

Interactive BIOS simulator

HP All-in-One PC 21-b0001/A

Welcome to the interactive BIOS simulator for the
HP All-in-One PC 21-b0001/A

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	[09/18/2020]
Product Name	HP All-in-One 21-b0xxx
System Family	HP OPP
Product Number	12134567#ABA
System Board ID	87F8
Processor Type	Intel(R) Core(TM) i5-1035G1 CPU @ 1.00 GHz
Total Memory	32 GB
BIOS Vendor	AMI
BIOS Revision	B.10
Serial Number	1CZ0250BP3
UUID	5C9F4AEE-569D-22E6-0E0E-085783A8A377
System Board CT Number	PJVVE02MVDU25H
Factory installed OS	Win10
Primary Battery SN	00600 12/04/2019
Build ID	20WW2WITaf#SABA#DABA
Feature Byte	3K3Q 6b7K 7P7S 7WaB apaq asbC bhcb dUdX dpdq fPm9 mHmM n3n4 .2M

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	63.16
Intel ME (Management Engine)	13.0.35.1508
GOP (Graphic Output Protocol)	14.0.1039

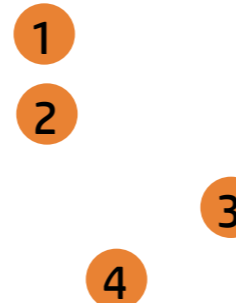
Item Specific Help

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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

1

Power-On Password

2

Intel Software Guard Extensions (SGX)

3

HP SpareKey

<Disabled>

HP SpareKey

<Not Enrolled>

TPM Device

4

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 4
- Num Lock State at Power-On 5
- S4/S5 Wake on LAN 6

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. When set to AHCI, SATA is configured to AHCI mode. When set to RAID, SATA is configured to RAID mode.
4. Determine the system's state after power is lost to the unit.
5. Sets the Num Lock state after POST.
6. Permits the user to control whether the system should wake 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

Language

Item Specific Help

Configuration Menu



Configuration

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

Virtualization Technology

Item Specific Help

Configuration Menu



Configuration

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

SATA Emulation

Item Specific Help

Configuration Menu



Configuration

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

After Power Loss

Item Specific Help

Configuration Menu



Configuration

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

Num Lock State at Power-On

Item Specific Help

Configuration Menu



Configuration

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

S4/S5 Wake on LAN

Item Specific Help

Configuration Menu



Configuration

UEFI HII Configuration

Item Specific Help

Configuration Menu



Configuration

Intel(R) RST 17.8.0.4507 RAID Driver

Non-RAID Physical Disks:

Item Specific Help

Configuration Menu



Configuration

PHYSICAL DISK INFO

Port :	0.0
Model Number:	ST1000DM003-1SB102
Serial Number:	ZN1FN6AP
Size:	931.5GB
Status:	Non-RAID
Controller Type:	AHCI
Controller Interface :	SATA

Item Specific Help

Configuration Menu



Configuration

Driver Information

Driver Name: Realtek UEFI UNDI Driver
Driver Version: 2.050
Driver Released Date: 2019/09/19

Device Information

Device Name: Realtek PCIe GBE Family Controller
PCI Slot: 02:00:00
MAC Address: 54:B2:03:99:54:65

Patent Information

This product is covered by one or more of the following patents:
US6,570,884, US6,115,776, and
US6,327,625

Item Specific Help

Configuration Menu



Configuration

Device Options
Internal Speaker

Item Specific Help

Configuration Menu



Configuration

Thermal

CPU Fan Speed

: 1405 RPM

Item Specific Help

Boot Options Menu



Boot Options

Post Hotkey Delay (sec)
USB Boot **1**
Network Boot **2**
Network Boot Protocol **3**

Platform Key **4** Enrolled MSFT
Pending Action None

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
 ▶ OS Boot Manager
 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

Post Hotkey Delay (sec)

UEFI Boot Order

- ▶ OS Boot Manager
- 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 **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

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



Boot Options

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

1
2
4

3

Platform Key
Pending Action

Enrolled MSFT
None

Load HP Factory Default Keys
Load MSFT Debug Policy Keys

UEFI Boot Order
▶ OS Boot Manager
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

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

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 **4**

Pending Action

Enrolled MSFT

None

Load HP Factory Default Keys

Load MSFT Debug Policy Keys

UEFI Boot Order

- ▶ OS Boot Manager
- 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 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.