

Interactive BIOS simulator

HP 285 G8 MT Pro

Welcome to the interactive BIOS simulator for the
HP 285 G8 MT Pro

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	[01:10:31]
System Date	05/26/2021
Product Name	HP 285 GB Microtower PC
System Family	HP 285
Product Number	1Y4D5AV
System Board ID	870E
Asset Tag	
Ownership Tag	
Processor Type	AMD Ryzen 3 PRO 5350G with Radeon Graphics
Processor Speed	4000 MHz
Total Memory	4 GB
BIOS Vendor	AMI
BIOS Revision	B.12
Serial Number	HMLW301008
UUID	EBFE1DF2-39DF-87D0-78C4-3B4DA84-1B2BB
System Board CT Number	PLERDX2CYEI01R
Factory installed OS	Win10
Build ID	21WW1MAT6AL#SACH#DACH
Feature Byte	2U3E 3K3N 3P3X 476b 6y7J 7M7T 7Yap aqau bDbh cbdU dpdq eJfP kam9 .AD

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	73.03
GOP (Graphic Output Protocol)	2.15.0

Item Specific Help

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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 lose 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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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 lose 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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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 lose 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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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. 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 lose 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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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. 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 lose 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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

Stringent Password

TPM Device

3

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. 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 lose 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.

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

Item Specific Help

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

System Audio

Item Specific Help

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

Item Specific Help

Network Controller

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

SATA0

Item Specific Help

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

SATA1

Item Specific Help

Security Menu



Security

- Device Security
- System Audio
- Network Controller
- SATA0
- SATA1
- SATA2

SATA2

Item Specific Help

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

Front USB Ports

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 0

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 1

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 2

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 3

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 4

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 5

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

Rear USB Ports

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 6

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

USB Port 7

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

Item Specific Help

Internal USB Ports

Security Menu



Security

USB Security

Front USB Ports

USB Port 0

USB Port 1

USB Port 2

USB Port 3

USB Port 4

USB Port 5

Rear USB Ports

USB Port 6

USB Port 7

Internal USB Ports

USB Port 10

USB Port 10

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

PCI Express x16 Slot 1

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

PCI Express x1 Slot 1

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

PCI Slot 1

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

M.2 Card Slot 1

Item Specific Help

Security Menu



Security

Slot Security

PCI Express x16 Slot 1

PCI Express x1 Slot 1

PCI Slot 1

M.2 Card Slot 1

M.2 Card Slot 2

M.2 Card Slot 2

Item Specific Help

Security Menu



Security

Hard Drive Utilities

Item Specific Help

Security Menu



Security

Hard Drive Utilities

Item Specific Help

Security Menu



Security

Hard Drive Utilities

Automatic DriveLock

<Disabled>

Item Specific Help

Security Menu



Security

Hard Drive Utilities

Automatic DriveLock

<Disabled>

Item Specific Help

Security Menu



Security

Hard Drive Utilities

Automatic DriveLock

<Disabled>

Item Specific Help

Security Menu



Security

Smart Cover

Cover Removal Sensor

Item Specific Help

Security Menu



Security

Smart Cover

Cover Removal Sensor

Cover Removal Sensor

Item Specific Help

Configuration Menu



Configuration

- Language 1
- Virtualization Technology 2
- POST Messages 3
- After Power Loss 4
- Remote Wakeup Boot Source 5
- Wake on LAN Power-On Password Policy 6
- 7
- Num Lock State at Power-On 8
- S4/S5 Wake on LAN 9
- 10
- 11
- Runtime Power Management 12
- Idle Power Savings 13
- SATA Power Management 14

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. Allows for selection between splash screen and text-mode startup.
4. Determine the system's state after power is lost to the unit.
5. This option sets the boot source of remote wakeup.
6. This option the password policy for system wakup from LAN.
7. Enable the days of the week to turn the system on. This feature wakes the system up from a powered off state.
8. Sets the Num Lock state after POST.
9. Permits the user to control whether the system should wake from S4 or S5 if a magic packet is received by the NIC.
10. This option sets whether the device/function is shown/enabled or hidden/disabled from OS.
11. Provides thermal/FAN status of the system.
12. Enables Runtime Power Management.
13. Increases the OS's Idle Power Savings.
14. Enables or disables DIPM or HIPM.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Language

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

Virtualization Technology

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

POST Messages

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

After Power Loss



Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

Remote Wakeup Boot Source

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Wake on LAN Power-On Password Policy

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Sunday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Monday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Tuesday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Wednesday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Thursday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Friday

Item Specific Help

Configuration Menu



Configuration

Scheduled Power-On

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time (hh:mm)

<00:00>

Saturday

Item Specific Help

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

Num Lock State at Power-On

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

S4/S5 Wake on LAN



Configuration Menu



Configuration

- Device Options
- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Item Specific Help

Configuration Menu



Configuration

- Device Options
- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Serial Port A

Item Specific Help

Configuration Menu



Configuration

- Device Options
- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Item Specific Help

Internal Speaker

Configuration Menu



Configuration

- Device Options
- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Item Specific Help

NIC PXE Option ROM Download

Configuration Menu



Configuration

- Device Options
- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Item Specific Help

PCI SERR# Generation

Configuration Menu



Configuration

Device Options

- Serial Port A
- Internal Speaker
- NIC PXE Option ROM Download
- PCI SERR# Generation
- PCI VGA Palette Snooping

Item Specific Help

PCI VGA Palette Snooping

Configuration Menu



Configuration

Thermal

CPU Fan Speed : 604 RPM

System Fan Speed : 676 RPM

CPU Fan Check

System Fan Check

Item Specific Help

Configuration Menu



Configuration

Thermal

CPU Fan Speed : 604 RPM
System Fan Speed : 676 RPM
CPU Fan Check
System Fan Check

Item Specific Help

CPU Fan Check

Configuration Menu



Configuration

Thermal

CPU Fan Speed : 604 RPM
System Fan Speed : 676 RPM
CPU Fan Check
System Fan Check

Item Specific Help

System FanCheck

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

Runtime Power Management

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

Item Specific Help

Idle Power Savings

Configuration Menu



Configuration

- Language
- Virtualization Technology
- POST Messages
- After Power Loss
- Remote Wakeup Boot Source
- Wake on LAN Power-On Password Policy

- Num Lock State at Power-On
- S4/S5 Wake on LAN

- Runtime Power Management
- Idle Power Savings
- SATA Power Management

SATA Power Management

Item Specific Help

Boot Options Menu



Boot Options

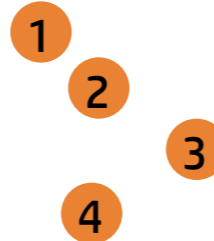
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol

Platform Key
Pending Action

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
▶ OS Boot Manager

Enrolled-MSFT
None



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 Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. The HP logo is in the top left. The menu items are: Post Hotkey Delay (sec), USB Boot, Network Boot, Network Boot Protocol, Platform Key, Pending Action, Load HP Factory Default Keys, Load MSFT Debug Policy Keys, UEFI Boot Order (with a sub-option OS Boot Manager), and Enrolled MSFT (with a sub-option None). A blue box highlights the 'Post Hotkey Delay (sec)' option. Four numbered callouts (1-4) are placed to the right of the menu items: 1 points to USB Boot, 2 points to Network Boot, 3 points to Network Boot Protocol, and 4 points to Enrolled MSFT. A 'Boot Options' title bar is at the top right of the menu area. An 'Item Specific Help' box on the right contains four numbered instructions corresponding to the callouts.

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot

Network Boot

Network Boot Protocol

Platform Key

Pending Action

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

 ▶ OS Boot Manager

Enrolled MSFT

None

Post Hotkey Delay (sec)

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 Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. On the left is the HP logo. The menu items are: 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, and OS Boot Manager. A blue box highlights the 'USB Boot' option. Four numbered callouts (1-4) point to 'USB Boot', 'Network Boot', 'Network Boot Protocol', and 'Enrolled MSFT' respectively. On the right, a 'Boot Options' header is above a 'Item Specific Help' panel containing four numbered instructions.

hp

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
▶ OS Boot Manager

Boot Options

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 Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

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 **4**

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Network Boot

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 Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

The screenshot shows the HP BIOS Boot Options menu. The HP logo is in the top left. The menu items are: 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, and OS Boot Manager. A blue box highlights the 'Network Boot Protocol' option, with four numbered callouts (1-4) pointing to it. A sidebar on the right titled 'Item Specific Help' provides instructions for each step.

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
▶ OS Boot Manager

1
2
3
4

Network Boot Protocol

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 Boot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Boot Options Menu

hp

Boot Options

Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Platform Key **4**

Pending Action

Enrolled MSFT

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

▶ OS Boot Manager

Secure Boot

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 IBoot is enabled, BIOS performs cryptographic check during bootup, for the integrity of the software image. It prevents unauthorized or maliciously modified software from running.

Exit Menu



Exit

Ignore Changes and Exit ¹ ² 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.

Exit Menu



Exit

Ignore Changes and Exit

- 1
- 2
- 3

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

- 1
- 2
- 3

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.