## Interactive BIOS simulator

# HP Pavilion Desktop PC

#### Welcome to the interactive BIOS simulator for the HP Pavilion 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**

Main

Security

Configuration

**Boot Options** 

Exit

#### Main Menu



#### Main

System Time System Date Product Name System Family Product Number System Board ID System Board ID Born On Date Processor Type Processor Speed Iotal Memory BIOS Vendor

Serial Number UUID System Board CT Number Factory installed OS

2

1

Build ID Feature Byte [02:08:24] 08/07/2019 HP Pavilion Desktop PC HP Pavilion Desktop PC 6GU13AV 8643 05/13/2019 AMD Ryzen 3 3200G with Rad 3600 MHz 4 GB AMI B.14

HLMW323285 73BB7114-8195-3FF8-6F4B-PHZGRX3CYC9A6A Win10

19WW2HAT6ah#SABA#DABA 2U3E 3K3N 4C6b 7K7M 7T7W aBap aqas aubC bhcb dUdp dqeJ fPkh .yF

	Item Specific Help
	1. Provides firmware revision information of devices built in the system.
	2. View System Log.
deon Vega Graphics	
B-8250828-F9E85	
A	

# Main Menu

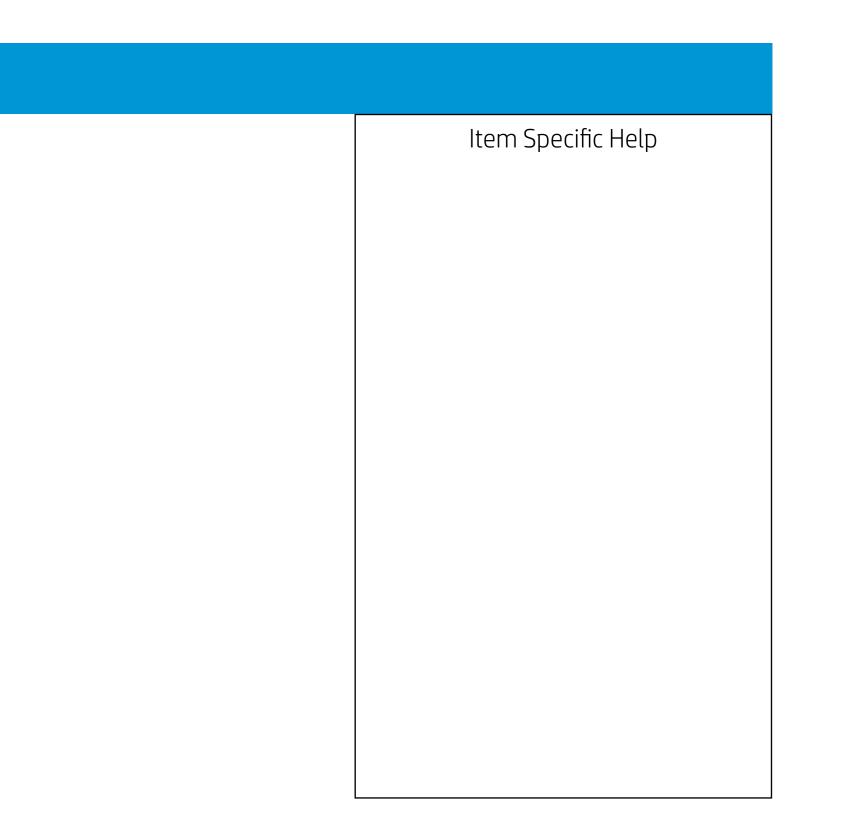


#### Main

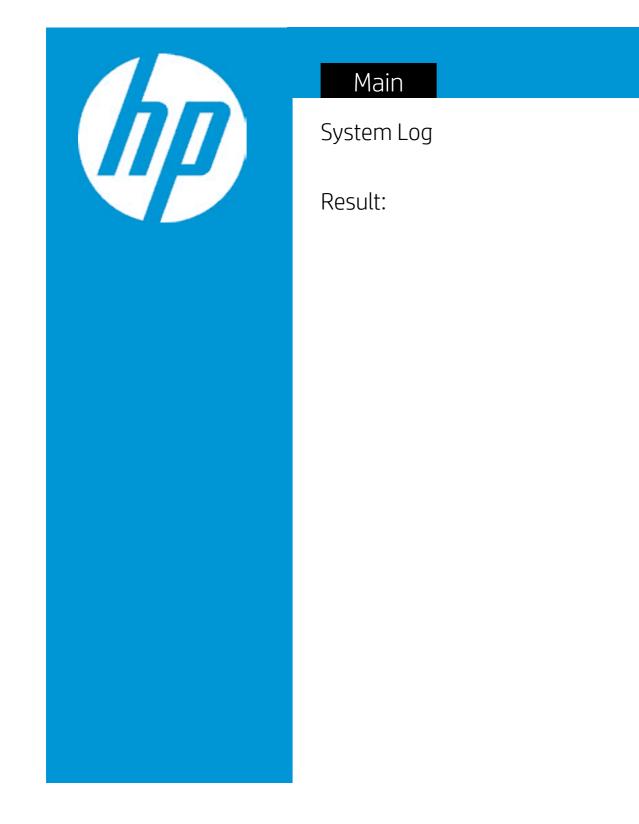
Device Firmware Revision

Embedded Controller	
GOP (Graphic Output Protocol)	
Video BIOS	

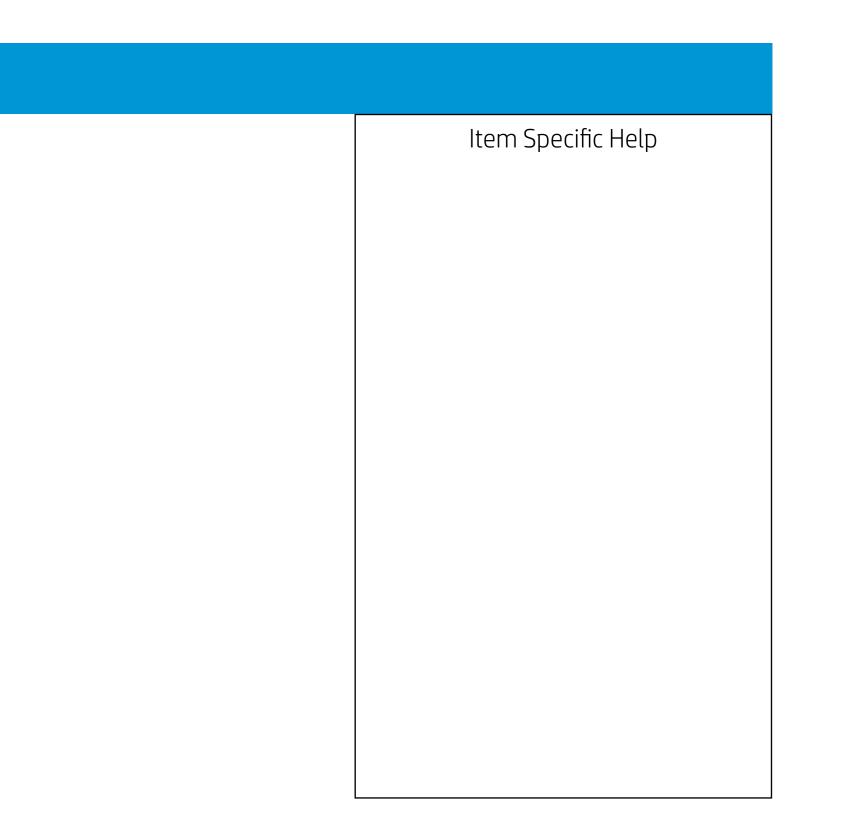
34.18 2.5.0 ATI 113-PICASSO-114



### Main Menu



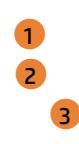
- Time:
- No Data -





#### Security

Administrator Password Power-On Password TPM Device



Item	Specif	fic⊦	lelp
ICCIII	Speen		reip

- 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.

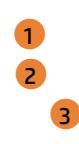
5. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_ Clear to clear the Storage and Endorsement Hierarchy. 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.



#### Security

Administrator Password Power-On Password TPM Device



Item	Specif	fic⊦	lelp
ICCIII	Speen		reip

- 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.

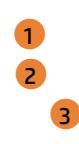
5. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_ Clear to clear the Storage and Endorsement Hierarchy. 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.



#### Security

Administrator Password Power-On Password TPM Device



Item	Specif	fic⊦	lelp
ICCIII	Speen		reip

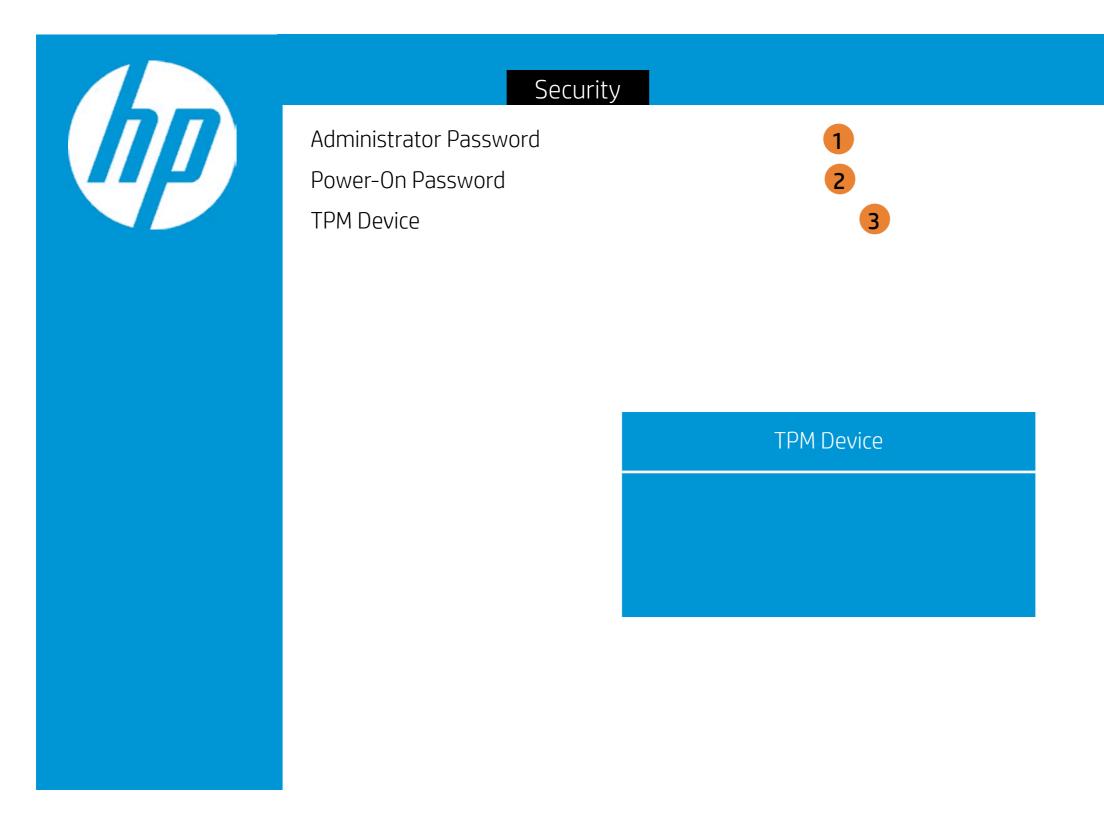
- 1. Administrator Password prevents unauthorized access to the Setup Utilities.
- 2. Power-On Password prevents unauthorized computer system start (boot).
- 3. If the item is set to HIdden, the TPM device is not visible to the operating system.
- 4. If the TPM device setting is set to Hidden, the BIOS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



#### Item Specific Help

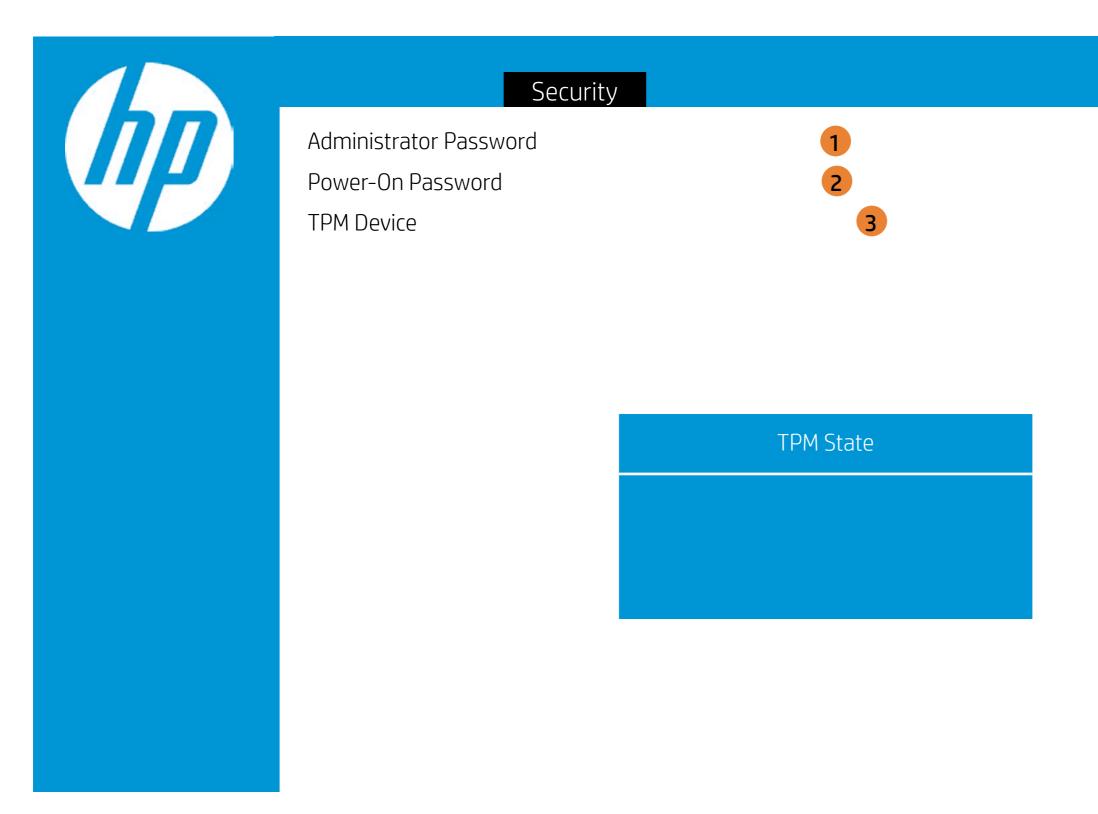
- 1. Administrator Password prevents unauthorized access to the Setup Utilities.
- 2. Power-On Password prevents unauthorized computer system start (boot).
- 3. If the item is set to HIdden, the TPM device is not visible to the operating system.
- 4. If the TPM device setting is set to Hidden, the BIOS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



#### Item Specific Help

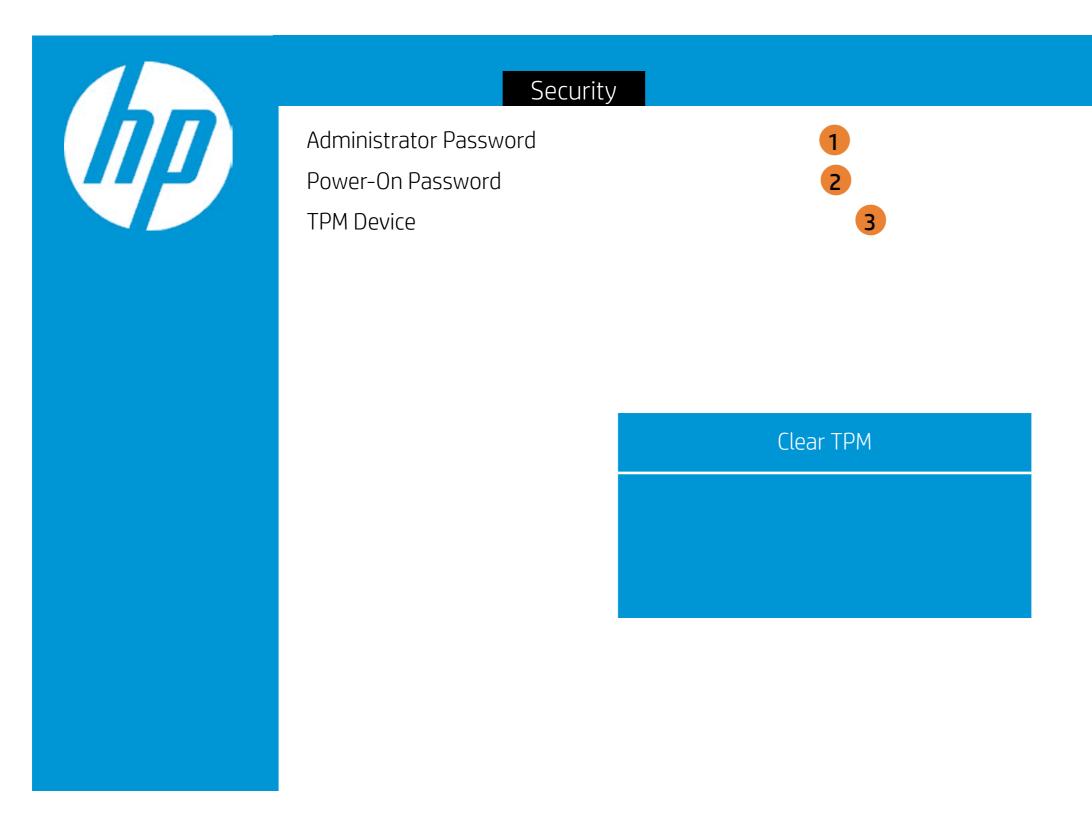
- 1. Administrator Password prevents unauthorized access to the Setup Utilities.
- 2. Power-On Password prevents unauthorized computer system start (boot).
- 3. If the item is set to HIdden, the TPM device is not visible to the operating system.
- 4. If the TPM device setting is set to Hidden, the BIOS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



#### 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.

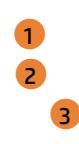
5. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_ Clear to clear the Storage and Endorsement Hierarchy. 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.



#### Security

Administrator Password Power-On Password TPM Device



Item	Specif	fic⊦	lelp
ICCIII	Speen		reip

- 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.



	Configuration	
nguage	1	
rtualization Technology	2	
57	3	
um Lock State at Power-On		
I/S5 Wake on Lan	4	
5		

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. Sets the Num Lock state after POST.
4. Permits the user to control wheth- er the system should wake from S4 or S5 if a magic packet is re- ceived by the NIC
5. Provides thermal/FAN status of the system.



	Configuration
Language	1
Virtualization Technology	2
Num Lock State at Power-On	3
S4/S5 Wake on Lan	4
5	
	Language

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. Sets the Num Lock state after POST.
4. Permits the user to control wheth- er the system should wake from S4 or S5 if a magic packet is re- ceived by the NIC
5. Provides thermal/FAN status of the system.



	Configuration
Language	1
Virtualization Technology	2
Num Lock State at Power-On	3
S4/S5 Wake on Lan	4
5	

Virtualizatiion Technology

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. Sets the Num Lock state after POST.
4. Permits the user to control wheth- er the system should wake from S4 or S5 if a magic packet is re- ceived by the NIC
5. Provides thermal/FAN status of the system.



	Configuration
Language	1
Virtualization Technology	2
Num Lock State at Power-On	3
S4/S5 Wake on Lan	4
5	

Num Lock State at Power-On

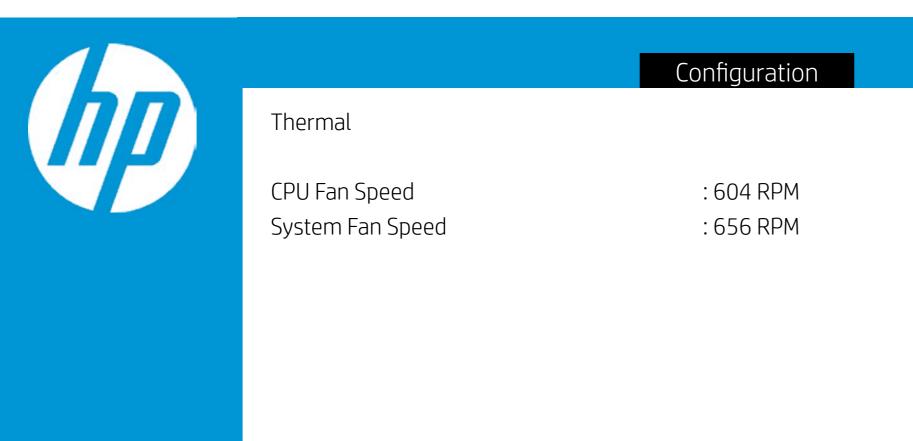
Item Specific Help
1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets the Num Lock state after POST.
4. Permits the user to control wheth- er the system should wake from S4 or S5 if a magic packet is re- ceived by the NIC
5. Provides thermal/FAN status of the system.

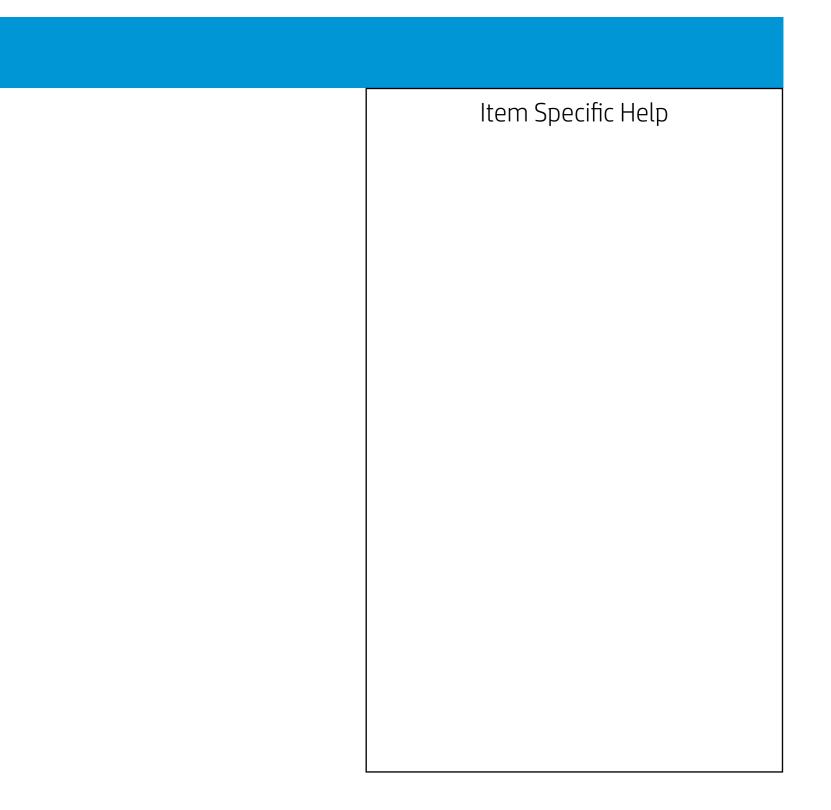


	Configuration
Language	1
Virtualization Technology	2
Num Lock State at Power-On	3
S4/S5 Wake on Lan	4
5	

S4/S5 Wake on Lan

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. Sets the Num Lock state after POST.
4. Permits the user to control wheth- er the system should wake from S4 or S5 if a magic packet is re- ceived by the NIC
5. Provides thermal/FAN status of the system.







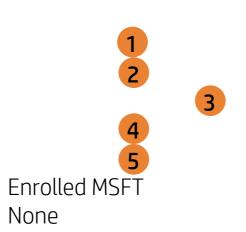
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



Boot Options	
Boot Options	<ol> <li>Item Specific Help</li> <li>Enable/Disable USB boot.</li> <li>Enable/Disable network boot during boot time.</li> <li>Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.</li> <li>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.</csm></li> <li>Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.</li> </ol>



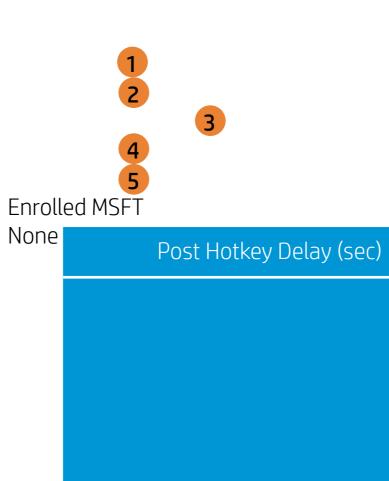
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



Boot Options	
	Item Specific Help
	1. Enable/Disable USB boot.
	2. Enable/Disable network boot during boot time.
Delay (sec)	3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, 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 sup- port newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.</csm>
	5. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.



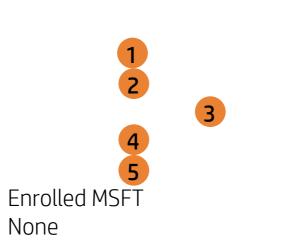
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



USB Boot

Boot Options	
Boot Options	Item Specific Help1. Enable/Disable USB boot.2. Enable/Disable network boot during boot time.3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.4. When Legacy Support Is enabled. BIOS will load Compatibility Support Module <csm> to support Legacy OS such as Windows</csm>
	7. Windows Vista. Windows XP und DOS. When legacy Support is disabled. BIOS will boot in UEFI Mode without CSM to sup- port 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.



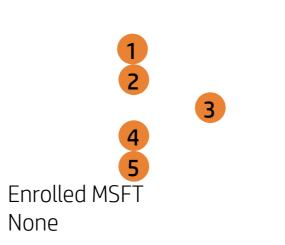
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



Network Boot

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



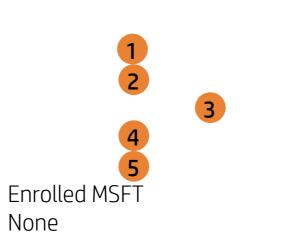
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ▶ Internal Hard Drive Internal CD/DVD ROM Drive



Network Boot Protoco

Boot Options	
Boot Options	Item Specific Help1. Enable/Disable USB boot.2. Enable/Disable network boot during boot time.3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.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 sup- port 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.</csm>



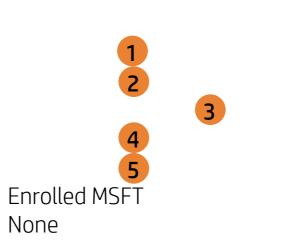
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



Legacy Support

Boot Options	
Bool Options	Item Specific Help 1. Enable/Disable USB boot. 2. Enable/Disable network boot during boot
	<ol> <li>2. Enable/Disable network boot during boot time.</li> <li>3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is selected, BIOS will use IPv4 first.</li> </ol>
/ Support	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 sup- port newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.</csm>
	5. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.



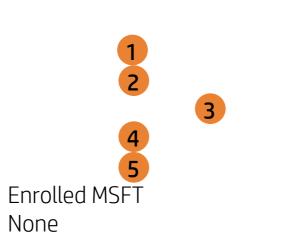
Post Hotkey Delay (sec) USB Boot Network Boot Network Boot Protocol Legacy Support

Platform Key Pending Action

Load HP Factory Default Keys Load MSFT Debug Policy Keys

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

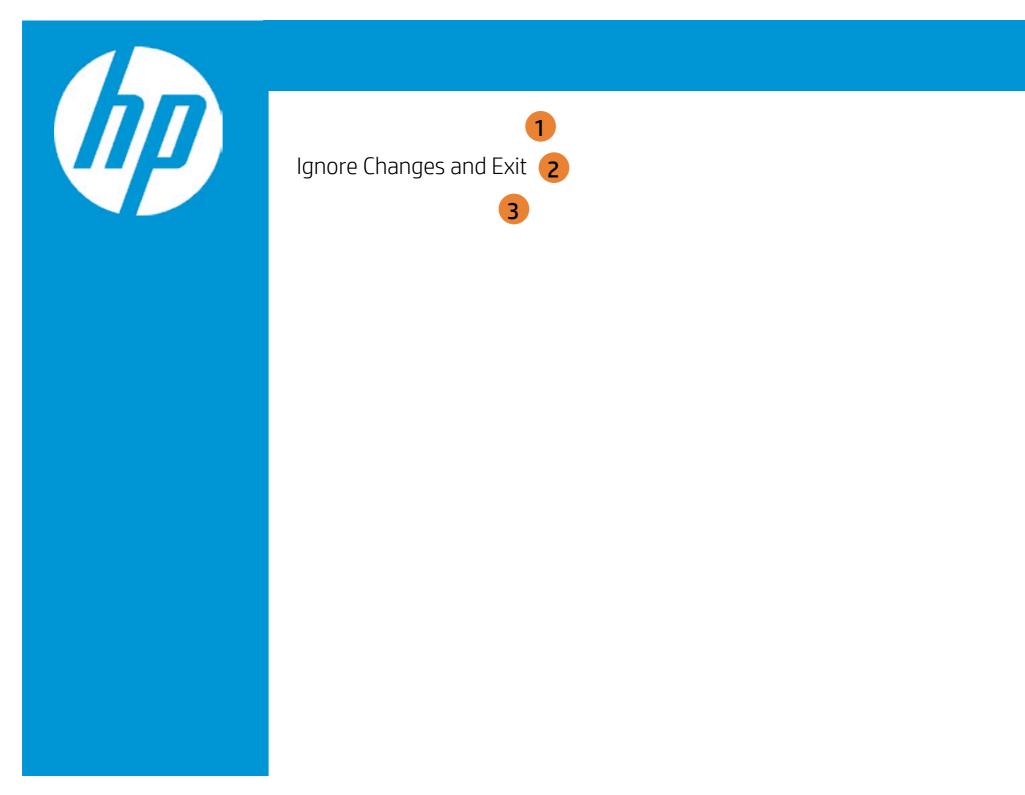
Legacy Boot Order ► Internal Hard Drive Internal CD/DVD ROM Drive



Secure Boot

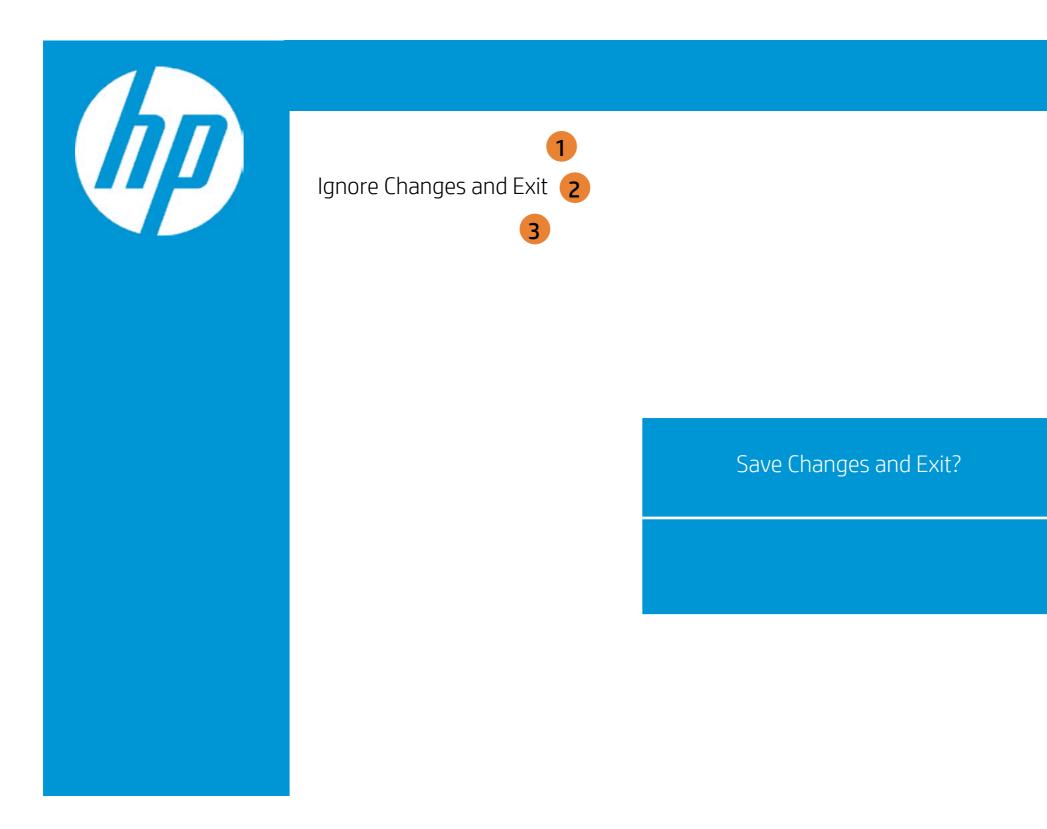
Root Options	
Boot Options	Item Specific Help 1. Enable/Disable USB boot. 2. Enable/Disable network boot during boot time.
	3. Select Network Boot Protocol using IPv4, IPv6 or IPv4+IPv6. When IPv4+IPv6 is se- lected, BIOS will use IPv4 first.
re Boot	4. When Legacy Support Is enabled. BIOS will load 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 sup- port newer OS such as Windows 8. System might be unable to boot Into operating system after changing this setting.</csm>
	5. Secure Boot flow control. Secure Boot is possible only if System runs in User Mode.

## Exit Menu



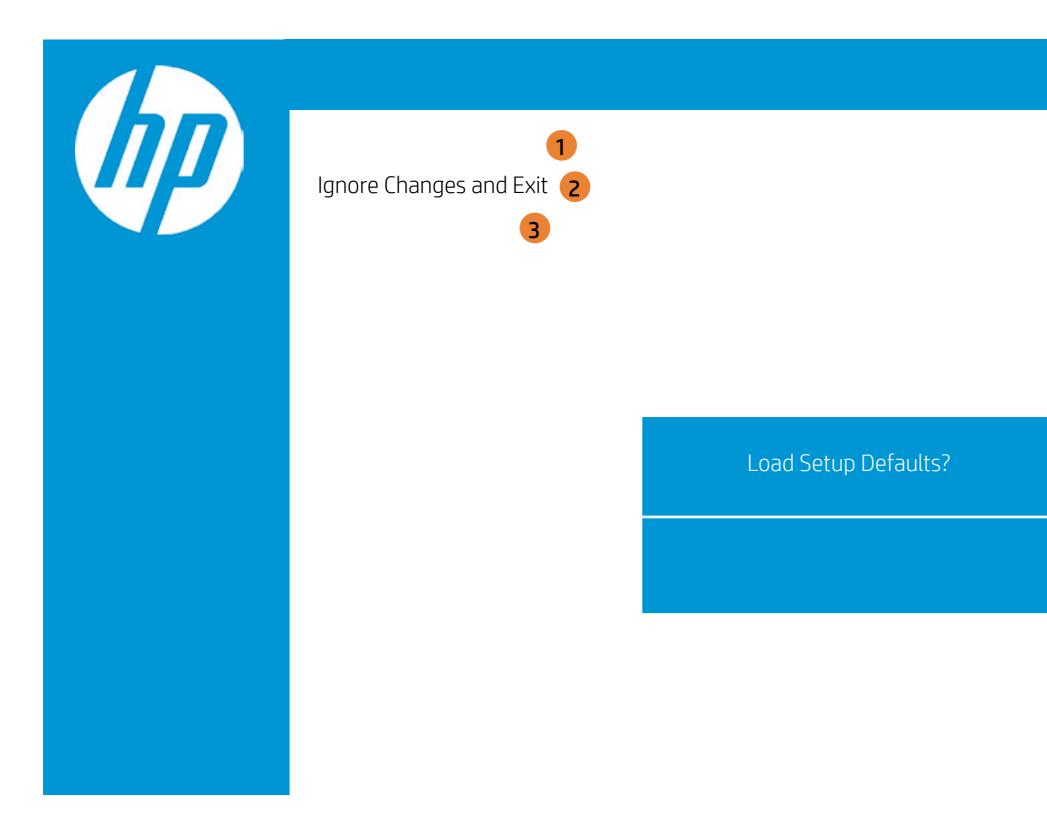
Exit	
	Item Specific Help
	1. Exit System Setup and save your changes to CMOS.
	2. Exit utility without saving Setup data to CMOS.
	3. Load default values for all SETUP items.

### Exit Menu



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

### Exit Menu



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