

Interactive BIOS simulator

HP Desktop M01-xxxxx series

Welcome to the interactive BIOS simulator for the
HP Desktop M01-xxxxx series

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	[02:08:24]
System Date	08/07/2019
Product Name	HP Desktop M01-xxxxx series
System Family	HP Desktop M01-xxxxx series
Product Number	6GU13AV
System Board ID	8643
Born On Date	05/13/2019
Processor Type	AMD Ryzen 3 3200G with Radeon Vega Graphics
Processor Speed	3600 MHz
Total Memory	4 GB
BIOS Vendor	AMI
BIOS Version	B.14
Serial Number	HLMW323285
UUID	73BB7114-8195-3FF8-6F4B-8250828-F9E85
System Board CT Number	PHZGRX3CYC9A6A
Factory installed OS	Win10
Build ID	19WW2HAT6ah#SABA#DABA
Feature Byte	2U3E 3K3N 4C6b 7K7M 7T7W aBap aqas aubC bhcb dUdp dqeJ fPkh .yF

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 34.18

GOP (Graphic Output Protocol) 2.5.0

Video BIOS ATI 113-PICASSO-114

Item Specific Help

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Security Menu



Security

Administrator Password

1

Power-On Password

2

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. 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.
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.

Configuration Menu



Configuration

- Language 1
- Virtualization Technology 2
- Num Lock State at Power-On 3
- S4/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 whether the system should wake from S4 or S5 if a magic packet is received by the NIC
5. Provides thermal/FAN status of the system.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Num Lock State at Power-On
- S4/S5 Wake on Lan

- 1
- 2
- 3
- 4

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 whether the system should wake from S4 or S5 if a magic packet is received by the NIC
5. Provides thermal/FAN status of the system.

Configuration Menu



Configuration

- Language 1
- Virtualization Technology 2
- Num Lock State at Power-On 3
- S4/S5 Wake on Lan 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. Sets the Num Lock state after POST.
4. Permits the user to control whether the system should wake from S4 or S5 if a magic packet is received by the NIC
5. Provides thermal/FAN status of the system.

Configuration Menu



Configuration

- Language
- Virtualization Technology
- Num Lock State at Power-On
- S4/S5 Wake on Lan

5

1

2

3

4

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 whether the system should wake from S4 or S5 if a magic packet is received by the NIC
5. Provides thermal/FAN status of the system.

Configuration Menu



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 whether the system should wake from S4 or S5 if a magic packet is received by the NIC
5. Provides thermal/FAN status of the system.

Configuration Menu



Configuration


Thermal

CPU Fan Speed : 604 RPM

System Fan Speed : 656 RPM

Item Specific Help

Boot Options Menu



Post Hotkey Delay (sec)

USB Boot **1**

Network Boot **2**

Network Boot Protocol **3**

Legacy Support **4**

Platform Key **5** 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

Legacy Boot Order

- ▶ Internal Hard Drive
- 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. 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.
5. 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

Legacy Support

Platform Key

Pending Action

Enrolled MSFT

None

Post Hotkey Delay (sec)

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

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. 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.
5. 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
Legacy Support

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

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

1
2
3
4
5

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. When Legacy Support is enabled. BIOS will load Compatibility Support Module <CSM> to support Legacy OS such as Windows 7, Windows Vista, Windows XP and 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.
5. 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
Legacy Support

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

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

Network Boot

1
2
3
4
5

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. 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.
5. 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
Legacy Support
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
Legacy Boot Order
 ▶ Internal Hard Drive
 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. 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.
5. 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**

Legacy Support **4**

Platform Key

Pending Action

Enrolled MSFT **5**

None

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

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. 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.
5. 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**

Legacy Support **4**

Platform Key

Pending Action

Enrolled MSFT **5**

None

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

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. 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.
5. 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.