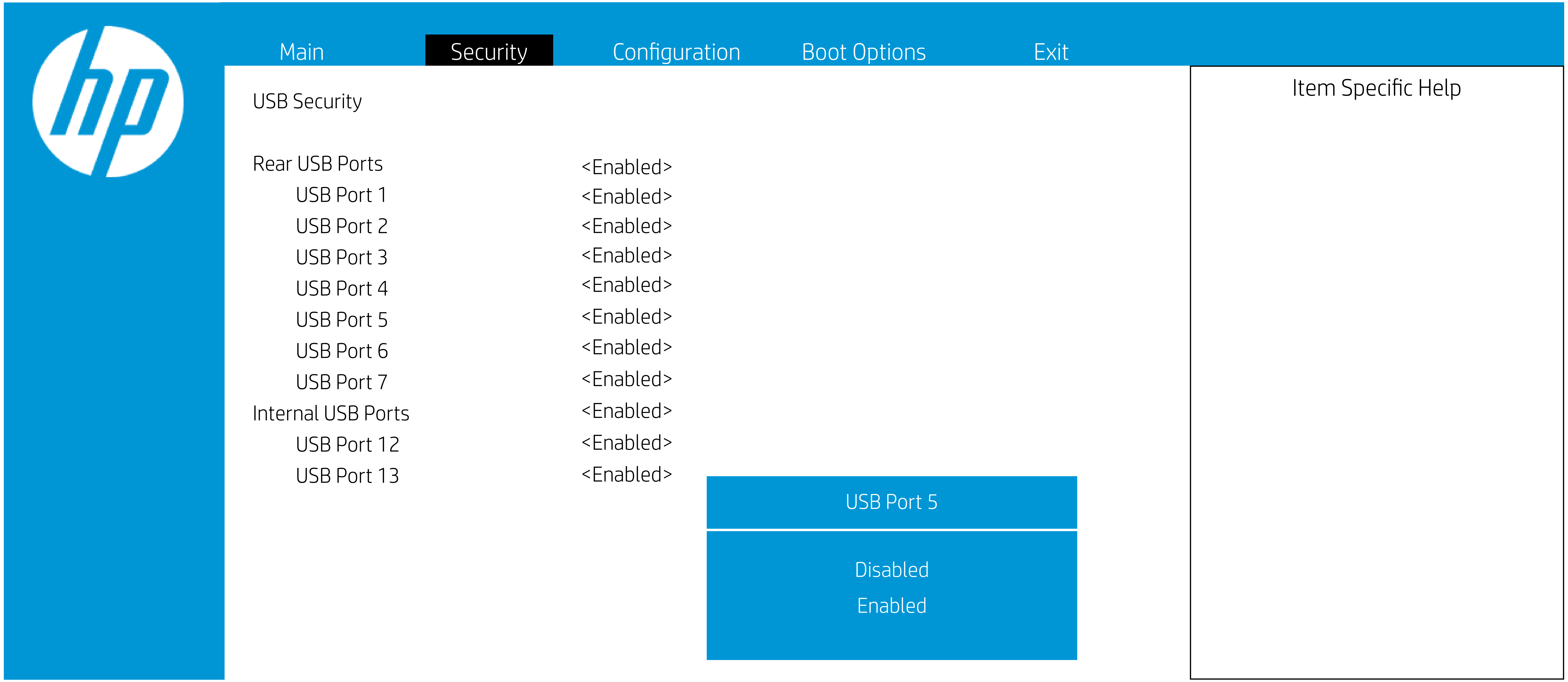
```
USB Security

Rear USB Ports              <Enabled>
     USB Port 1             <Enabled>
     USB Port 2             <Enabled>
     USB Port 3             <Enabled>
     USB Port 4             <Enabled>
     USB Port 5             <Enabled>
     USB Port 6             <Enabled>
     USB Port 7             <Enabled>
Internal USB Ports          <Enabled>
     USB Port 12            <Enabled>
     USB Port 13            <Enabled>
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



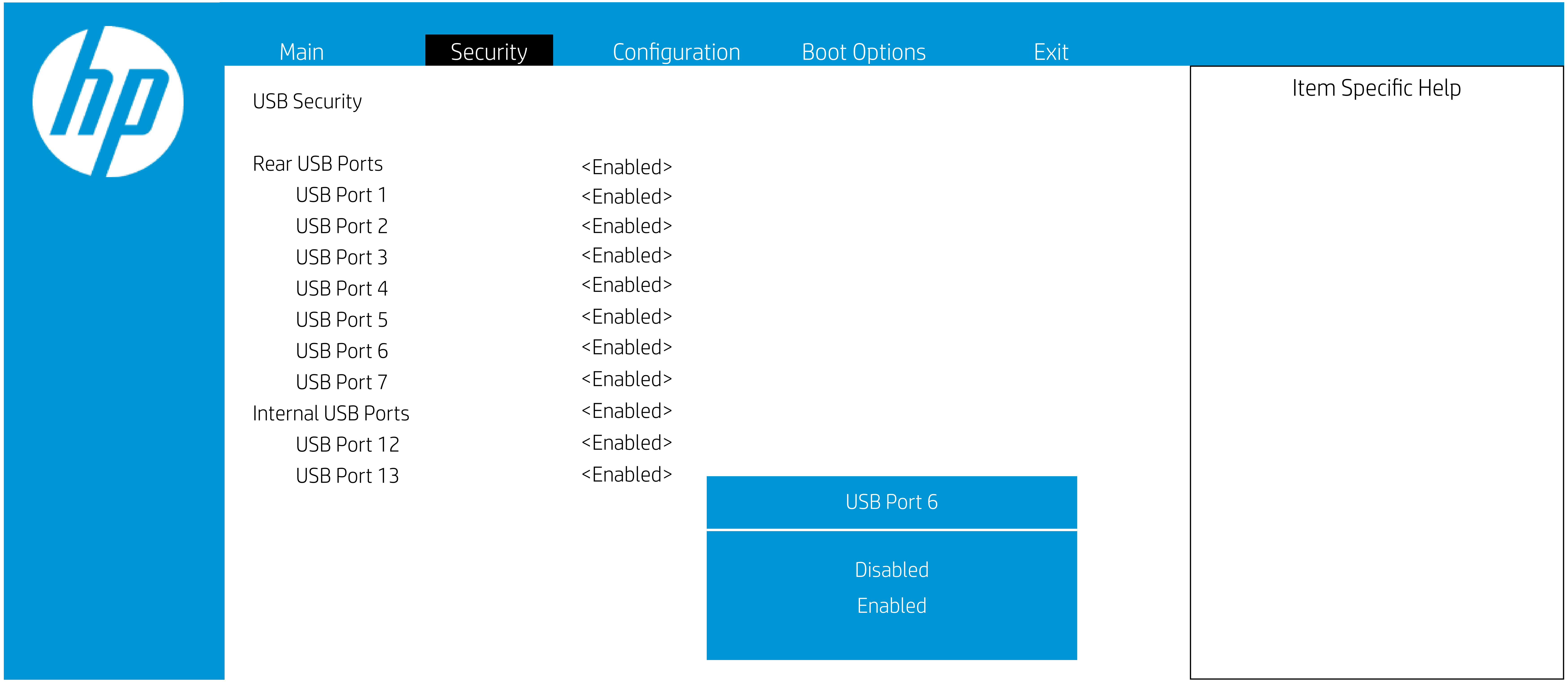
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



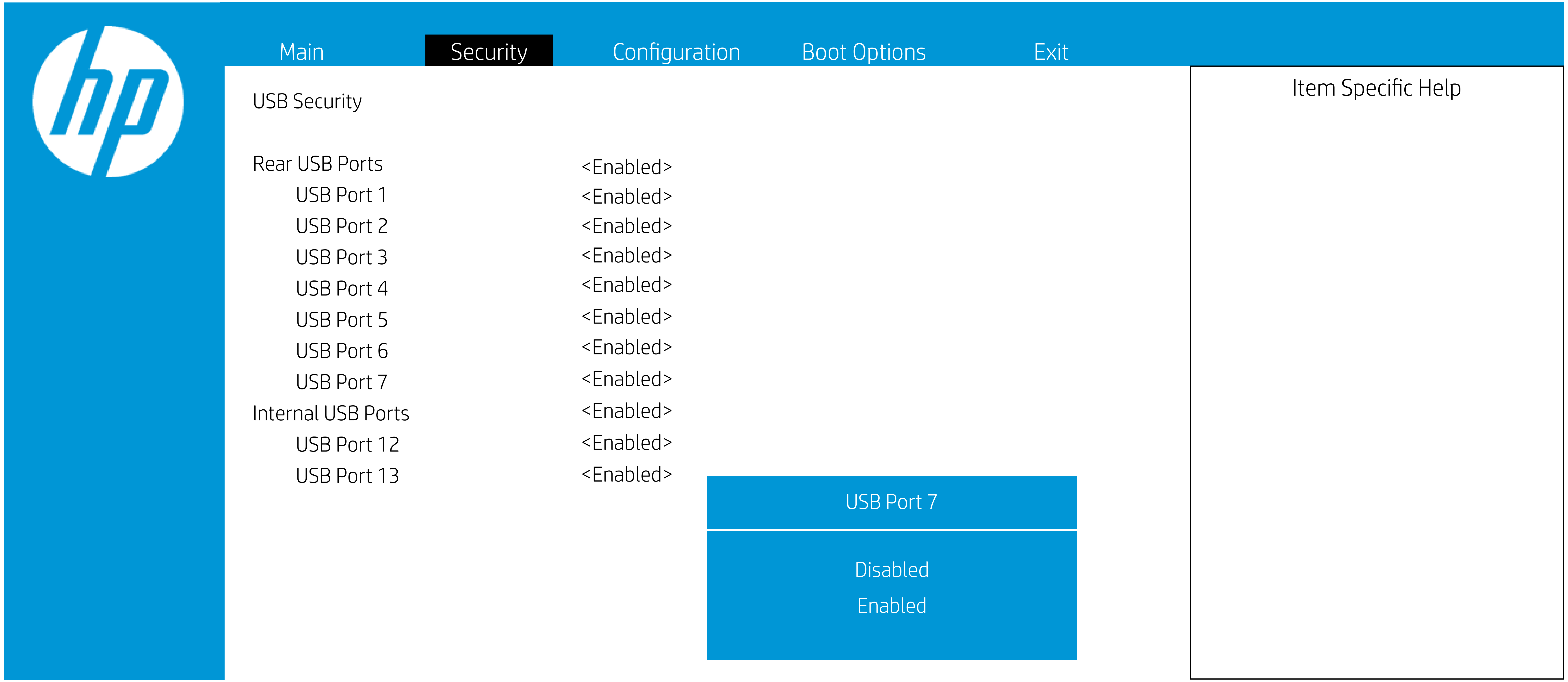
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

USB Port 7

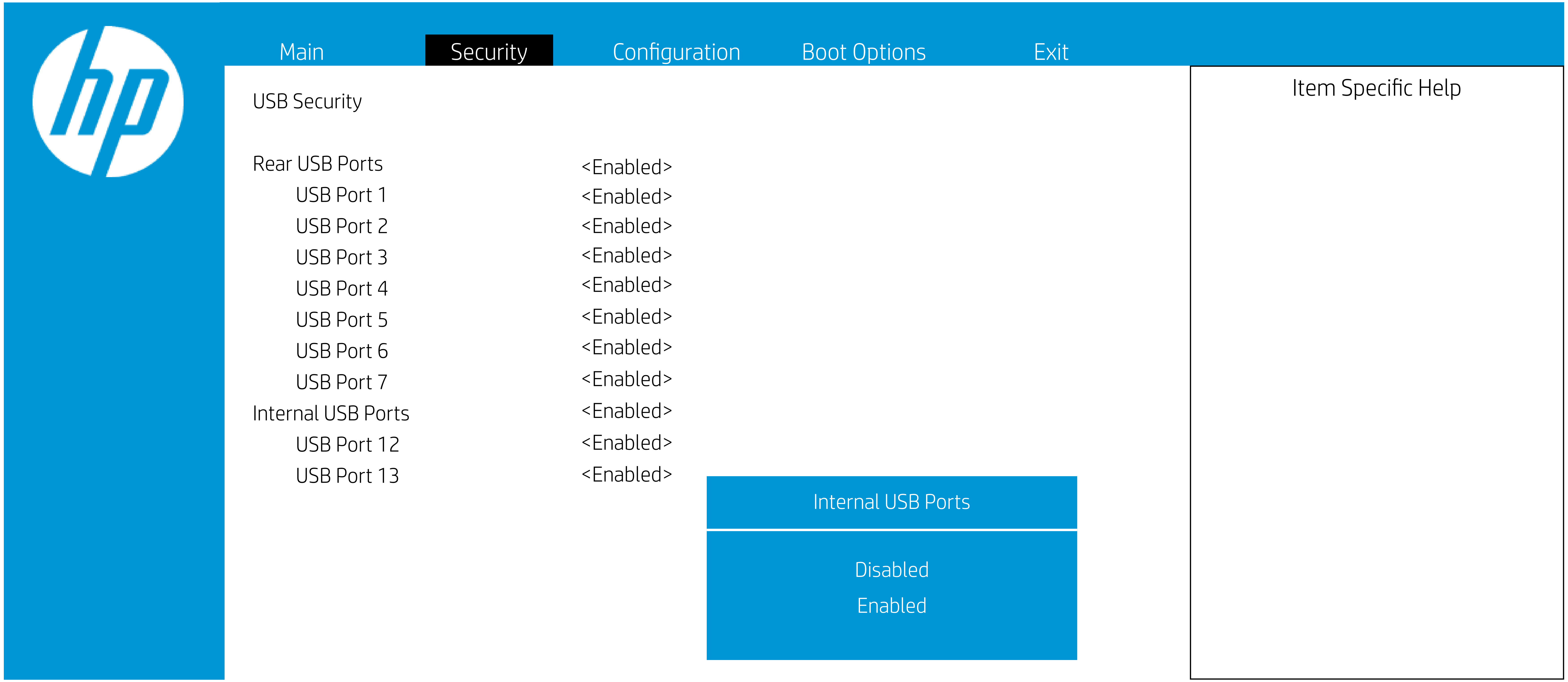
Disabled
Enabled

Item Specific Help

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



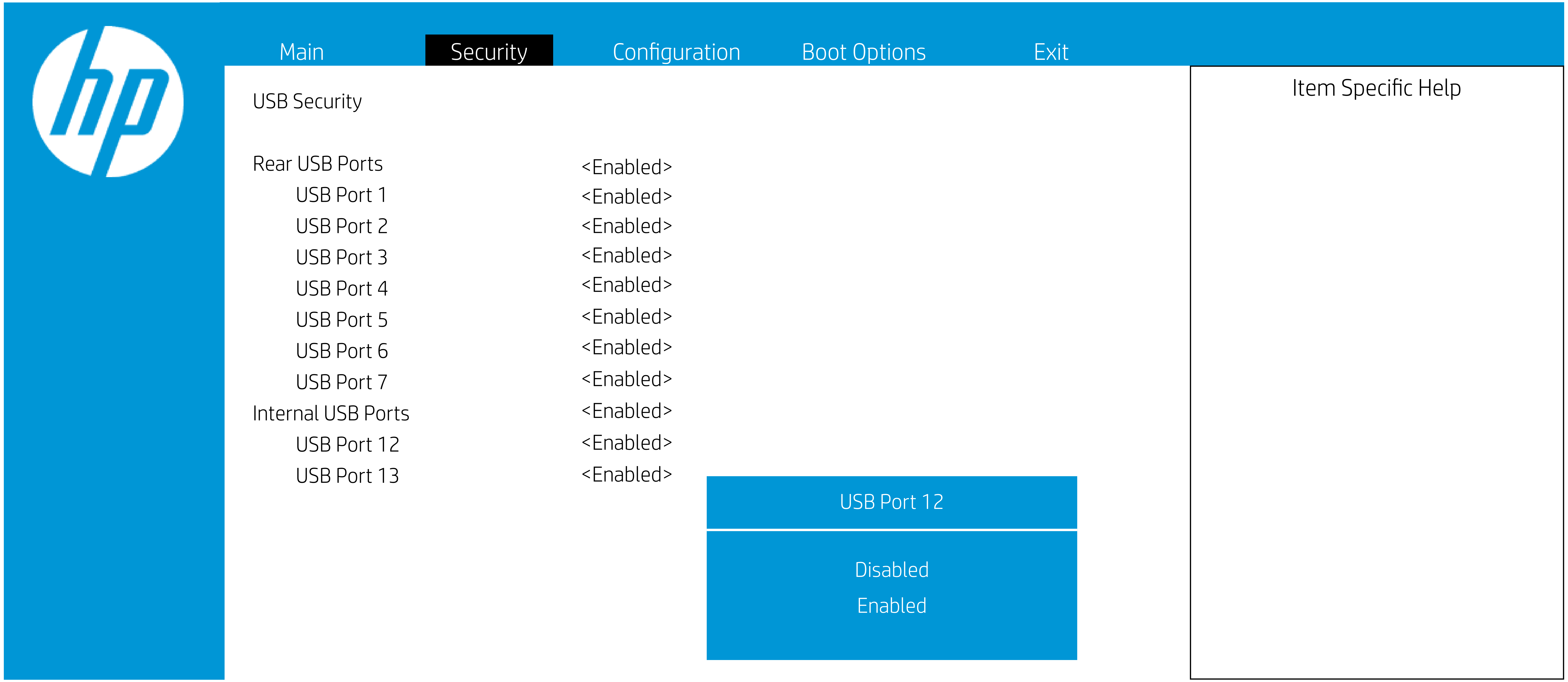
```
USB Security

Rear USB Ports                <Enabled>
      USB Port 1              <Enabled>
      USB Port 2              <Enabled>
      USB Port 3              <Enabled>
      USB Port 4              <Enabled>
      USB Port 5              <Enabled>
      USB Port 6              <Enabled>
      USB Port 7              <Enabled>
Internal USB Ports            <Enabled>
      USB Port 12             <Enabled>
      USB Port 13             <Enabled>
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



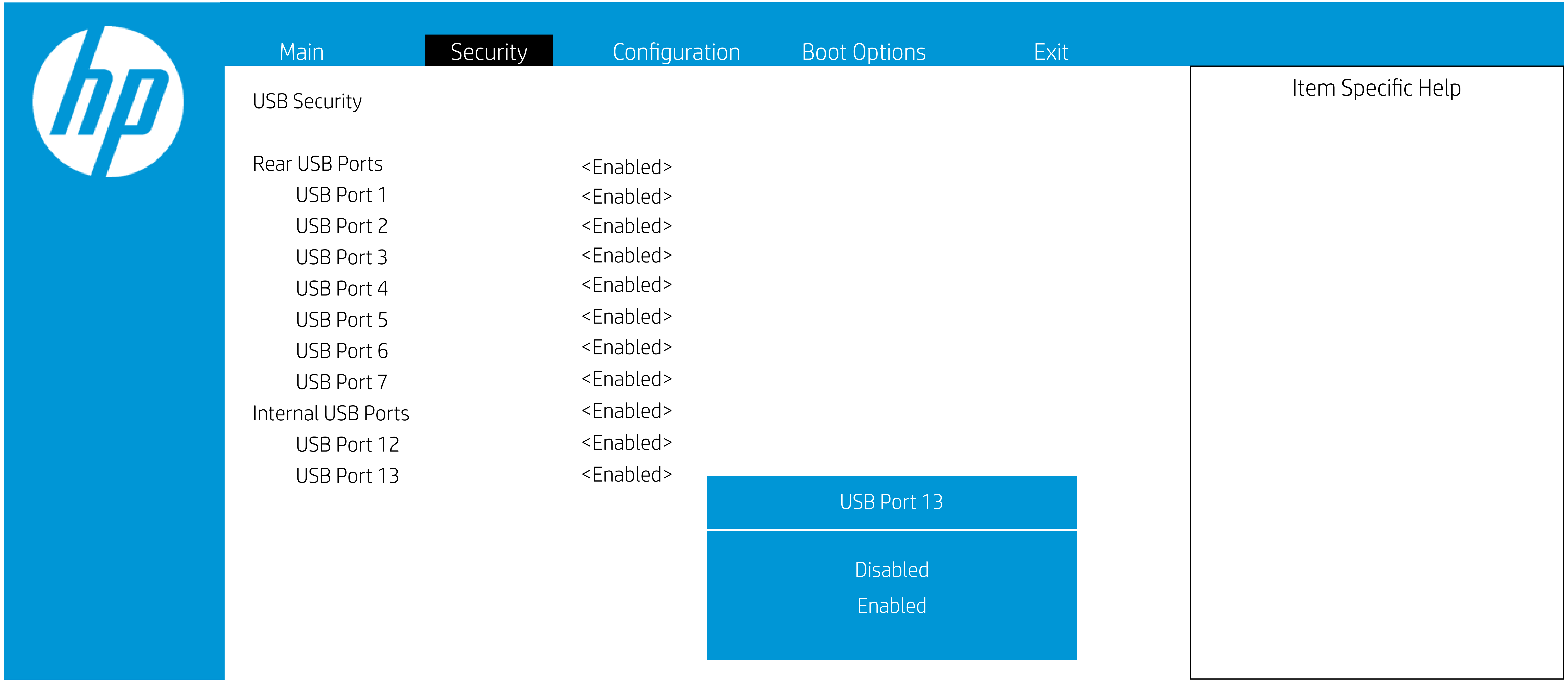
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



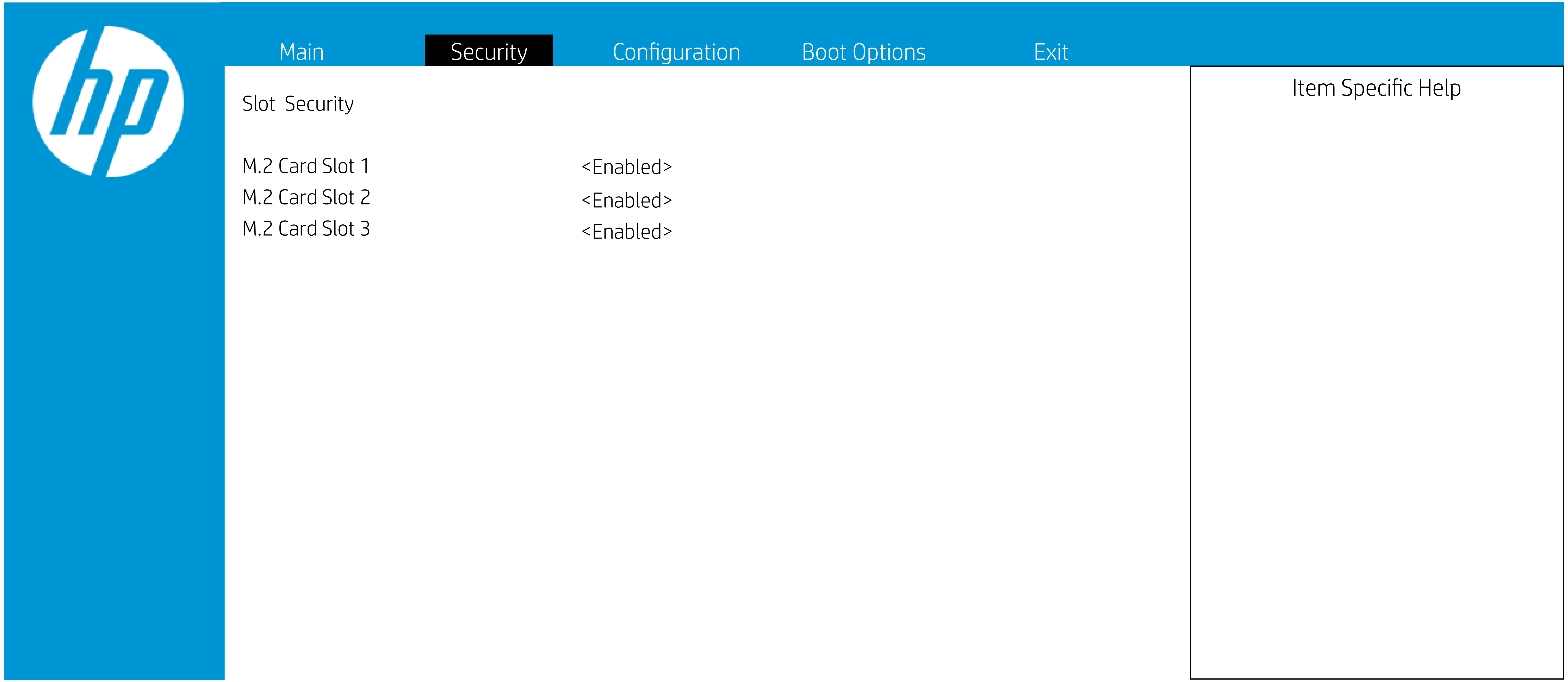
USB Security

Rear USB Ports	<Enabled>
USB Port 1	<Enabled>
USB Port 2	<Enabled>
USB Port 3	<Enabled>
USB Port 4	<Enabled>
USB Port 5	<Enabled>
USB Port 6	<Enabled>
USB Port 7	<Enabled>
Internal USB Ports	<Enabled>
USB Port 12	<Enabled>
USB Port 13	<Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



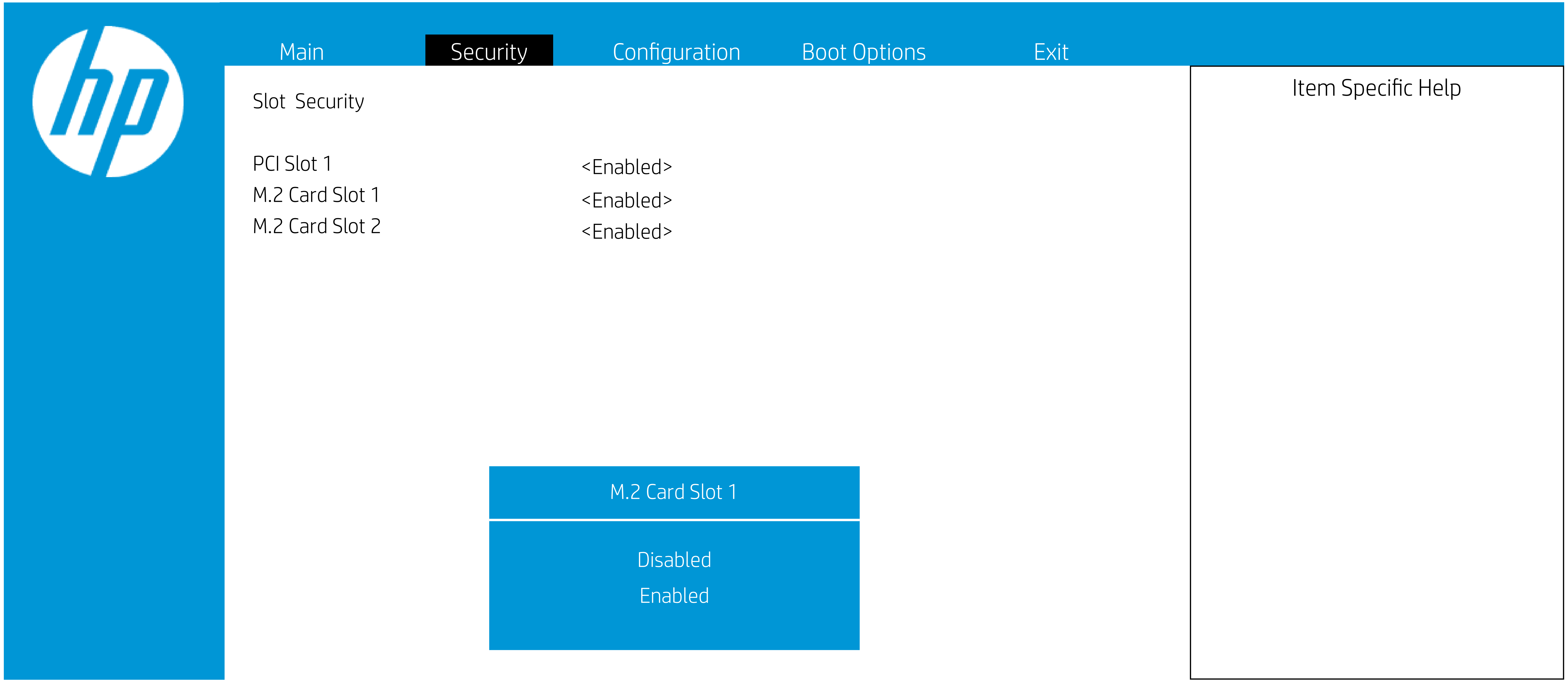
Slot Security

M.2 Card Slot 1 <Enabled>
M.2 Card Slot 2 <Enabled>
M.2 Card Slot 3 <Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



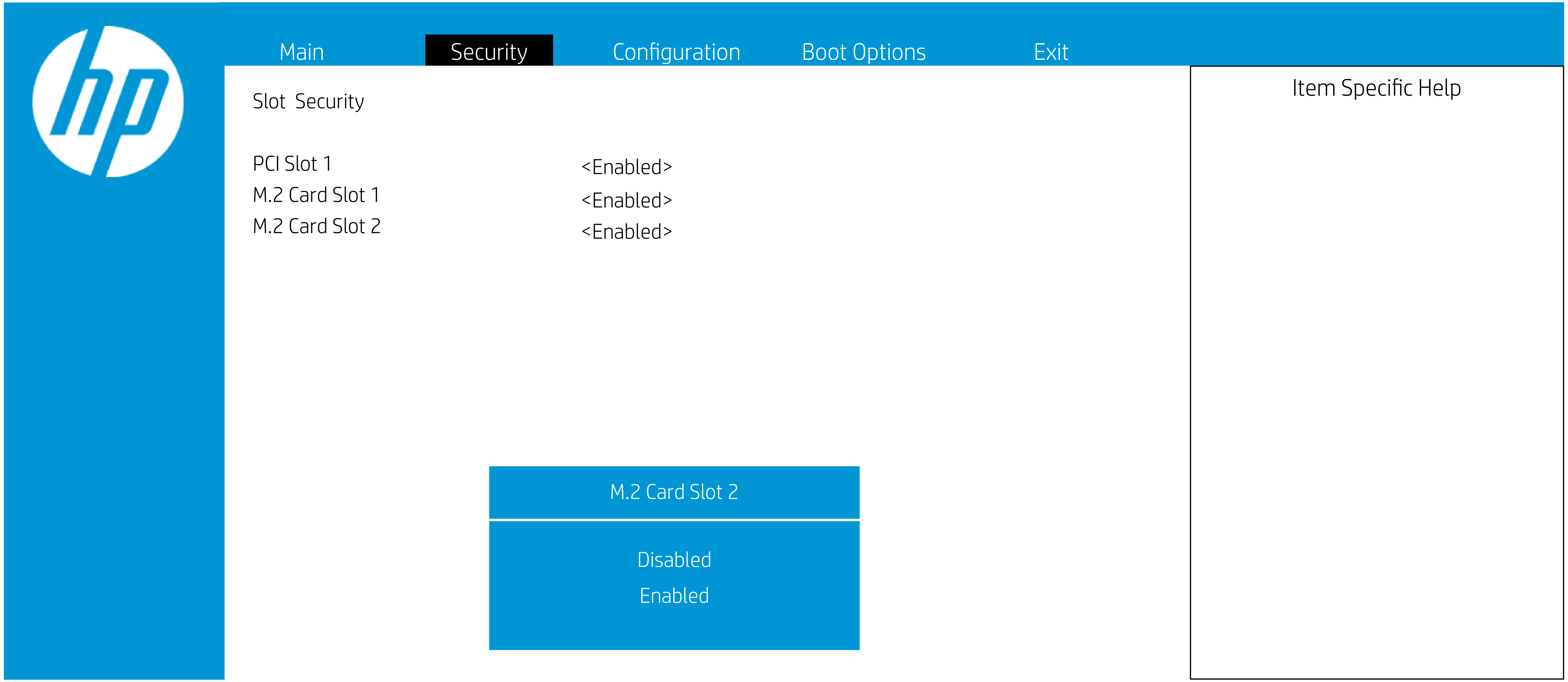
Slot Security

```
PCI Slot 1              <Enabled>
M.2 Card Slot 1         <Enabled>
M.2 Card Slot 2         <Enabled>
```

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Slot Security

PCI Slot 1 <Enabled>

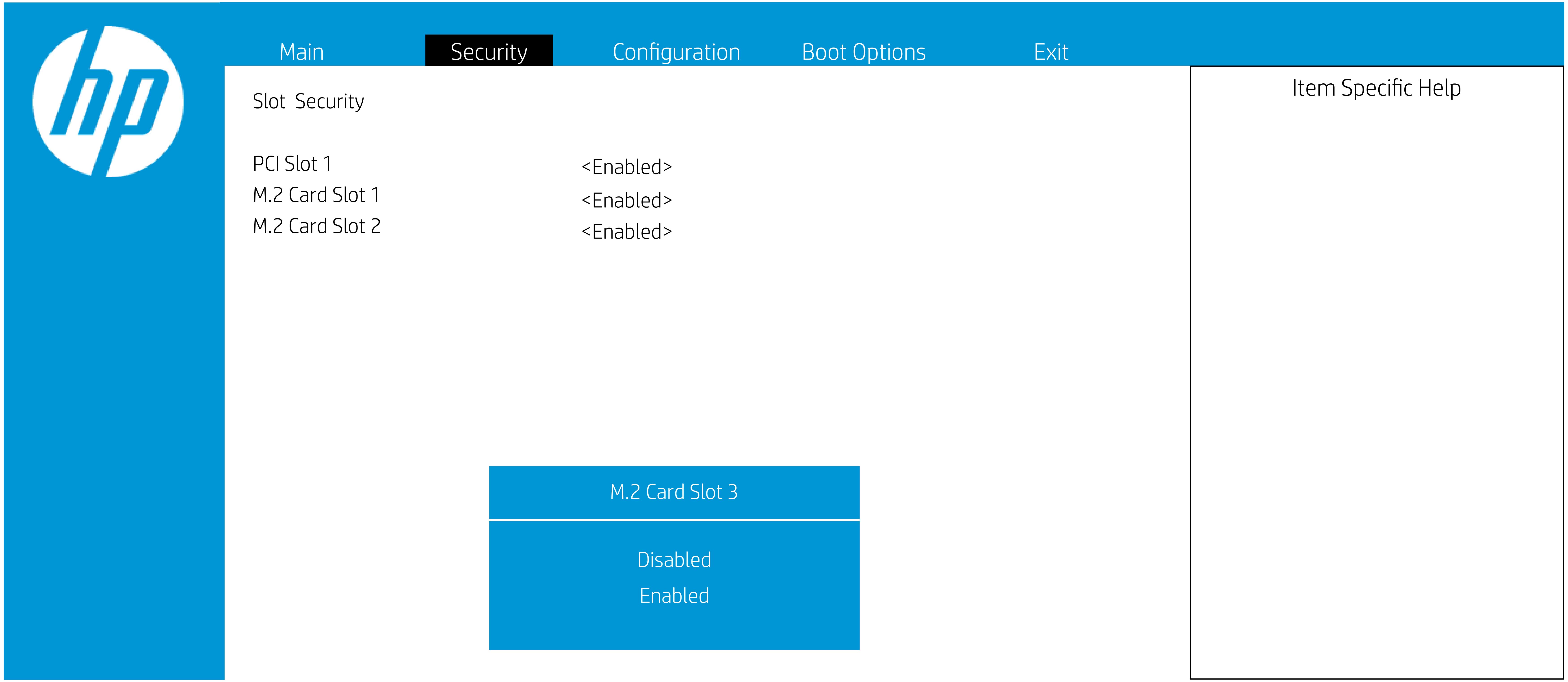
M.2 Card Slot 1 <Enabled>

M.2 Card Slot 2 <Enabled>

Back to Welcome Page

Security Menu

Back to BIOS Utility Menus



Slot Security

PCI Slot 1 <Enabled>

M.2 Card Slot 1 <Enabled>

M.2 Card Slot 2 <Enabled>

M.2 Card Slot 3

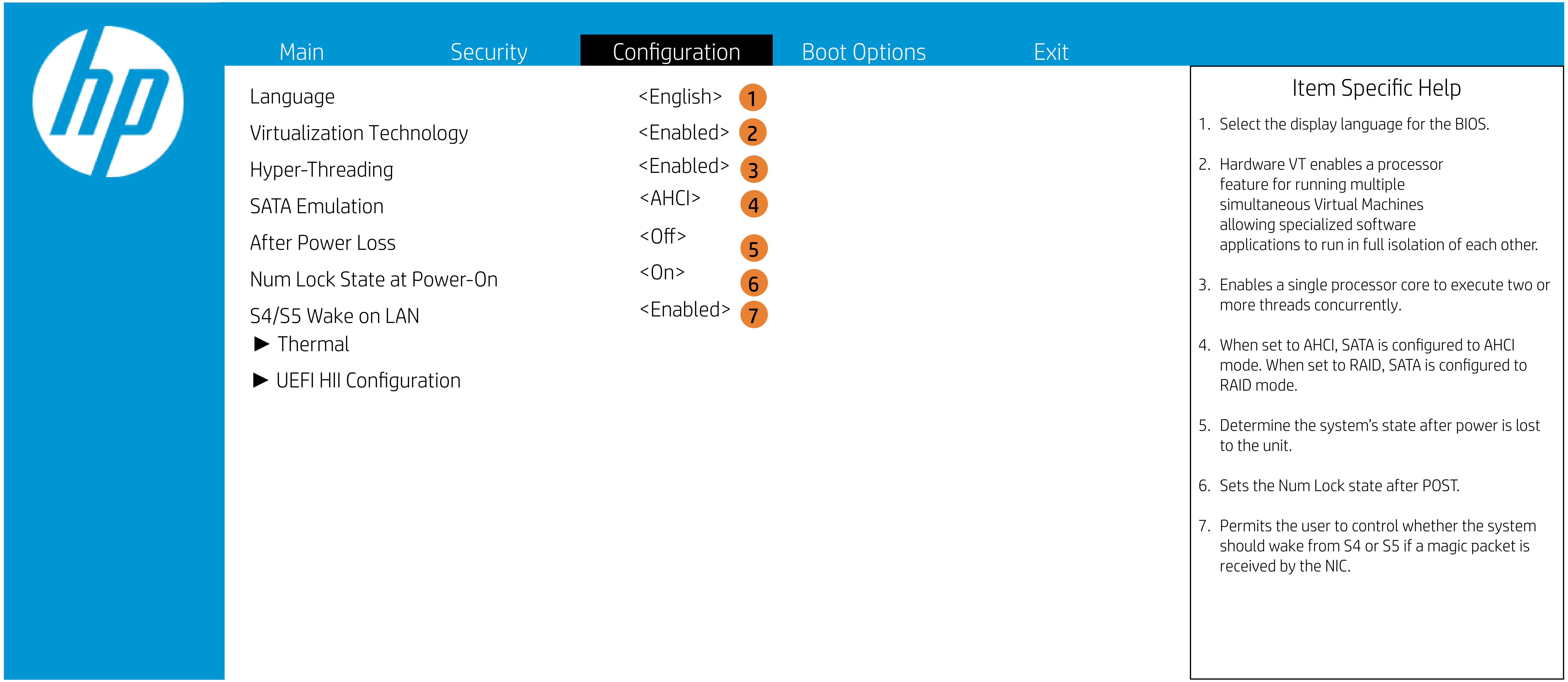
Disabled

Enabled

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



```
Language                          <English>  1
Virtualization Technology         <Enabled>  2
Hyper-Threading                   <Enabled>  3
SATA Emulation                    <AHCI>     4
After Power Loss                  <Off>      5
Num Lock State at Power-On        <On>       6
S4/S5 Wake on LAN                 <Enabled>  7
 ▶ Thermal
 ▶ UEFI HII Configuration
```

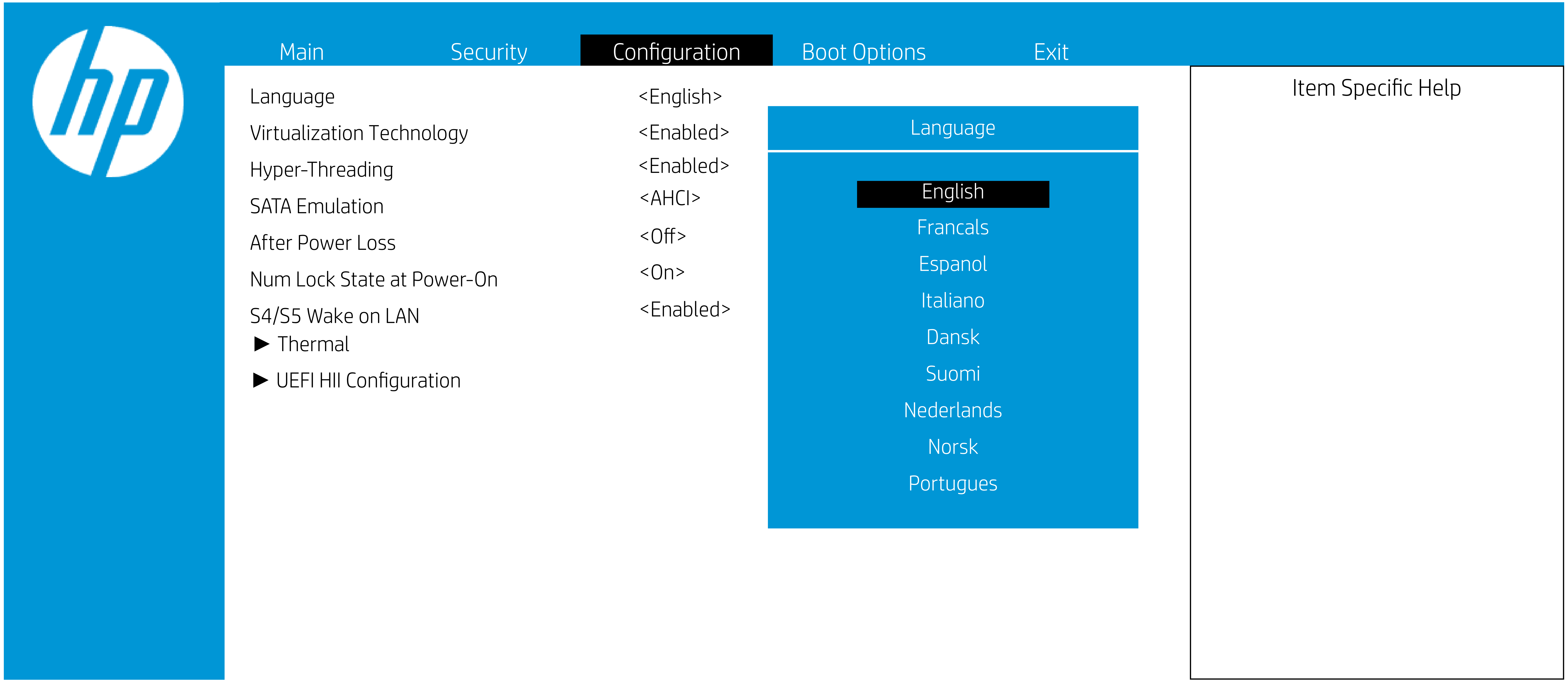
Item Specific Help

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. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
5. Determine the system’s state after power is lost to the unit.
6. Sets the Num Lock state after POST.
7. Permits the user to control whether the system should wake from S4 or S5 if a magic packet is received by the NIC.

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

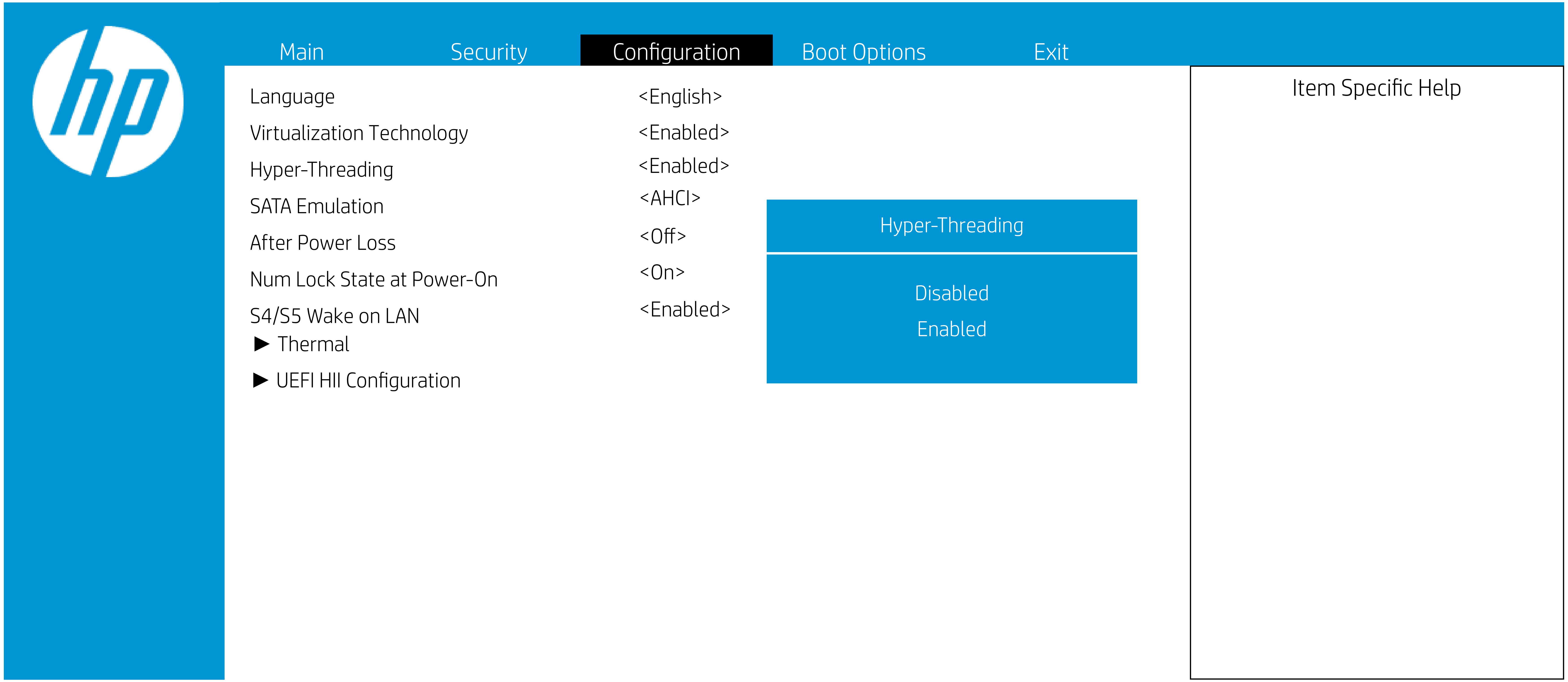


Language	<English>
Virtualization Technology	<Enabled>
Hyper-Threading	<Enabled>
SATA Emulation	<AHCI>
After Power Loss	<Off>
Num Lock State at Power-On	<On>
S4/S5 Wake on LAN	<Enabled>
▶ Thermal	
▶ UEFI HII Configuration	

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language	<English>
Virtualization Technology	<Enabled>
Hyper-Threading	<Enabled>
SATA Emulation	<AHCI>
After Power Loss	<Off>
Num Lock State at Power-On	<On>
S4/S5 Wake on LAN	<Enabled>

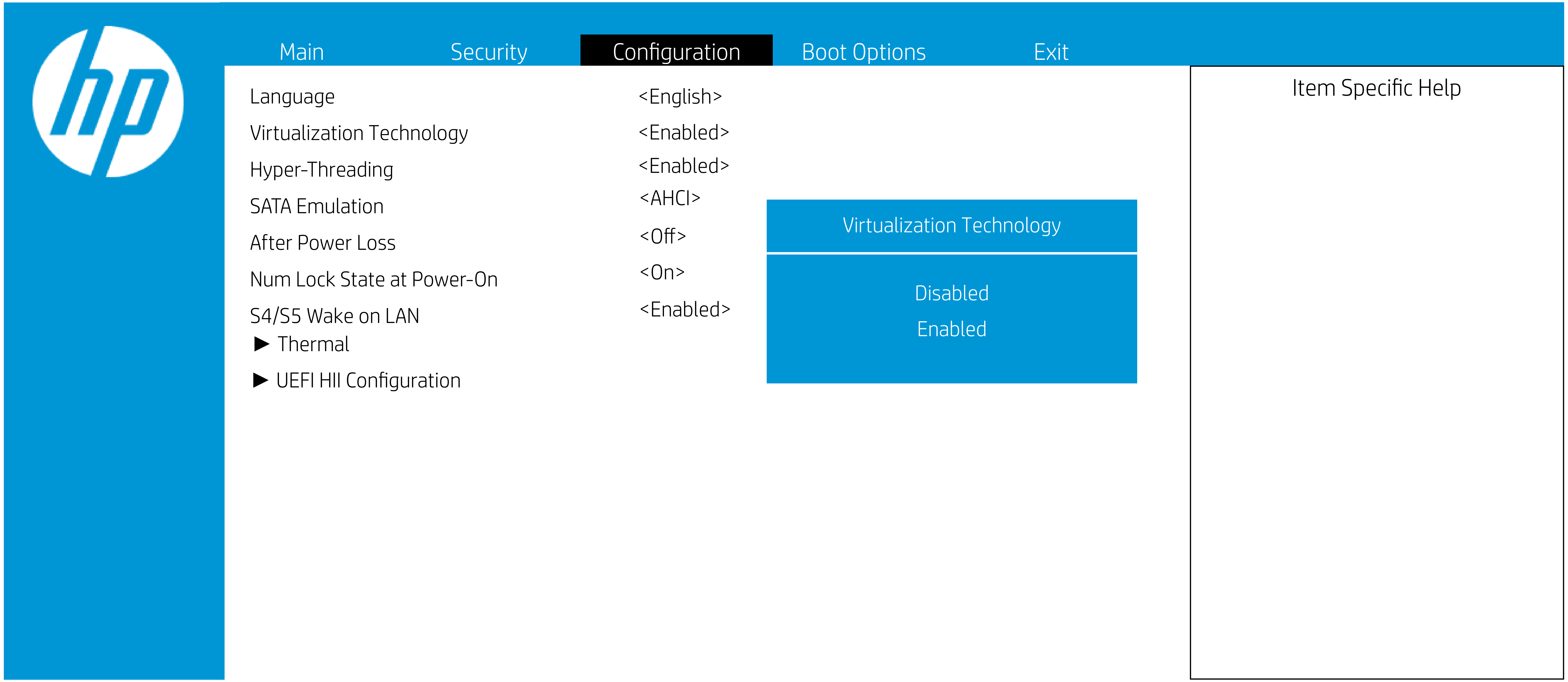
▶ Thermal

▶ UEFI HII Configuration

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

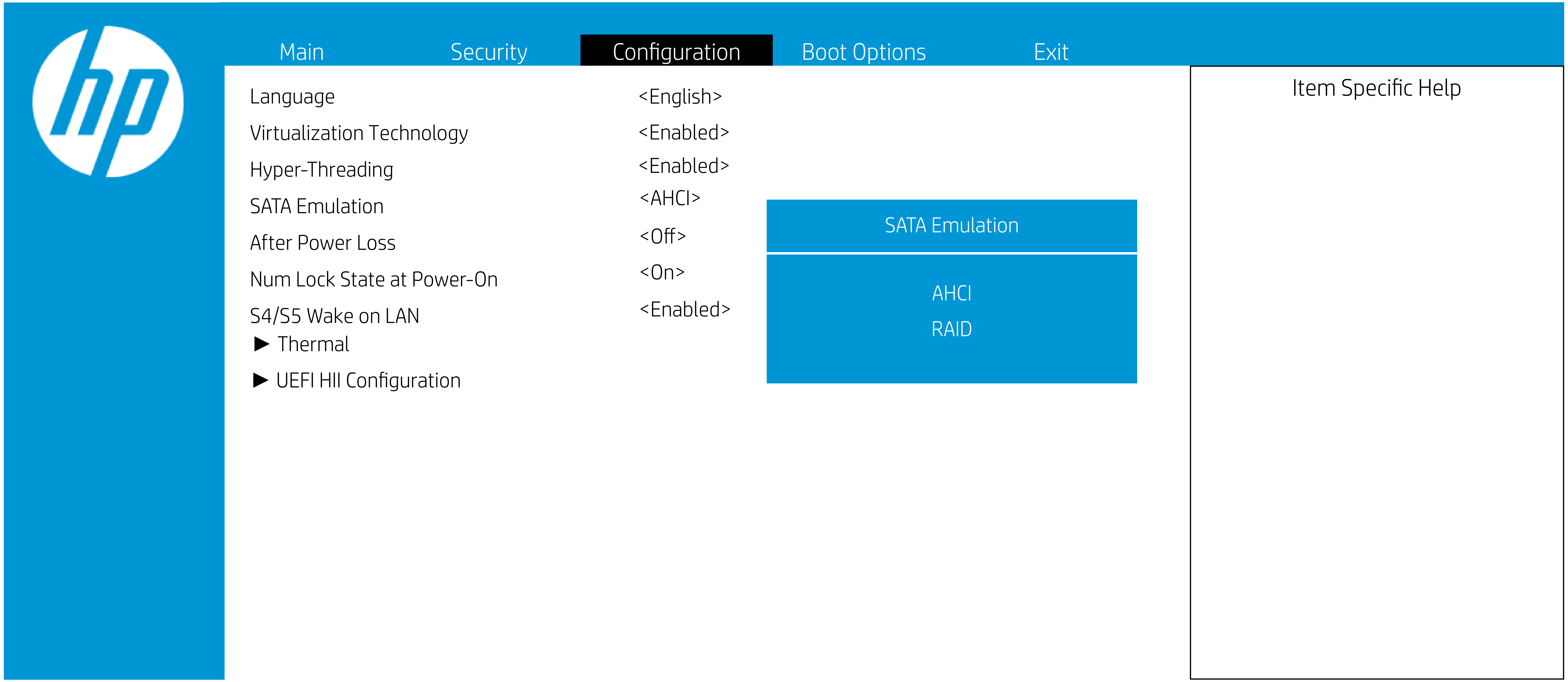


```
Language                          <English>
Virtualization Technology         <Enabled>
Hyper-Threading                   <Enabled>
SATA Emulation                    <AHCI>
After Power Loss                  <Off>
Num Lock State at Power-On        <On>
S4/S5 Wake on LAN                 <Enabled>
▶ Thermal
▶ UEFI HII Configuration
```

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language <English>

Virtualization Technology <Enabled>

Hyper-Threading <Enabled>

SATA Emulation <AHCI>

After Power Loss <Off>

Num Lock State at Power-On <On>

S4/S5 Wake on LAN <Enabled>

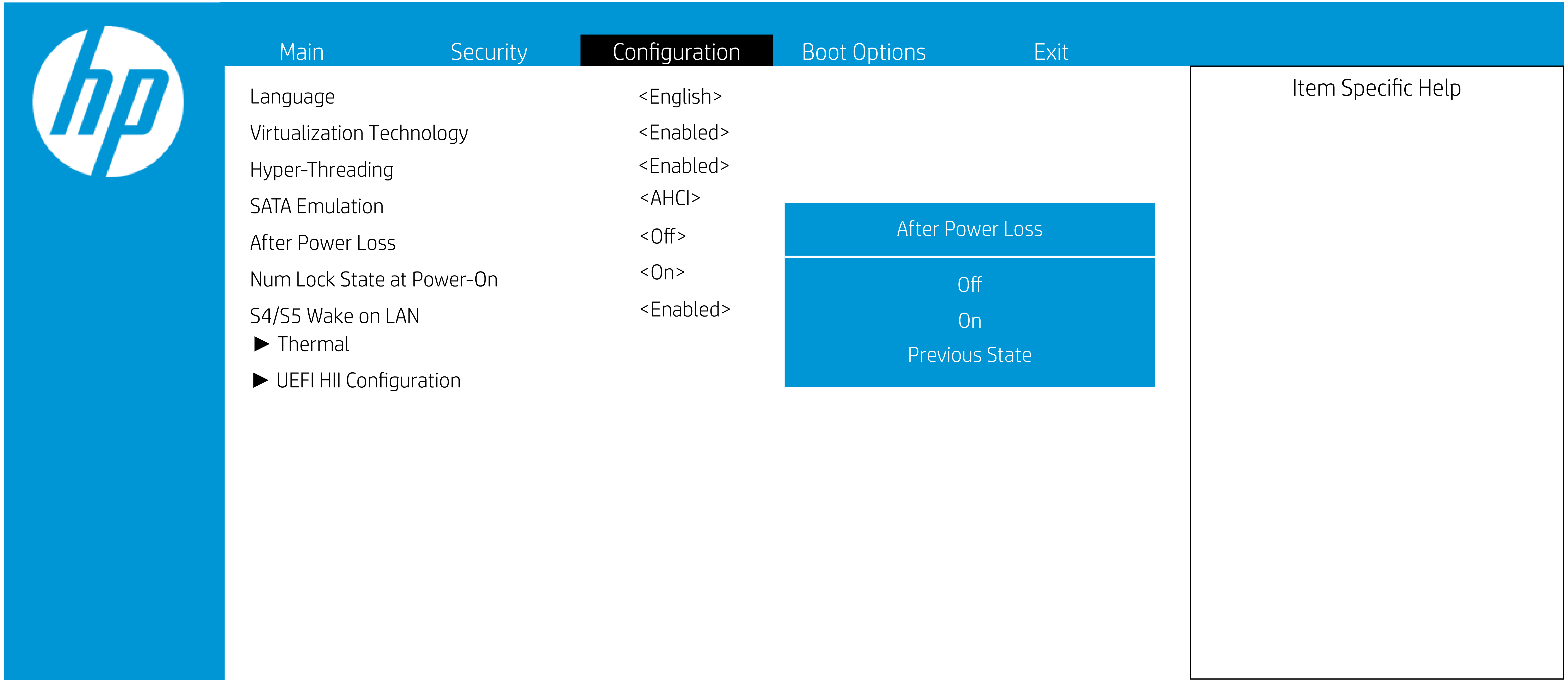
▶ Thermal

▶ UEFI HII Configuration

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

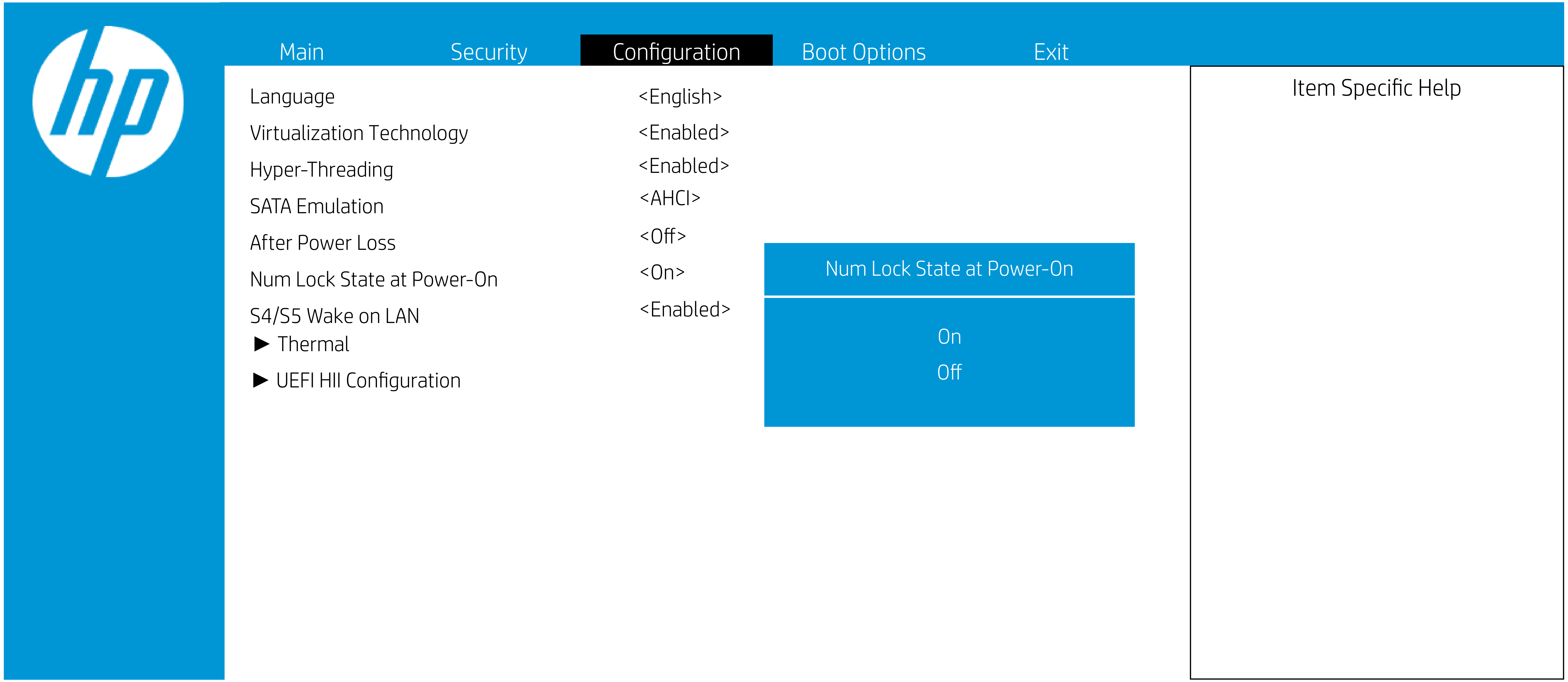


Language	<English>
Virtualization Technology	<Enabled>
Hyper-Threading	<Enabled>
SATA Emulation	<AHCI>
After Power Loss	<Off>
Num Lock State at Power-On	<On>
S4/S5 Wake on LAN	<Enabled>
▶ Thermal	
▶ UEFI HII Configuration	

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus

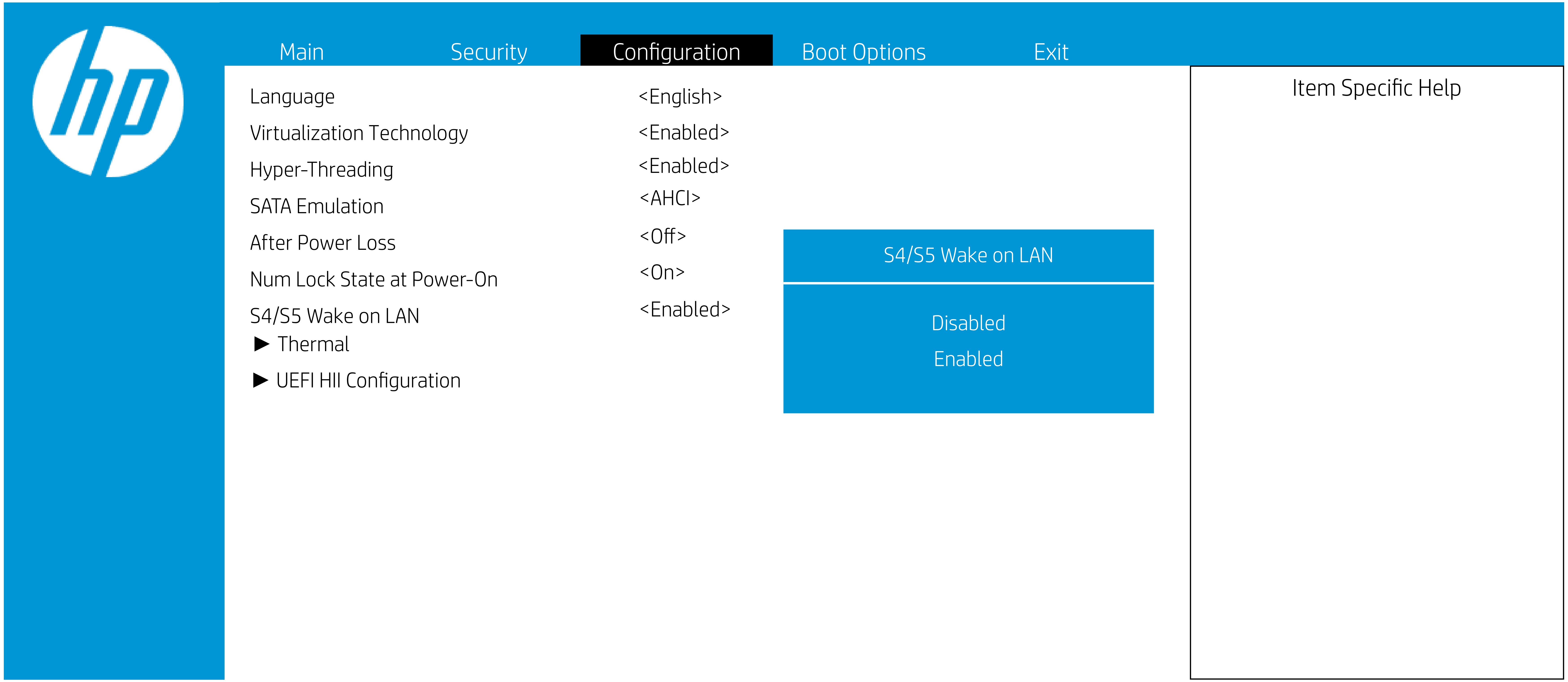


Language	<English>
Virtualization Technology	<Enabled>
Hyper-Threading	<Enabled>
SATA Emulation	<AHCI>
After Power Loss	<Off>
Num Lock State at Power-On	<On>
S4/S5 Wake on LAN	<Enabled>
▶ Thermal	
▶ UEFI HII Configuration	

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



Language <English>

Virtualization Technology <Enabled>

Hyper-Threading <Enabled>

SATA Emulation <AHCI>

After Power Loss <Off>

Num Lock State at Power-On <On>

S4/S5 Wake on LAN <Enabled>

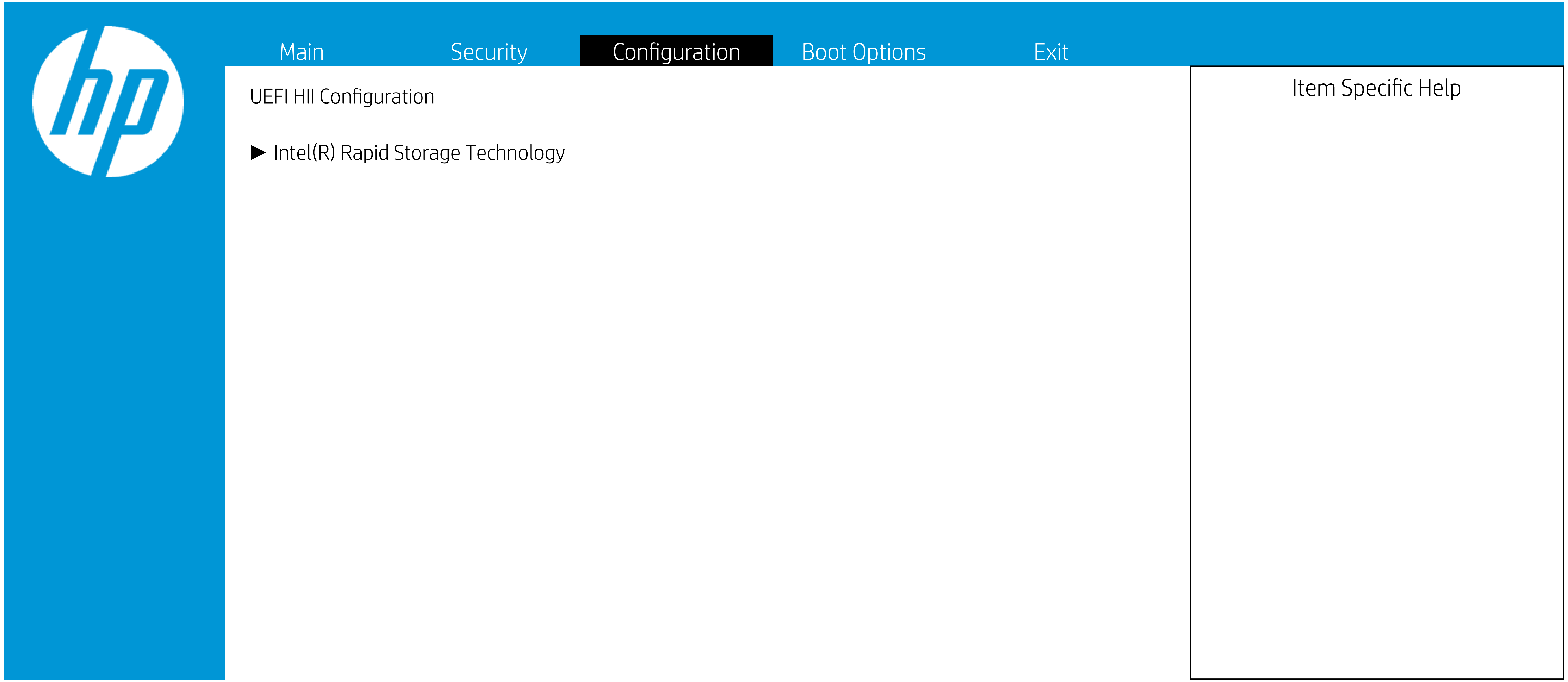
▶ Thermal

▶ UEFI HII Configuration

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



UEFI HII Configuration

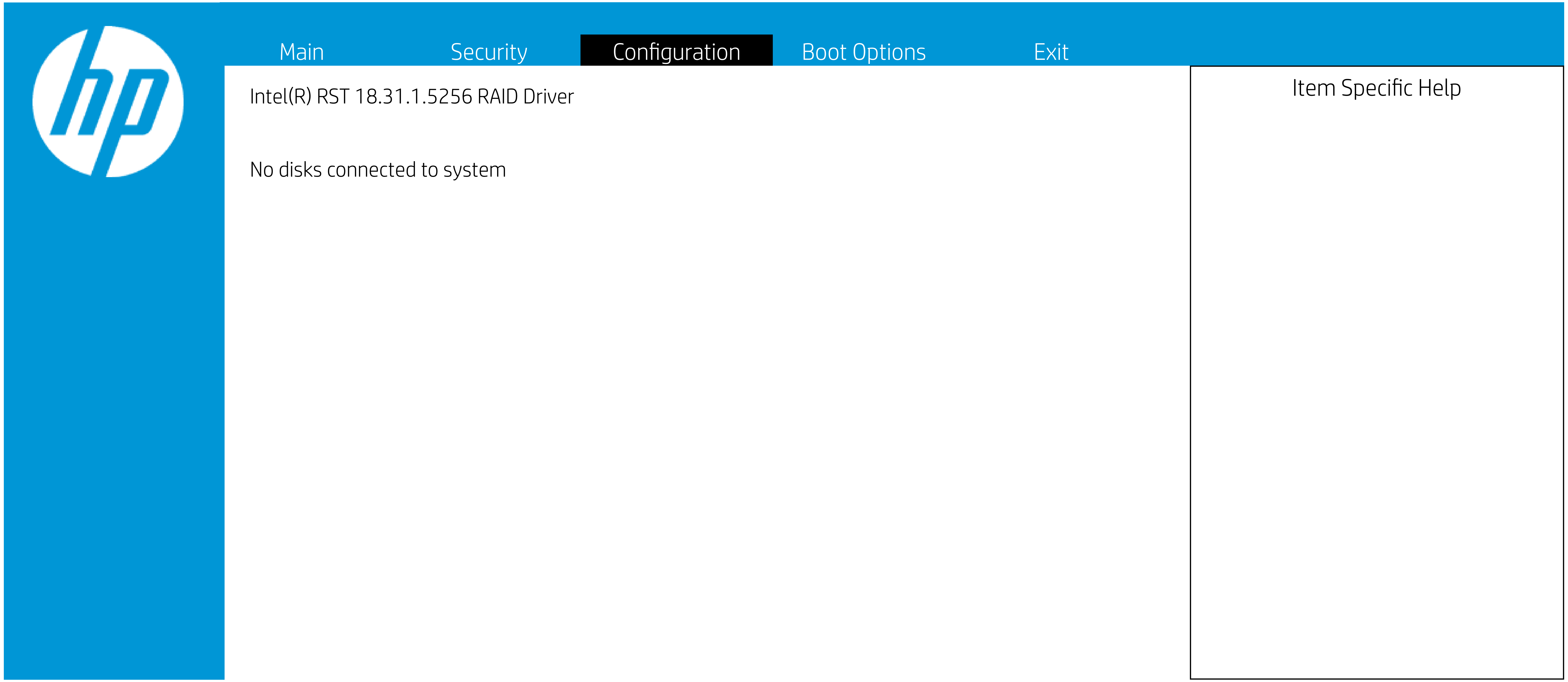
▶ Intel(R) Rapid Storage Technology

Item Specific Help

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



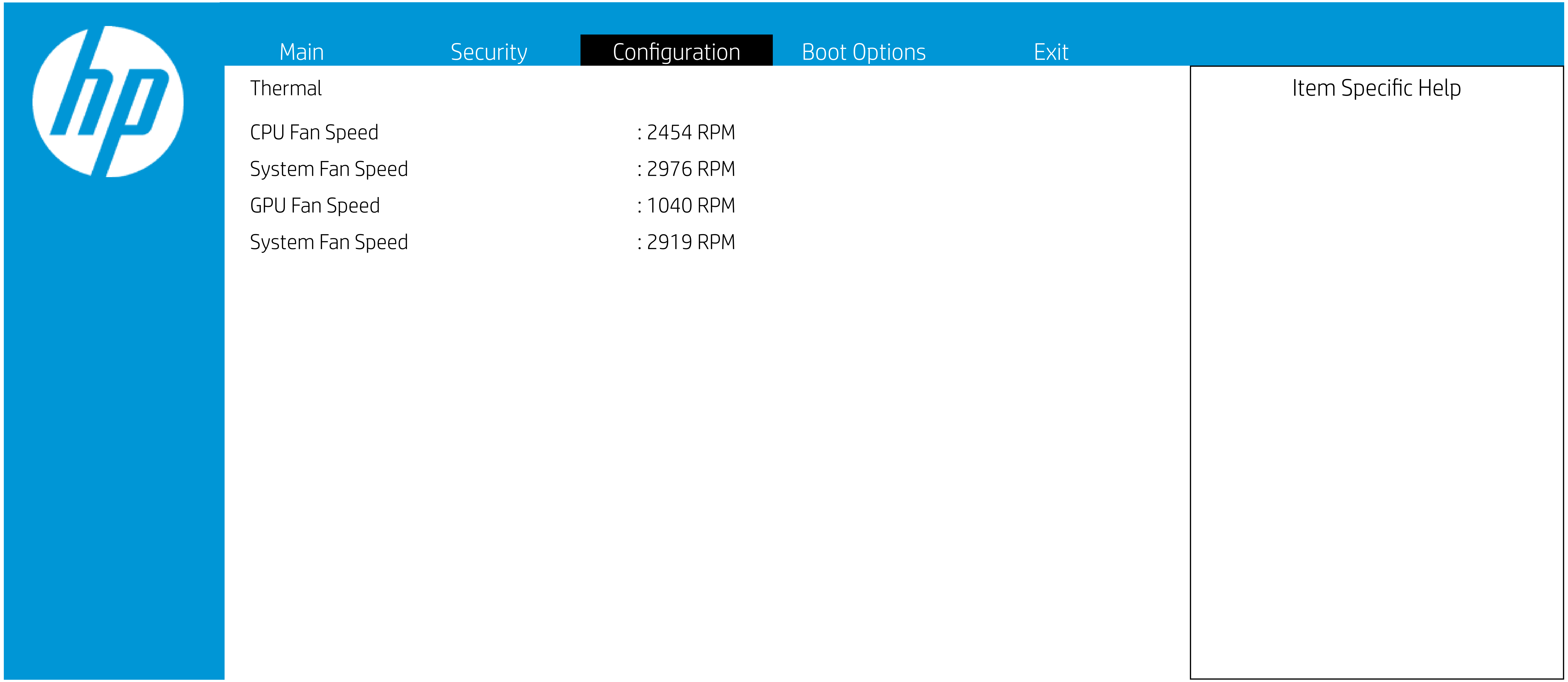
Intel(R) RST 18.31.1.5256 RAID Driver

No disks connected to system

Back to Welcome Page

Configuration Menu

Back to BIOS Utility Menus



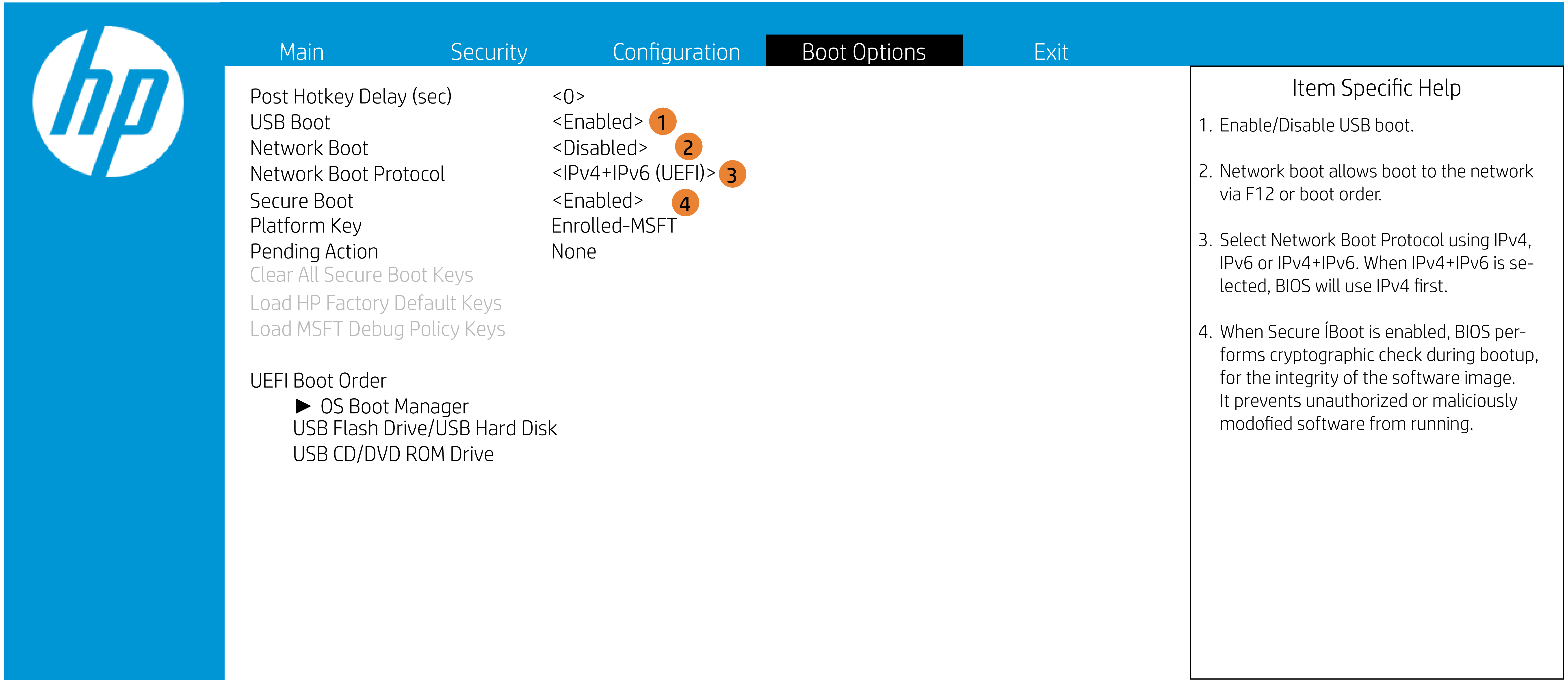
Thermal

```
CPU Fan Speed           : 2454 RPM
System Fan Speed        : 2976 RPM
GPU Fan Speed           : 1040 RPM
System Fan Speed        : 2919 RPM
```

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled>
Network Boot	<Disabled>
Network Boot Protocol	<IPv4+IPv6 (UEFI)>
Secure Boot	<Enabled>
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

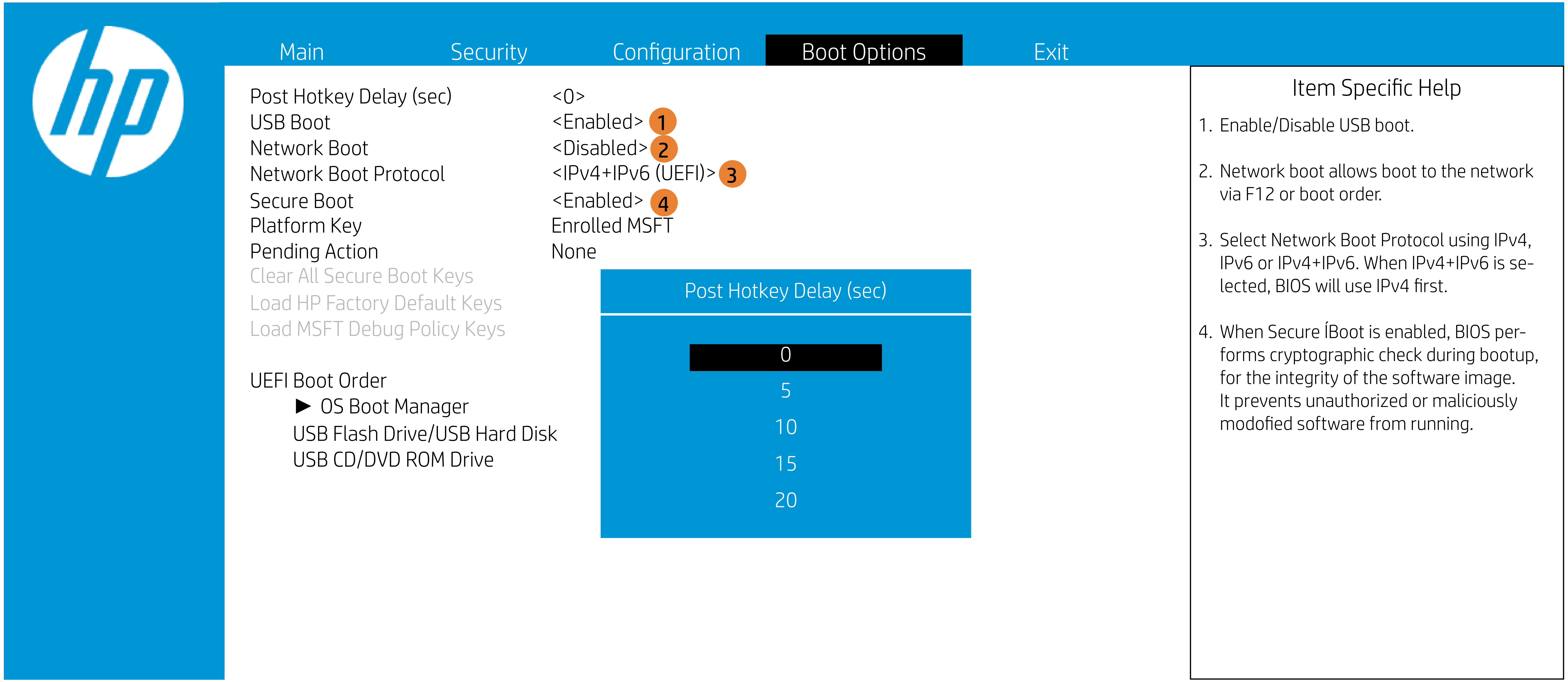
Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec) <0>
USB Boot <Enabled> 1
Network Boot <Disabled> 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

Post Hotkey Delay (sec)
0
5
10
15
20

Item Specific Help

1. Enable/Disable USB boot.

2. Network boot allows boot to the network via F12 or boot order.

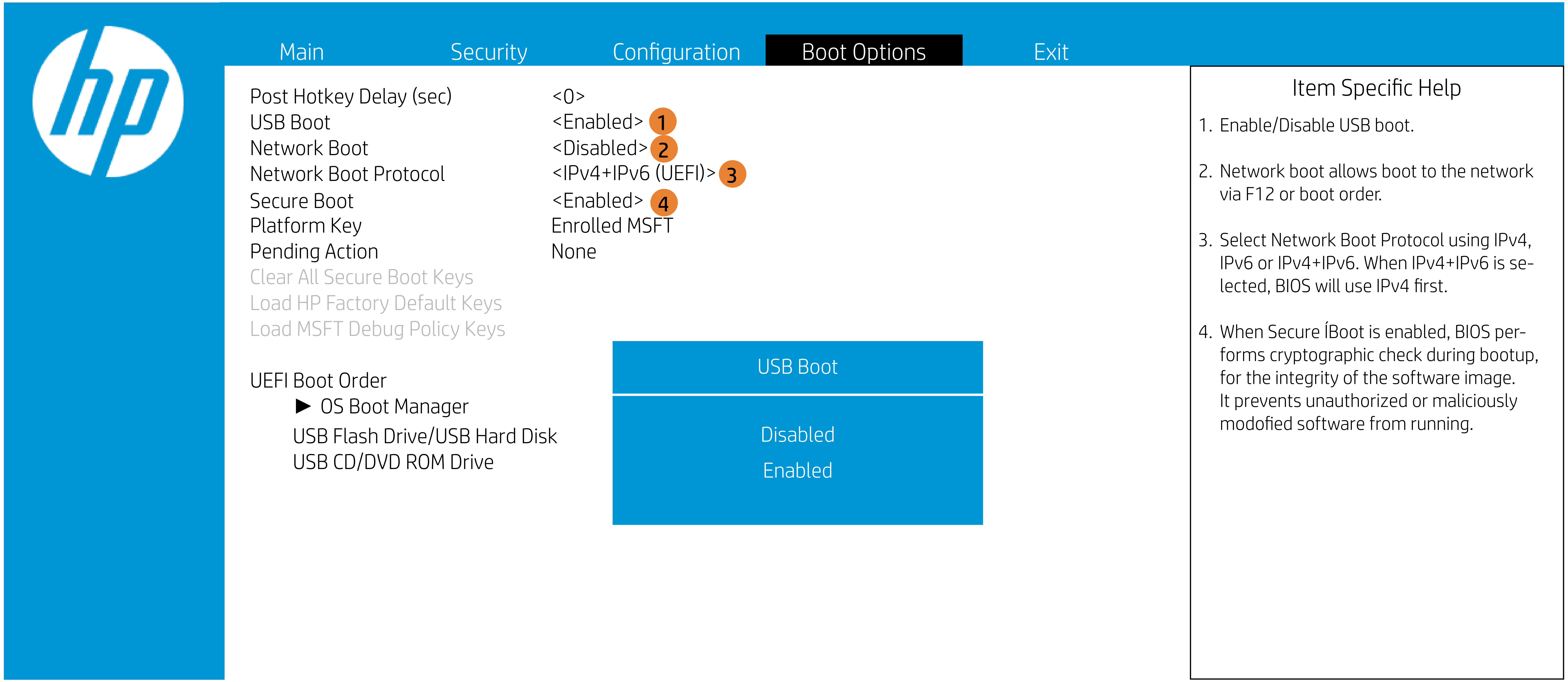
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.

4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Disabled> 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

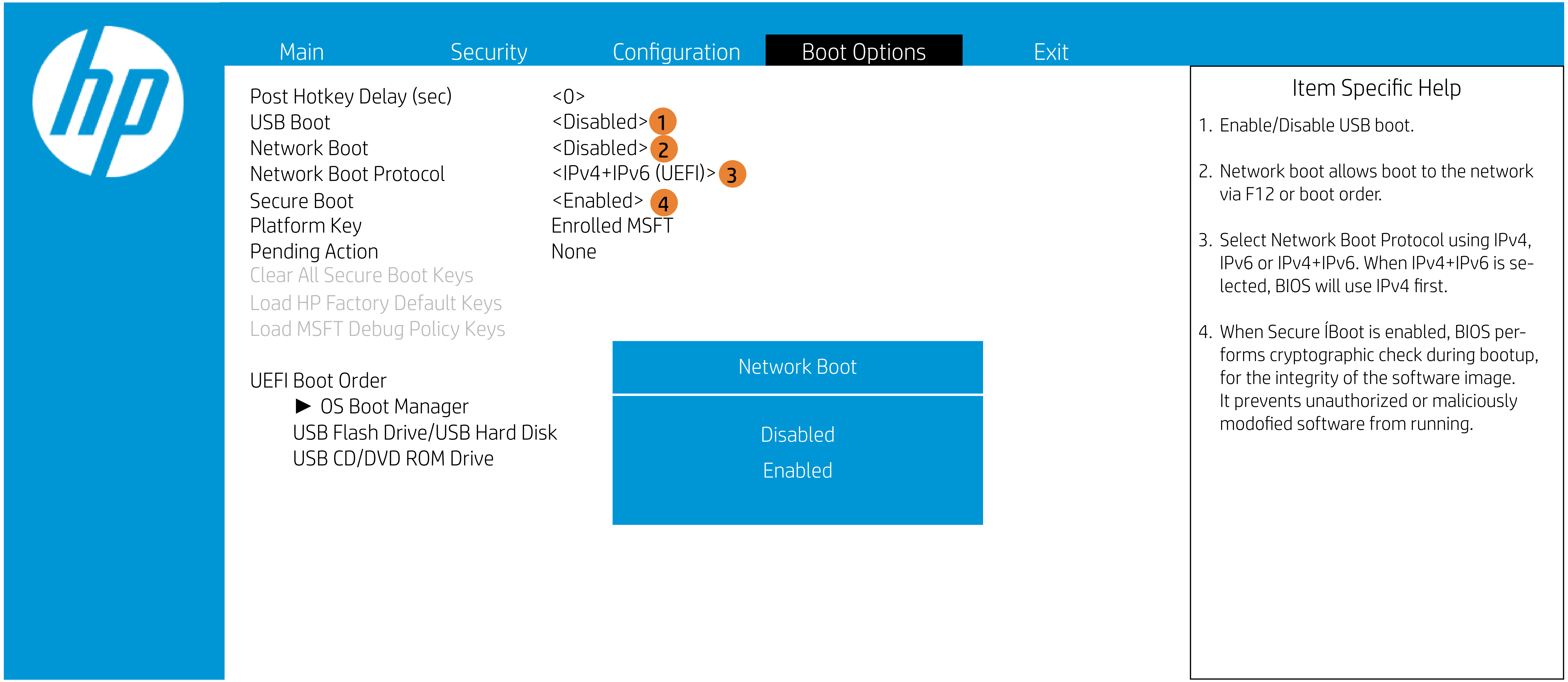
Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec)	<0>
USB Boot	<Disabled> 1
Network Boot	<Disabled> 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

Network Boot

Disabled
Enabled

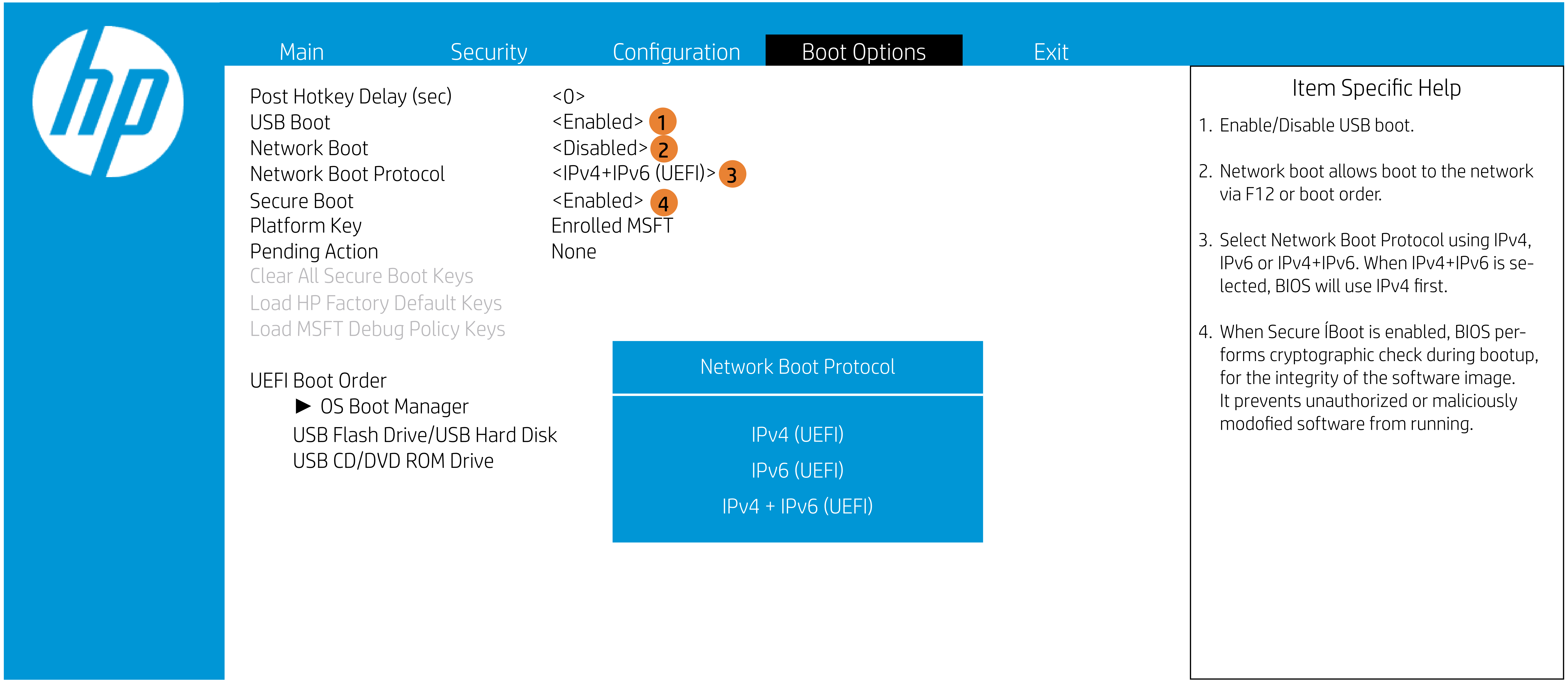
Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec)	<0>
USB Boot	<Enabled> 1
Network Boot	<Disabled> 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

Network Boot Protocol

IPv4 (UEFI)

IPv6 (UEFI)

IPv4 + IPv6 (UEFI)

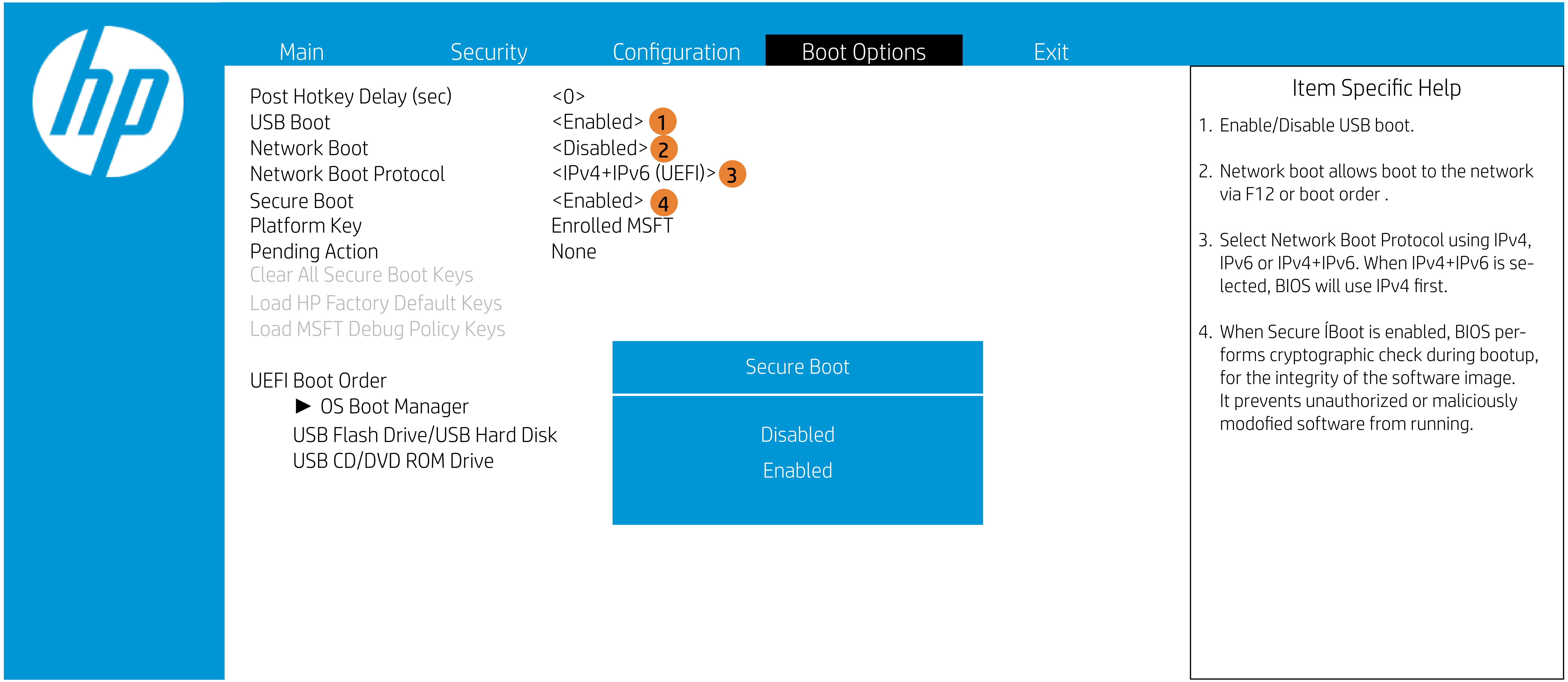
Item Specific Help

1. Enable/Disable USB boot.
2. Network boot allows boot to the network via F12 or boot order.
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.
4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

Back to Welcome Page

Boot Options Menu

Back to BIOS Utility Menus



Post Hotkey Delay (sec) <0>

USB Boot <Enabled> 1

Network Boot <Disabled> 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. Network boot allows boot to the network via F12 or boot order .

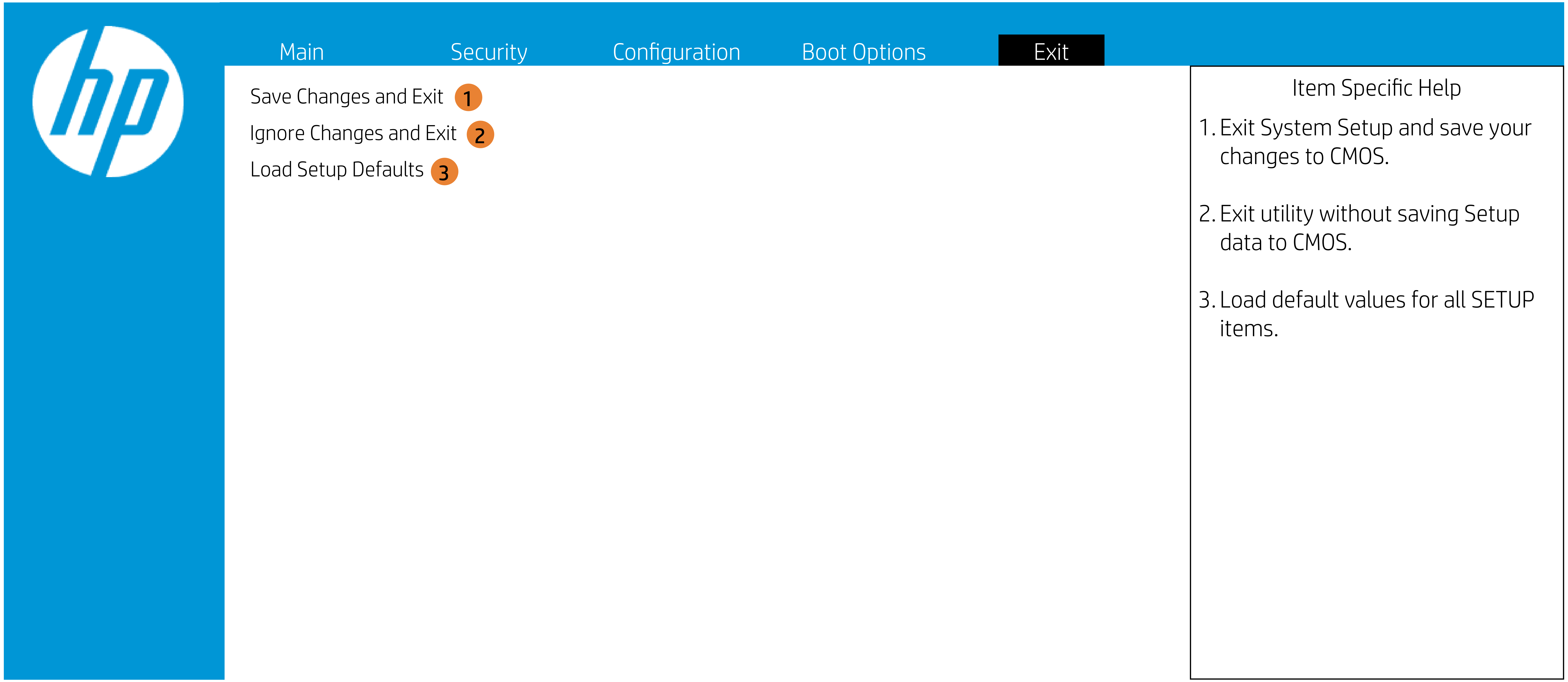
3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.

4. When Secure ÍBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modofied software from running.

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

Item Specific Help

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

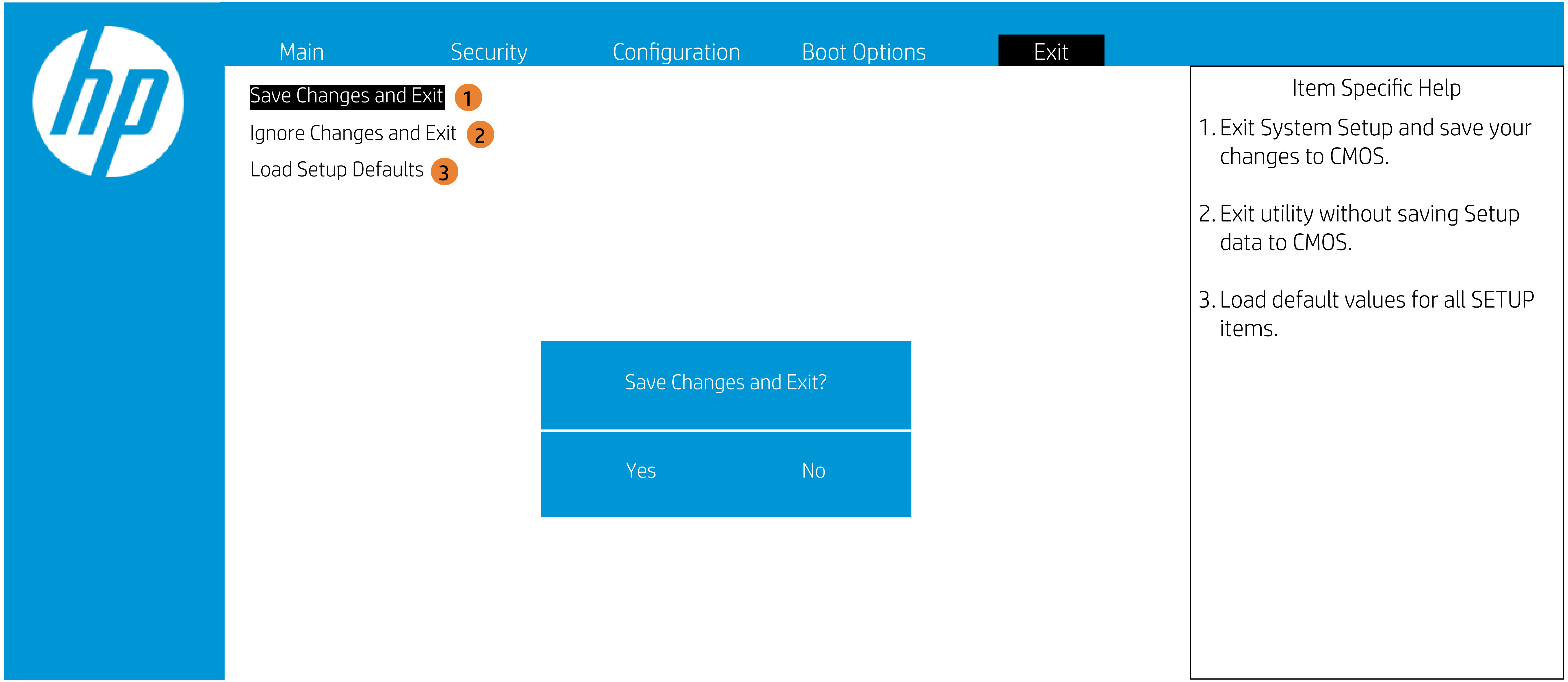
2. Exit utility without saving Setup data to CMOS.

3. Load default values for all SETUP items.

Back to Welcome Page

Exit Menu

Back to BIOS Utility Menus



Save Changes and Exit?

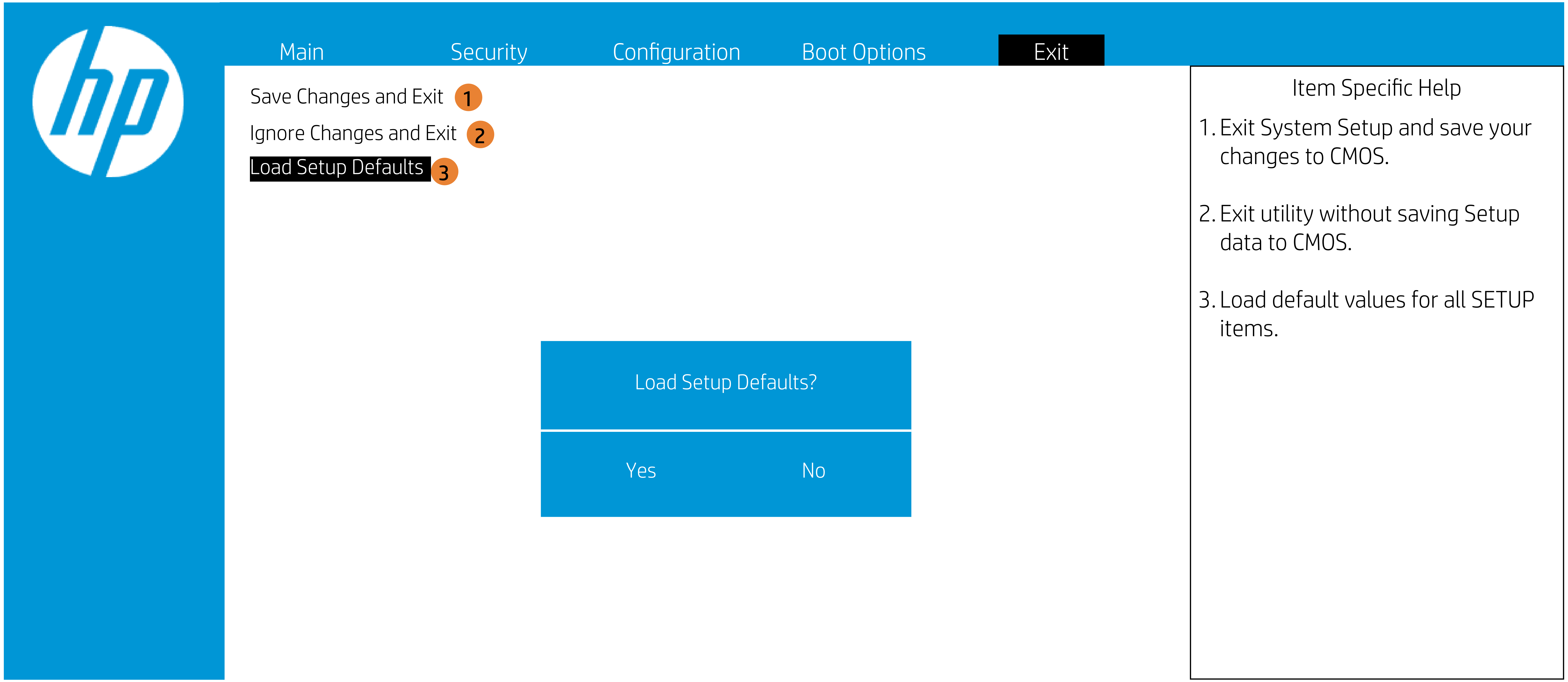
Item Specific Help

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



Load Setup Defaults?

Item Specific Help

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

Back to Welcome Page