

# Interactive BIOS simulator

## HP 22/24/27 All-in-One PC

Welcome to the interactive BIOS simulator for the  
HP 22/24/27 All-in-One 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	[22:02:59]
System Date	12/18/2019
Product Name	HP All-in-One
System Family	HP HP Bibury
Product Number	N17PVTB#01
System Board ID	86F8
Born On Date	00/00/0000
Processor Type	Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz
Total Memory	16 GB
BIOS Vendor	AMI
BIOS Version	B.10
Serial Number	8C94327RV
UUID	3B911C82-6D0D-3FD5-A4FA-F3164DF
System Board CT Number	PJHVA0A8JCW04M
Factory installed OS	Win10
Build ID	20WW1BIT6ag#SABA#DABA
Feature Byte	2U3E 3K3N 3Q4h 6b7K 7P7Q 7S7W 7saB apaq asbC bhcb dUdp dqeV fPkv kZm9 .n7

1

2

### Item Specific Help

1. Provides firmware revision information of devices built in the system.
2. View System Log.

# Main Menu



## Main

Device Firmware Revision

Embedded Controller	39.14
Intel ME (Management Engine)	12.0.40.1433
GOP (Graphic Output Protocol)	9.0.1086

Item Specific Help

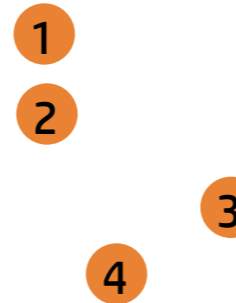


# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



## Item Specific Help

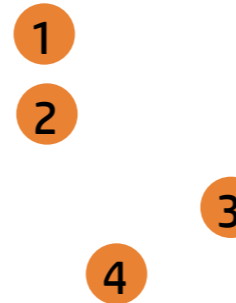
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



## Item Specific Help

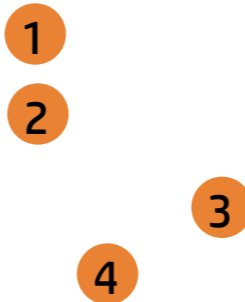
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



## Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

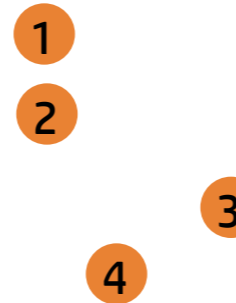


# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



### Intel Software Guard Extensions (SGX)

### Item Specific Help

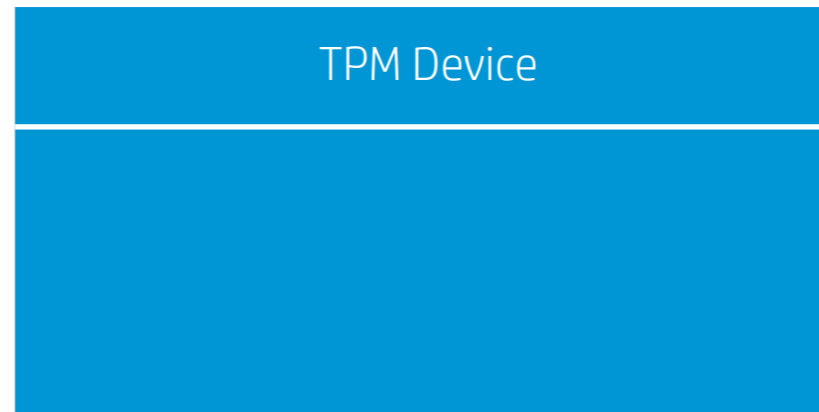
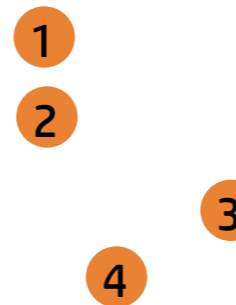
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



## Item Specific Help

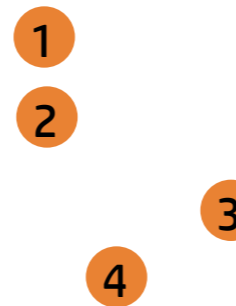
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



### TPM State

## Item Specific Help

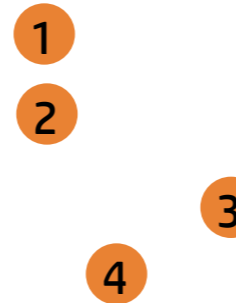
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



Clear TPM

## Item Specific Help

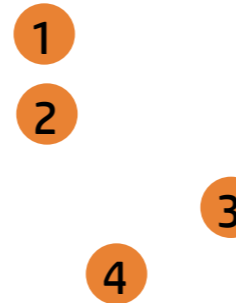
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Security Menu



## Security

- Administrator Password
- Power-On Password
- Intel Software Guard Extensions (SGX)
- TPM Device



## Item Specific Help

1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. Enable/Disable Intel Software Guard Extensions (SGX)
4. If the item is set to Hidden, the TPM device is not visible to the operating system.
5. If the TPM device setting is set to Hidden, the BIOS hides this item. If the TPM Device setting changes from Hidden to Available, the BIOS makes this item visible immediately without a restart. The TPM state setting is saved when the TPM Device setting changes to Hidden and is restored when it is changed back to Available. The TPM State setting can change only if you confirm the request via the Physical Presence check prompted by the BIOS during the next startup.
6. If the TPM device setting is set to Hidden, the BIOS hides this item. The TPM can be cleared only when you confirm the request via the Physical Presence check prompted by the BIOS during the next startup. If you select Yes, the BIOS sends TPM2\_Clear to clear the Storage and Endorsement Hierarchy. Once the TPM is cleared, the BIOS disables TPM Power-on Authentication and sets the Clear TPM setting stays the same before and after the clear TPM operation. The Clear TPM settings is also set to No without any action taken if you select No for the Physical Presence check.
7. This option will restore all the security settings to factory defaults. For example, TPM device will be cleared and set to default shipping state.

# Configuration Menu



## Configuration

- Language 1
- Virtualization Technology 2
- SATA Emulation 3
- After Power Loss
- Num Lock State at Power-On 4
- S4/S5 Wake on LAN 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. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
4. Sets the Num Lock state after POST.
5. Permits the user to control whether the system should wale from S4 or S5 if a magic packet is received by the NIC

# Configuration Menu



## Configuration

- Language
- Virtualization Technology
- SATA Emulation
- After Power Loss
- Num Lock State at Power-On
- S4/S5 Wake on LAN

1

2

3

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

# Configuration Menu



## Configuration

- Language
- Virtualization Technology
- SATA Emulation
- After Power Loss
- Num Lock State at Power-On
- S4/S5 Wake on LAN

1

2

3

4

5

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



# Configuration Menu



## Configuration

- Language
- Virtualization Technology
- SATA Emulation
- After Power Loss
- Num Lock State at Power-On
- S4/S5 Wake on LAN

1

2

3

4

5

SATA Emulation

### Item Specific Help

1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
4. Sets the Num Lock state after POST.
5. Permits the user to control whether the system should wale from S4 or S5 if a magic packet is received by the NIC

# Configuration Menu



## Configuration

- Language 1
- Virtualization Technology 2
- SATA Emulation 3
- After Power Loss
- Num Lock State at Power-On 4
- S4/S5 Wake on LAN 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. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
4. Sets the Num Lock state after POST.
5. Permits the user to control whether the system should wale from S4 or S5 if a magic packet is received by the NIC

# Configuration Menu



## Configuration

- Language
- Virtualization Technology
- SATA Emulation
- After Power Loss
- Num Lock State at Power-On
- S4/S5 Wake on LAN

1

2

3

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

# Configuration Menu



## Configuration

Thermal

CPU Fan Speed 1310 RPM

System Fan Speed 1061 RPM

### Item Specific Help

1. This formset allows the user to manage RAID volumes on the Intel(R) RAID Controller

# Boot Options Menu



## Boot Options

- Post Hotkey Delay (sec)
- USB Boot 1
- Network Boot 2
- Network Boot Protocol 3
- Platform Key 5 Enrolled MSFT
- Pending Action None
- Load HP Factory Default Keys
- Load MSFT Debug Policy Keys
- UEFI Boot Order
  - USB Flash Drive/USB Hard Disk
  - ▶ OS Boot Manager
  - USB CD/DVD ROM Drive
  - Network Adapter
  - Internal 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.

# Boot Options Menu

**hp**

**Boot Options**

Post Hotkey Delay (sec)

USB Boot

Network Boot

Network Boot Protocol

Platform Key

Pending Action

Enrolled MSFT

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- USB Flash Drive/USB Hard Disk
- ▶ OS Boot Manager
- USB CD/DVD ROM Drive
- Network Adapter
- Internal CD/DVD ROM Drive

Post Hotkey Delay (sec)

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.

# Boot Options Menu

**hp**

**Boot Options**

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key Enrolled MSFT

Pending Action None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- USB Flash Drive/USB Hard Disk
- ▶ OS Boot Manager
- USB CD/DVD ROM Drive
- Network Adapter
- Internal CD/DVD ROM Drive

**USB Boot**

**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.

# Boot Options Menu

**hp**

**Boot Options**

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key Enrolled MSFT **5**

Pending Action None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- USB Flash Drive/USB Hard Disk
- ▶ OS Boot Manager
- USB CD/DVD ROM Drive
- Network Adapter
- Internal CD/DVD ROM Drive

**Network Boot**

**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.



# Boot Options Menu

**hp**

**Boot Options**

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key

Pending Action

Enrolled MSFT **5**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ USB Flash Drive/USB Hard Disk

▶ OS Boot Manager

▶ USB CD/DVD ROM Drive

▶ Network Adapter

▶ Internal CD/DVD ROM Drive

**Network Boot Protocol**

**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.

# Boot Options Menu

**hp**

**Boot Options**

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key **5** Enrolled MSFT

Pending Action None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- USB Flash Drive/USB Hard Disk
- ▶ OS Boot Manager
- USB CD/DVD ROM Drive
- Network Adapter
- Internal CD/DVD ROM Drive

**Secure Boot**

**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.

# Exit Menu



Exit

Ignore Changes and Exit <sup>1</sup> <sup>2</sup> <sup>3</sup>

## 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

Ignore Changes and Exit <sup>1</sup> <sup>2</sup> <sup>3</sup>

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.

# Exit Menu



Exit

Ignore Changes and Exit <sup>1</sup> <sup>2</sup> <sup>3</sup>

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.