Contents

HP M01 Series Desktop User Manual

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

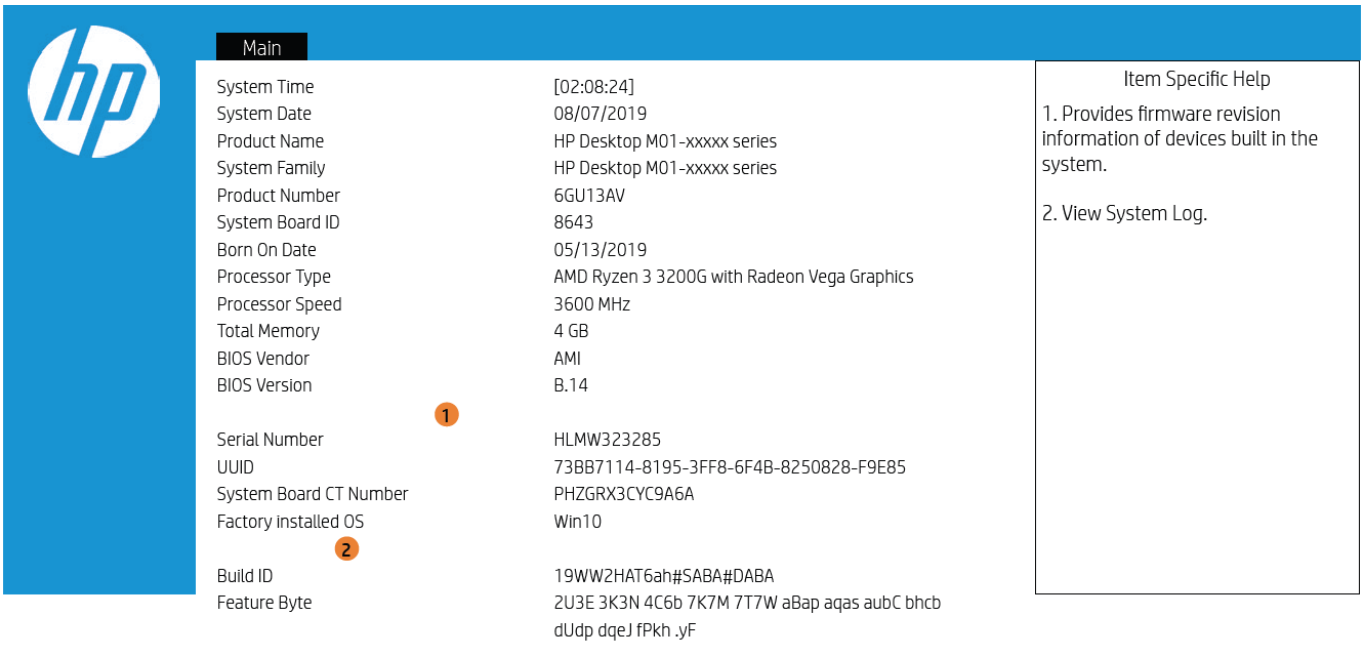
While the menu options cannot be toggled, many of them offer item-specific information about that option. To view this information, use the cursor to rollover the option, and the information will be presented in a pane on the right of the BIOS screen.

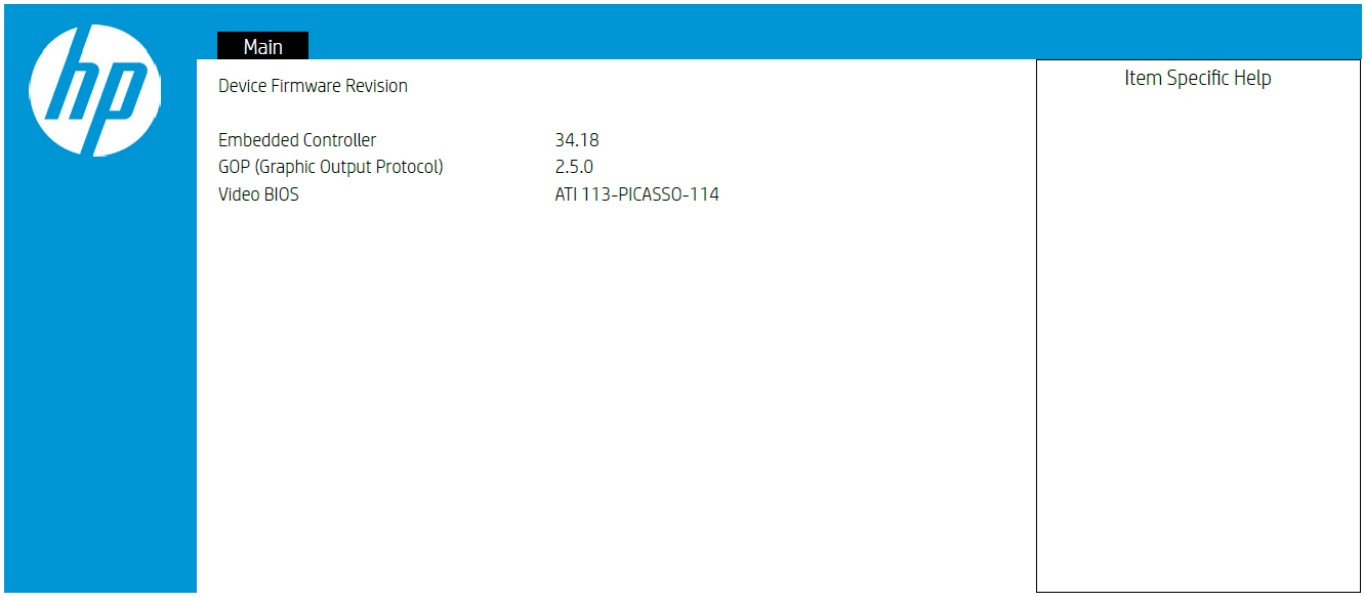
That's it!
On every page, there is a link that brings you back to either this Welcome page or the BIOS Utility Menus page, enabling you to navigate to whatever BIOS option you wish to review.

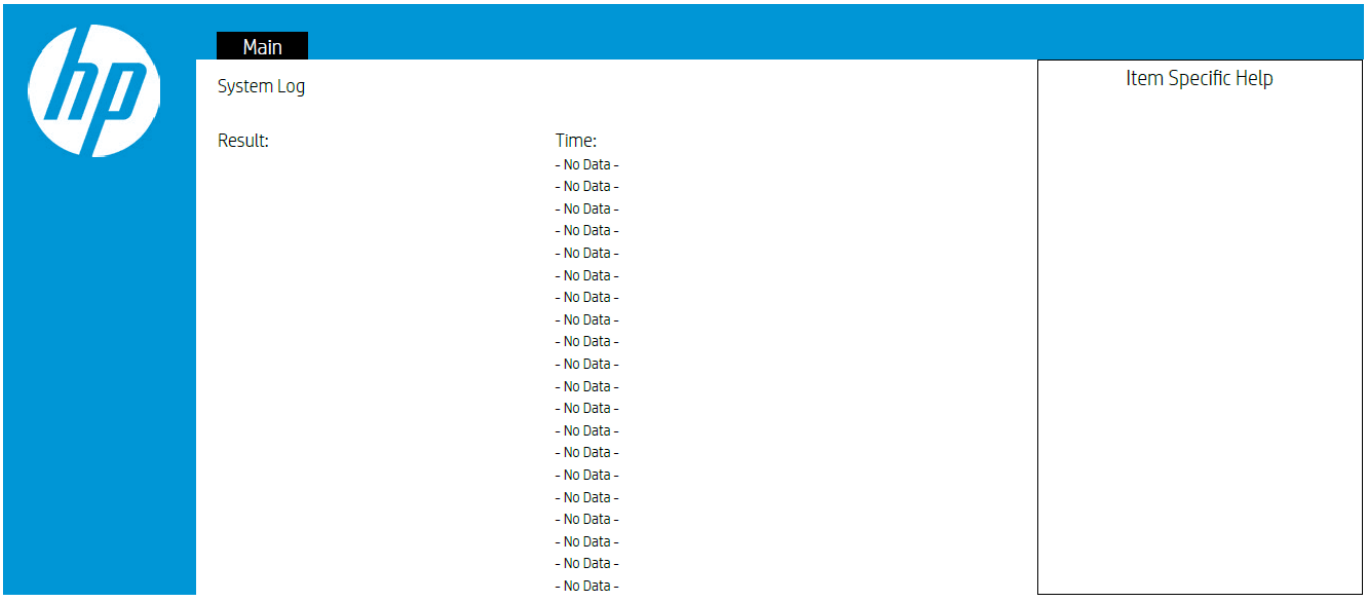
BIOS Utility Menus

Main Security Configuration Boot Options Exit

Main Menu







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 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

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 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

Administrator Password 1

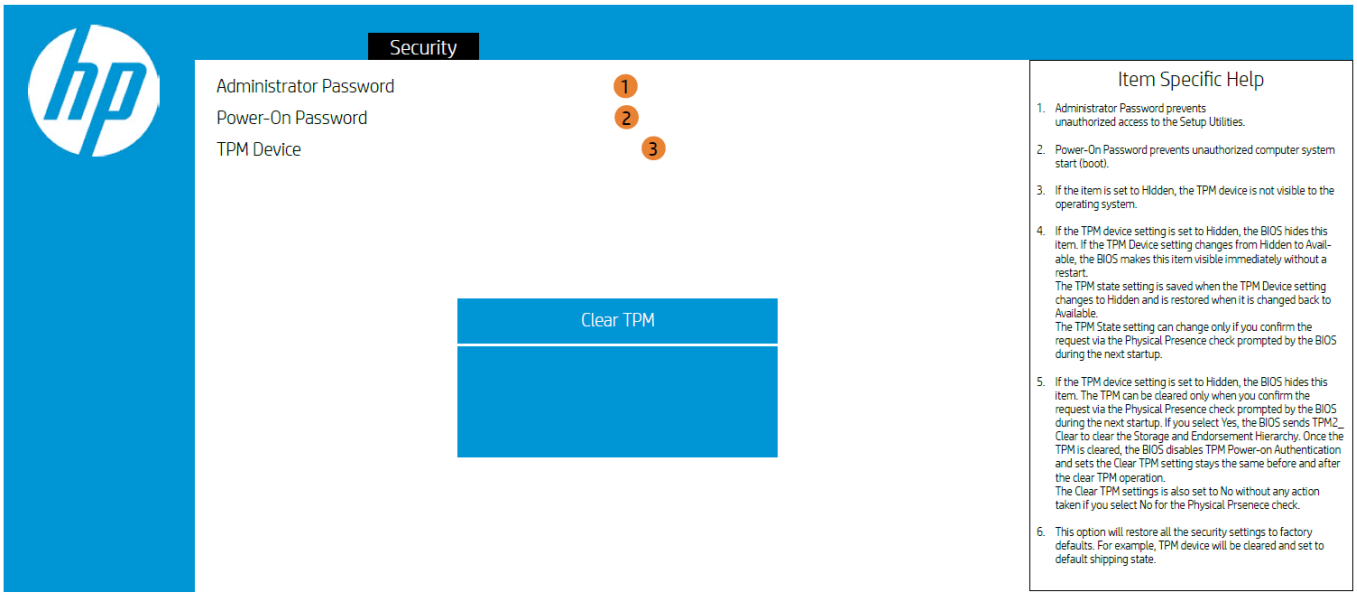
Power-On Password 2

TPM Device 3

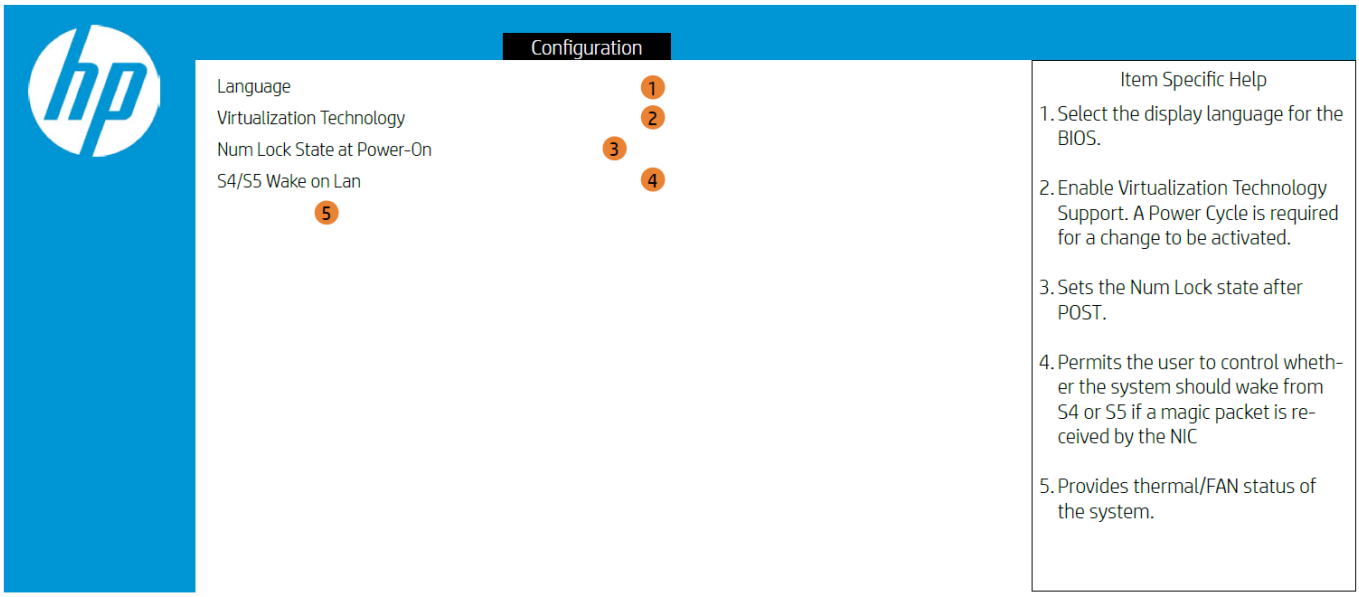
TPM Device

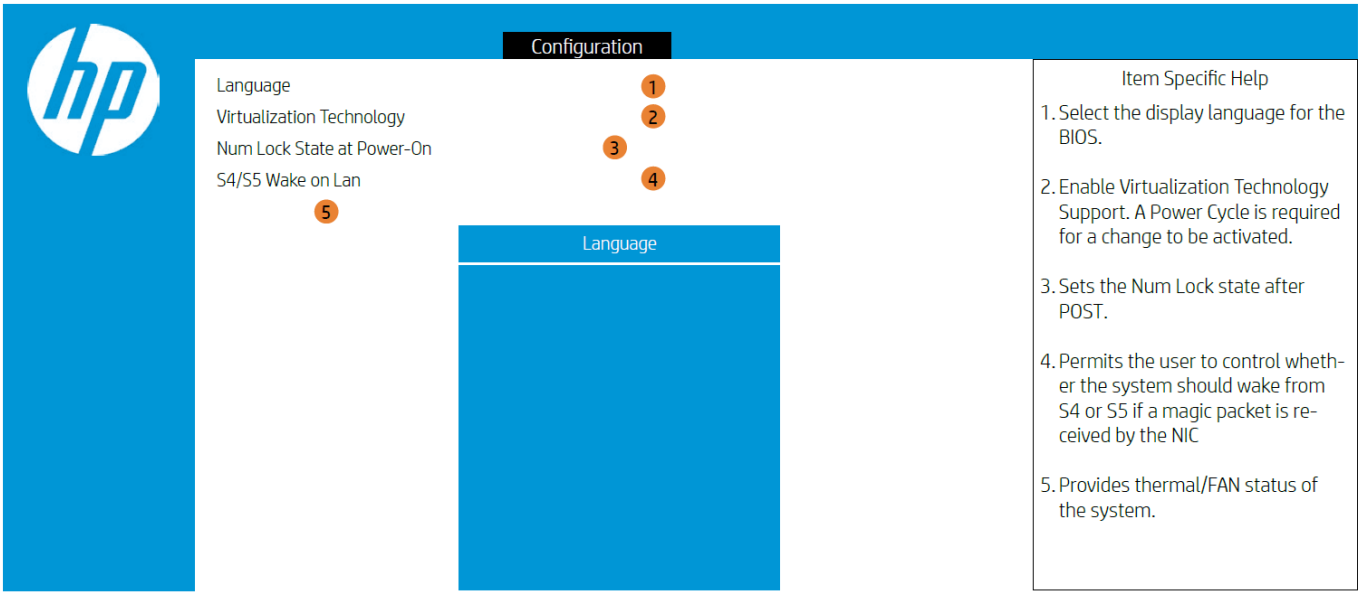
Item Specific Help

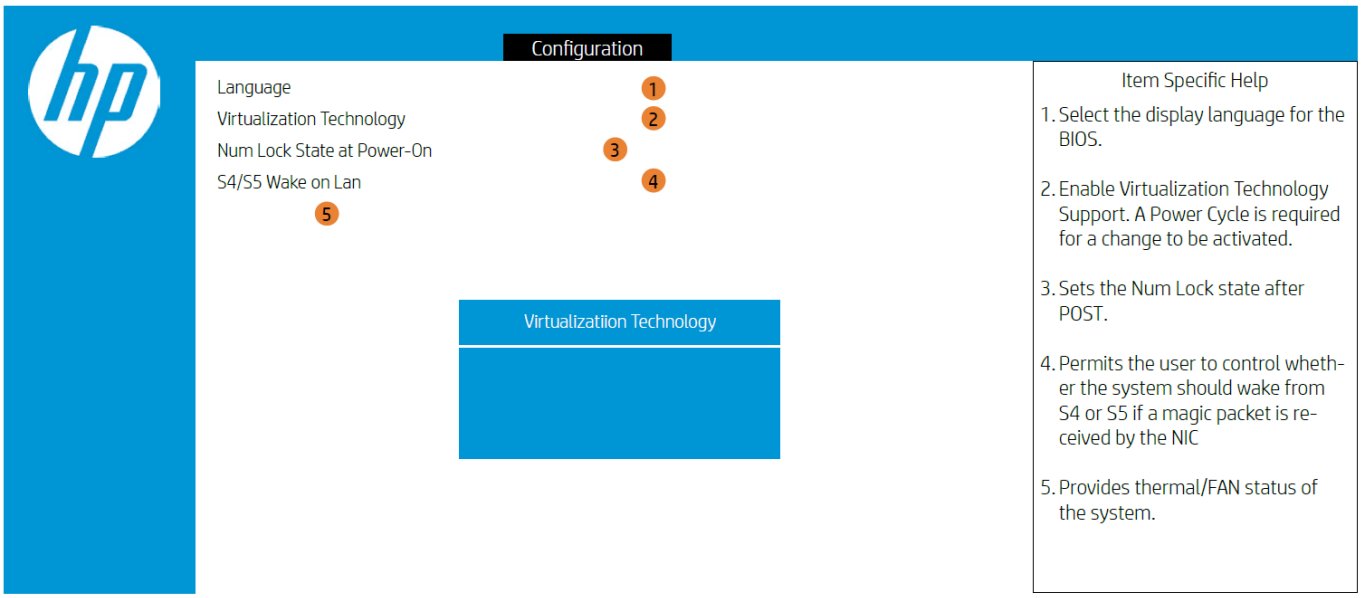
1. Administrator Password prevents unauthorized access to the Setup Utilities.
2. Power-On Password prevents unauthorized computer system start (boot).
3. If the item is set to Hidden, the TPM device is not visible to the operating system.
4. If the TPM device setting is set to Hidden, the BIOS hides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

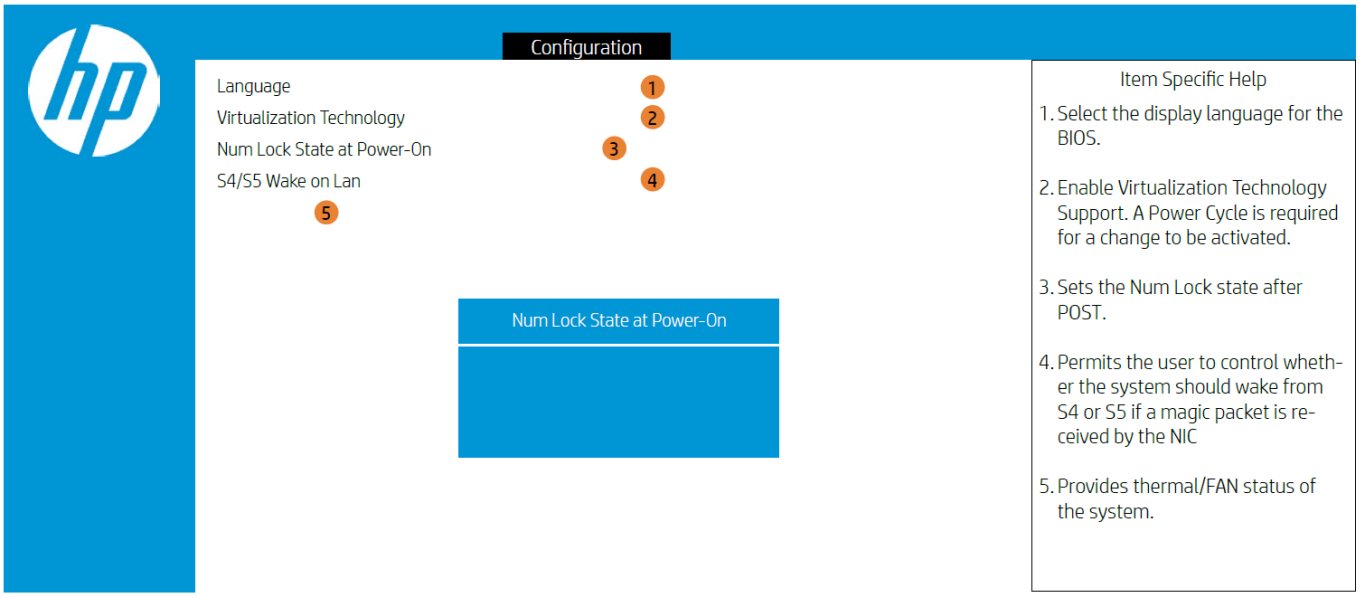


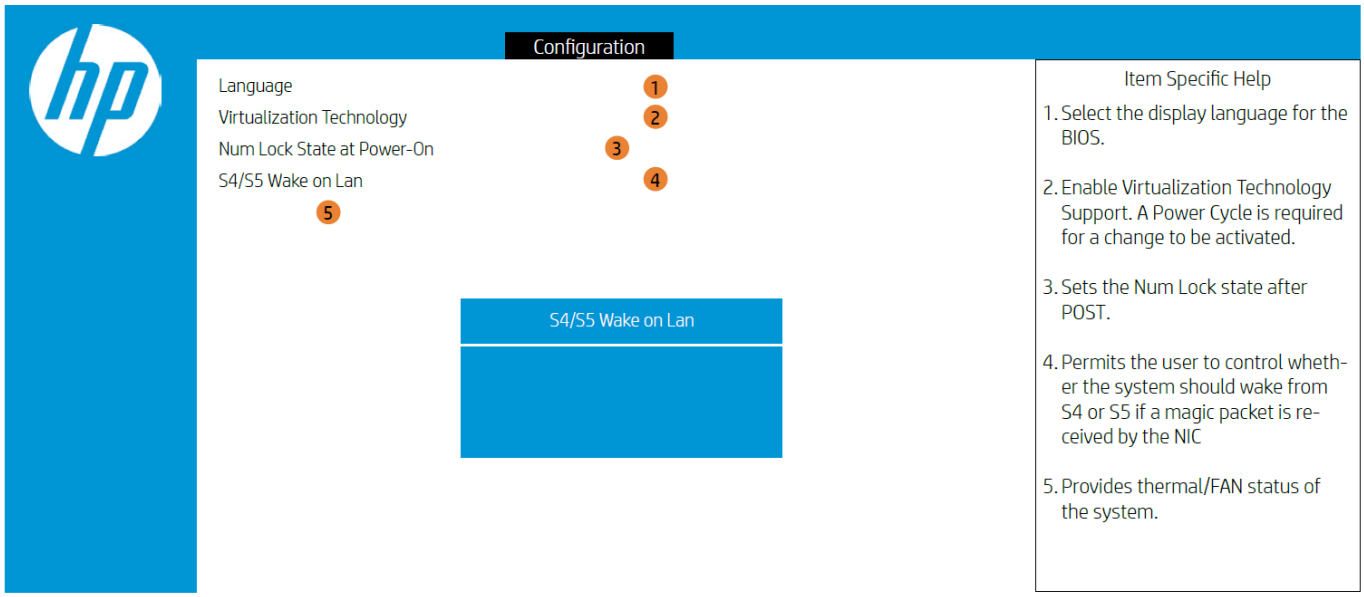
Configuration Menu

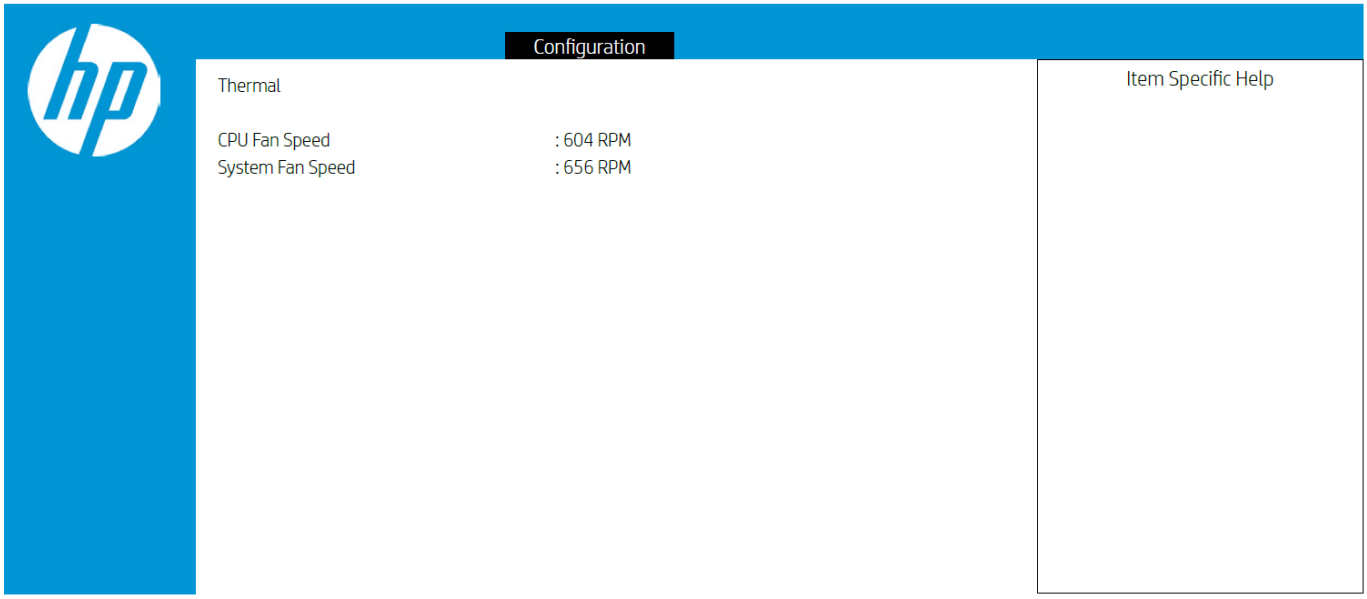



Configuration
Language 1
Virtualization Technology 2
Num Lock State at Power-On 3
S4/S5 Wake on Lan 4
5
Language
Item Specific Help
1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets the Num Lock state after POST.
4. Permits the user to control 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.

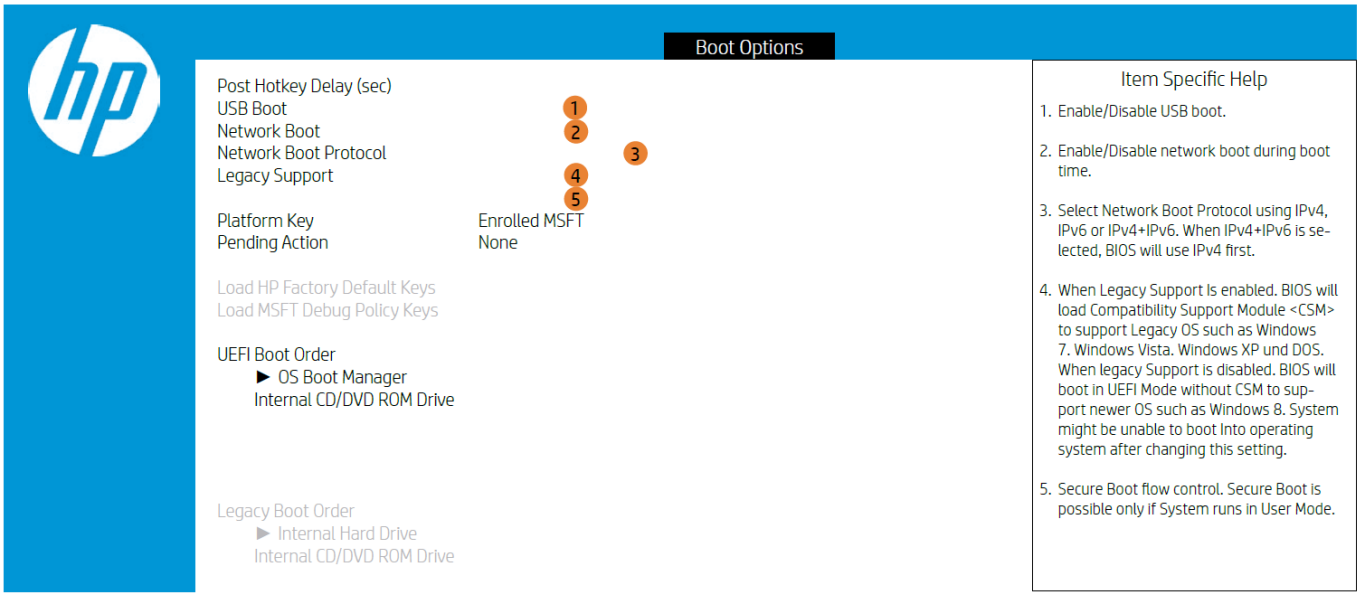

Configuration
Language 1
Virtualization Technology 2
Num Lock State at Power-On 3
S4/S5 Wake on Lan 4
5
Virtualizatiion Technology
Item Specific Help
1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets the Num Lock state after POST.
4. Permits the user to control 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.

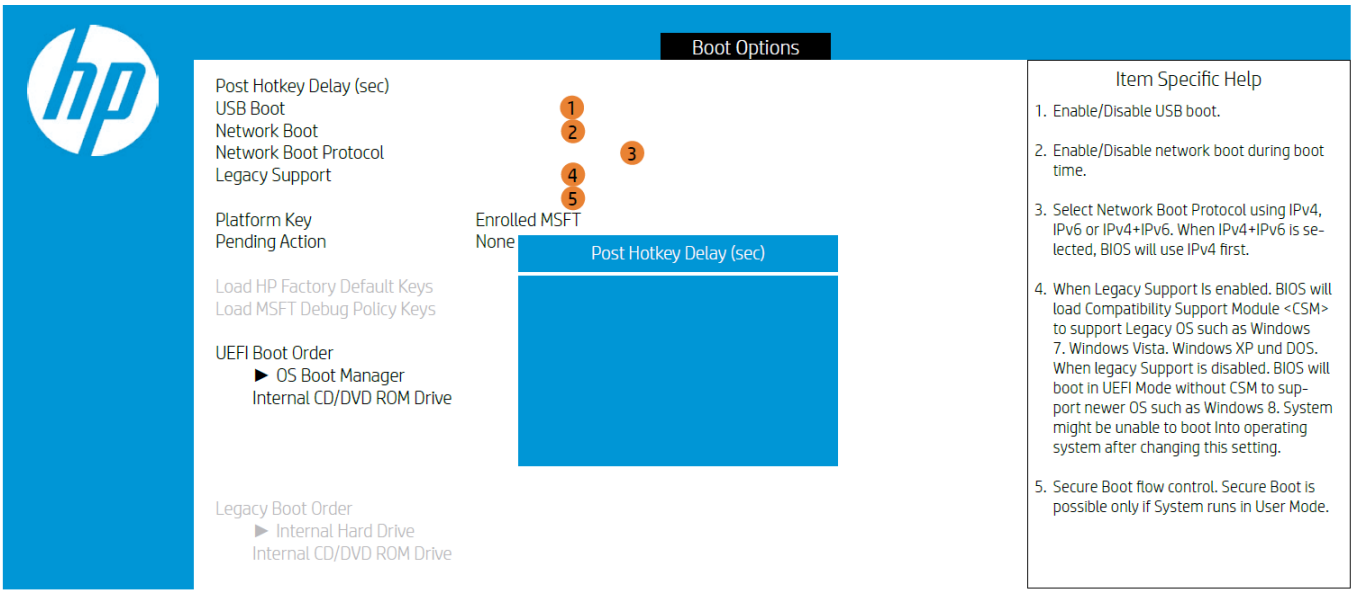

Configuration
Language 1
Virtualization Technology 2
Num Lock State at Power-On 3
S4/S5 Wake on Lan 4
5
Num Lock State at Power-On
Item Specific Help
1. Select the display language for the BIOS.
2. Enable Virtualization Technology Support. A Power Cycle is required for a change to be activated.
3. Sets the Num Lock state after POST.
4. Permits the user to control 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.

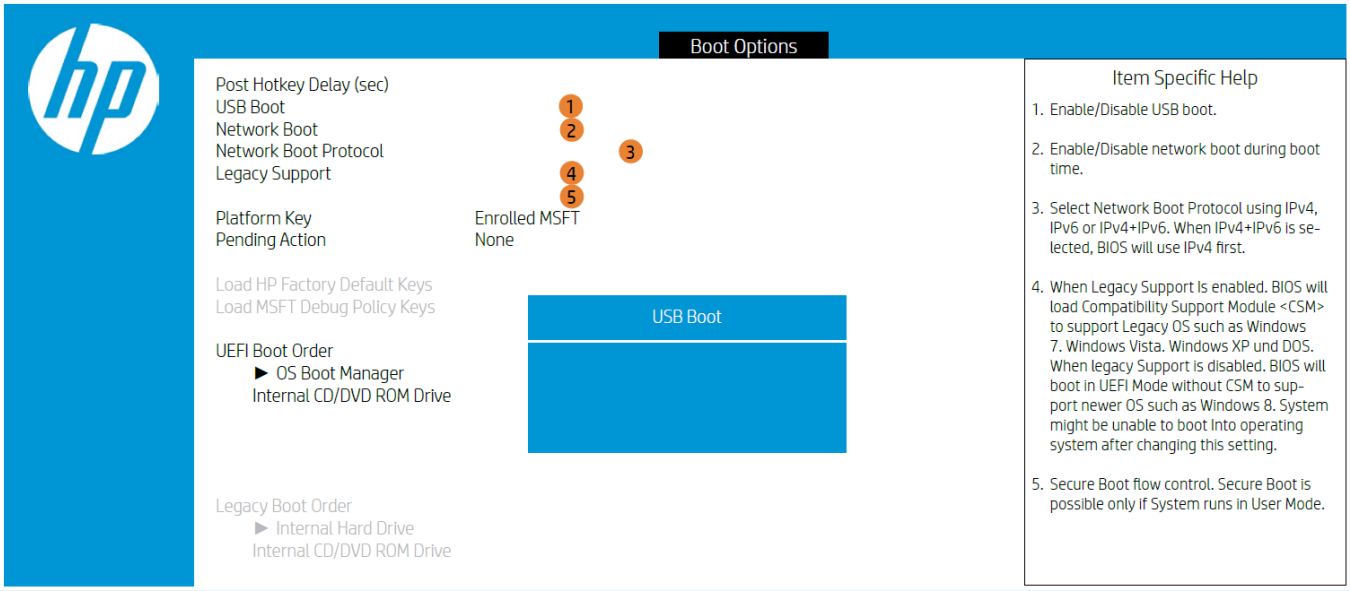


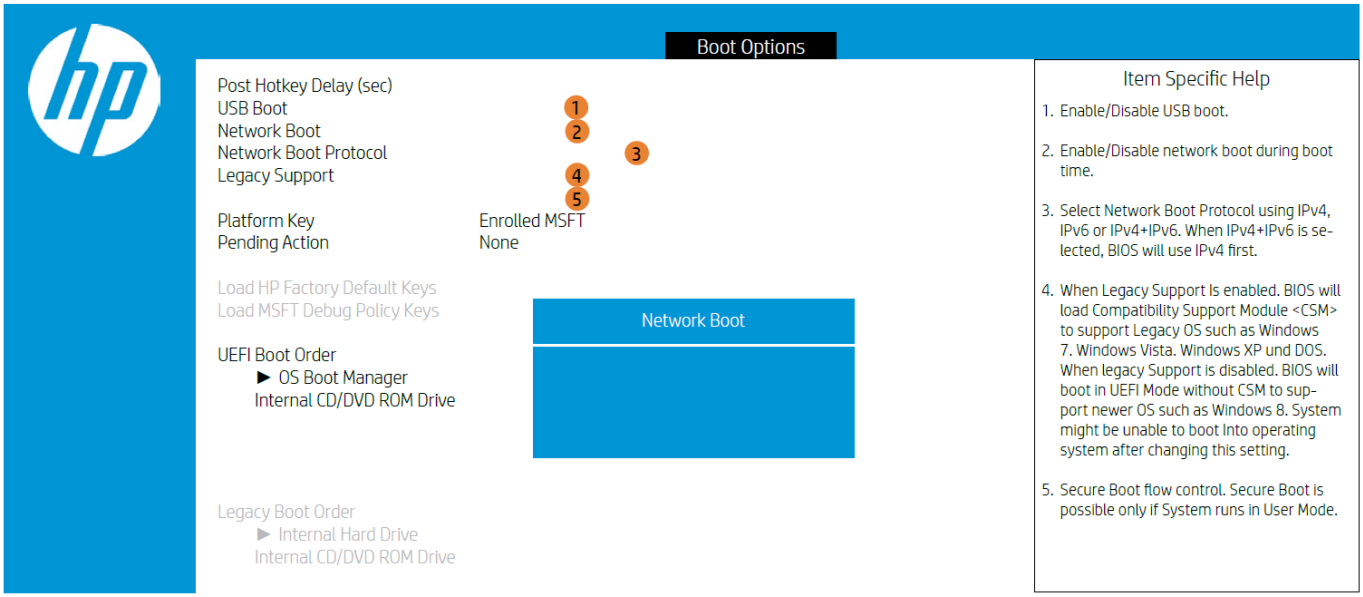


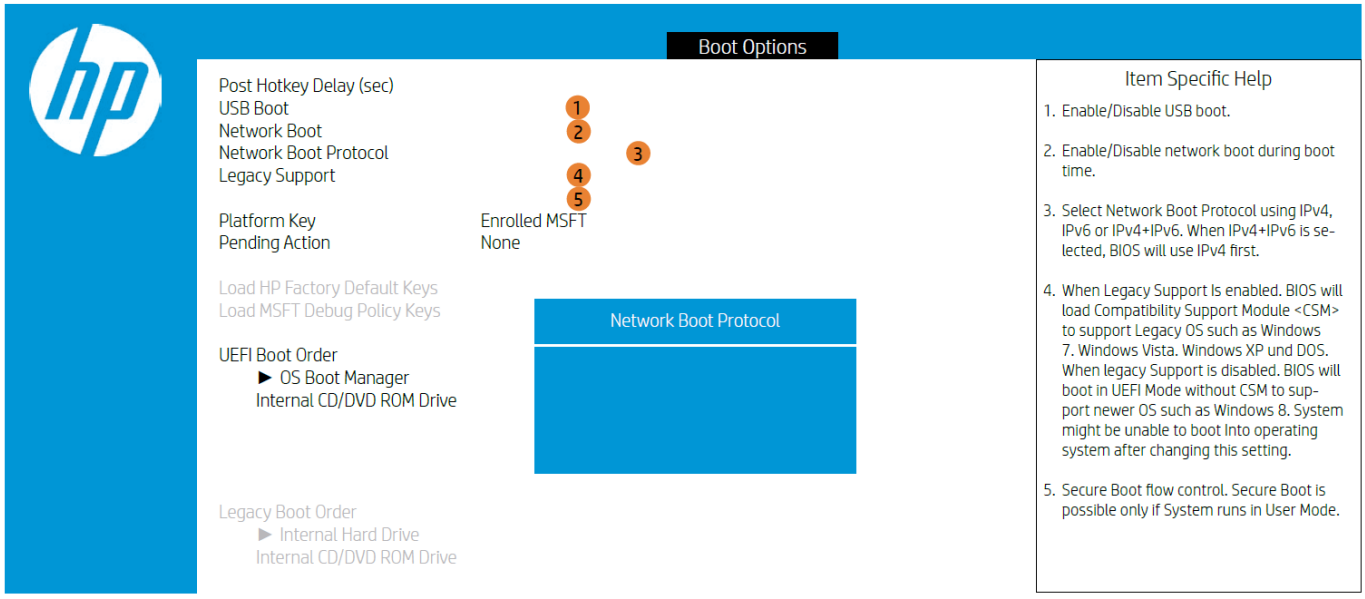
Boot Options Menu

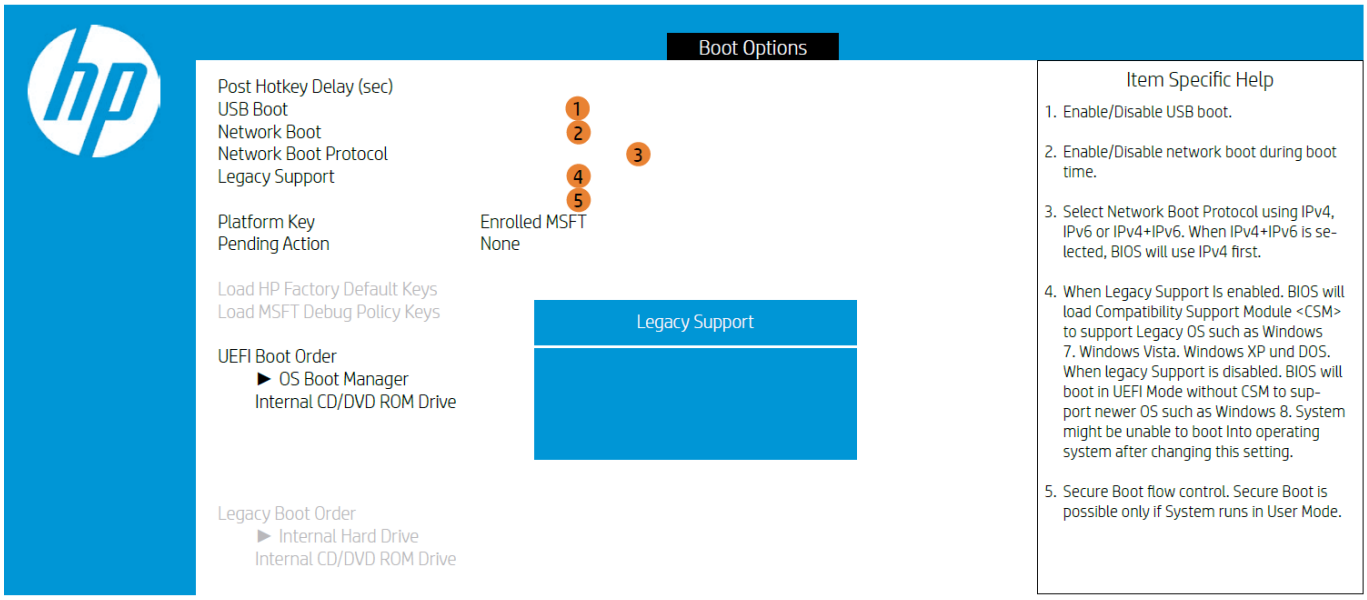


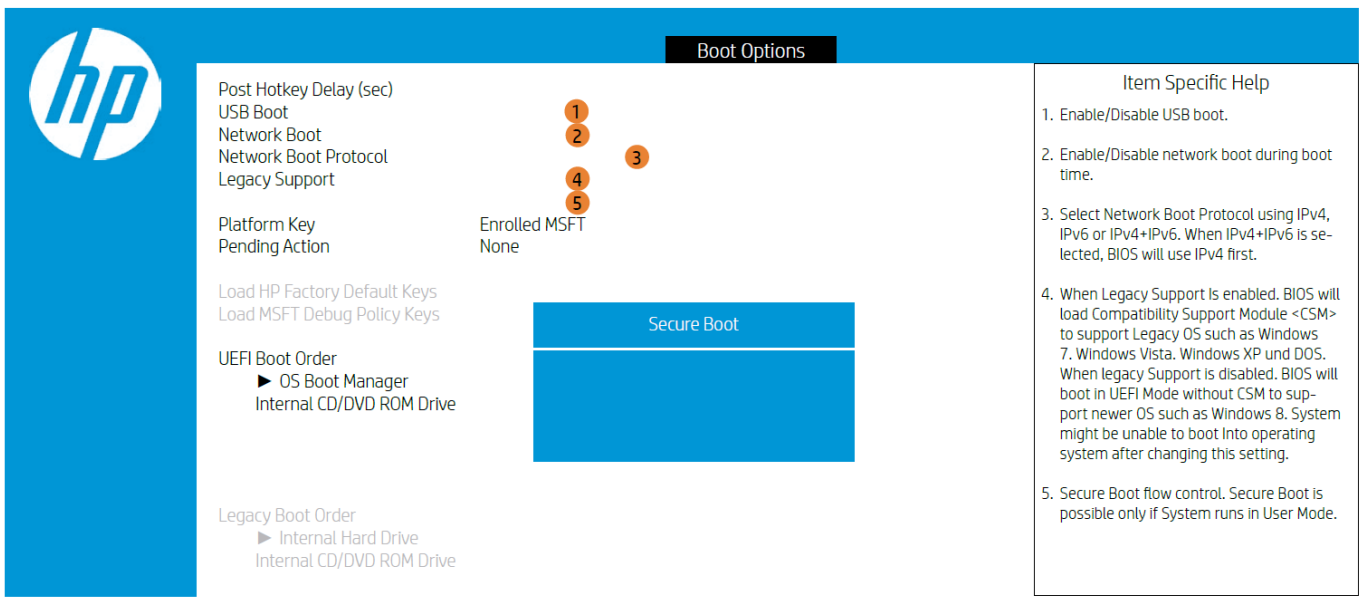

Boot Options
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Legacy Support
Platform Key
Pending Action
Enrolled MSFT
None
Load HP Factory Default Keys
Load MSFT Debug Policy Keys
UEFI Boot Order
► OS Boot Manager
Internal CD/DVD ROM Drive
Legacy Boot Order
► Internal Hard Drive
Internal CD/DVD ROM Drive
Post Hotkey Delay (sec)
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
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
USB 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.

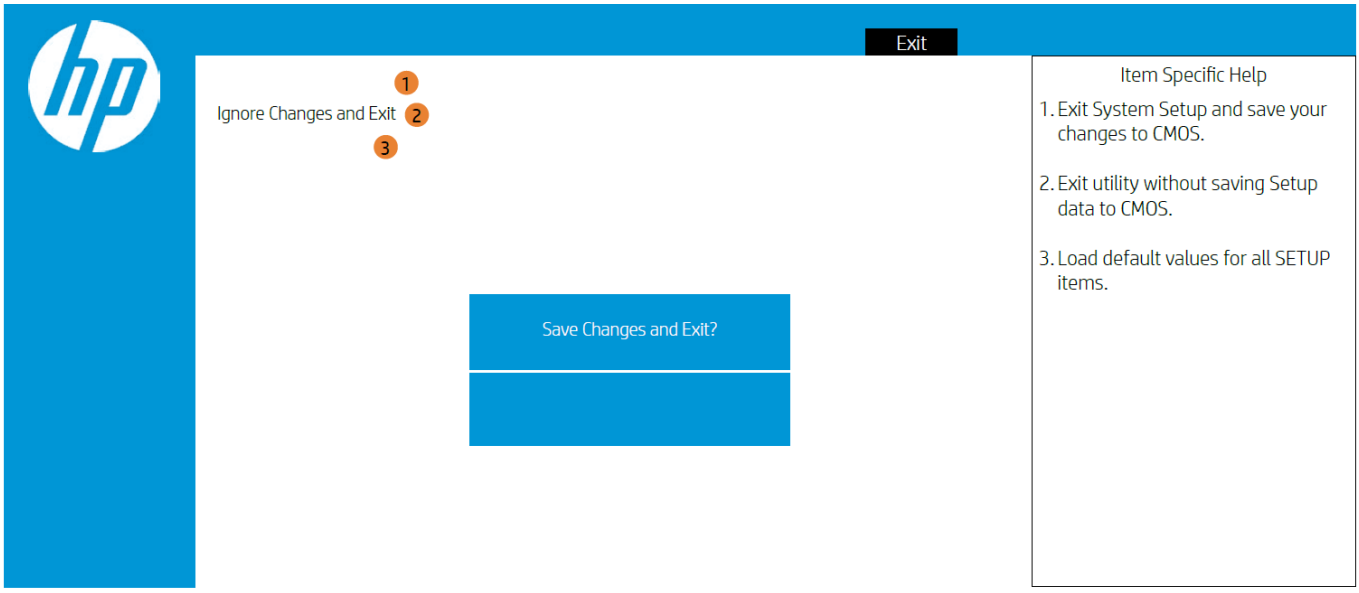

Boot Options
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Legacy Support
Platform Key
Pending Action
Enrolled MSFT
None
Load HP Factory Default Keys
Load MSFT Debug Policy Keys
UEFI Boot Order
► OS Boot Manager
Internal CD/DVD ROM Drive
Legacy Boot Order
► Internal Hard Drive
Internal 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.

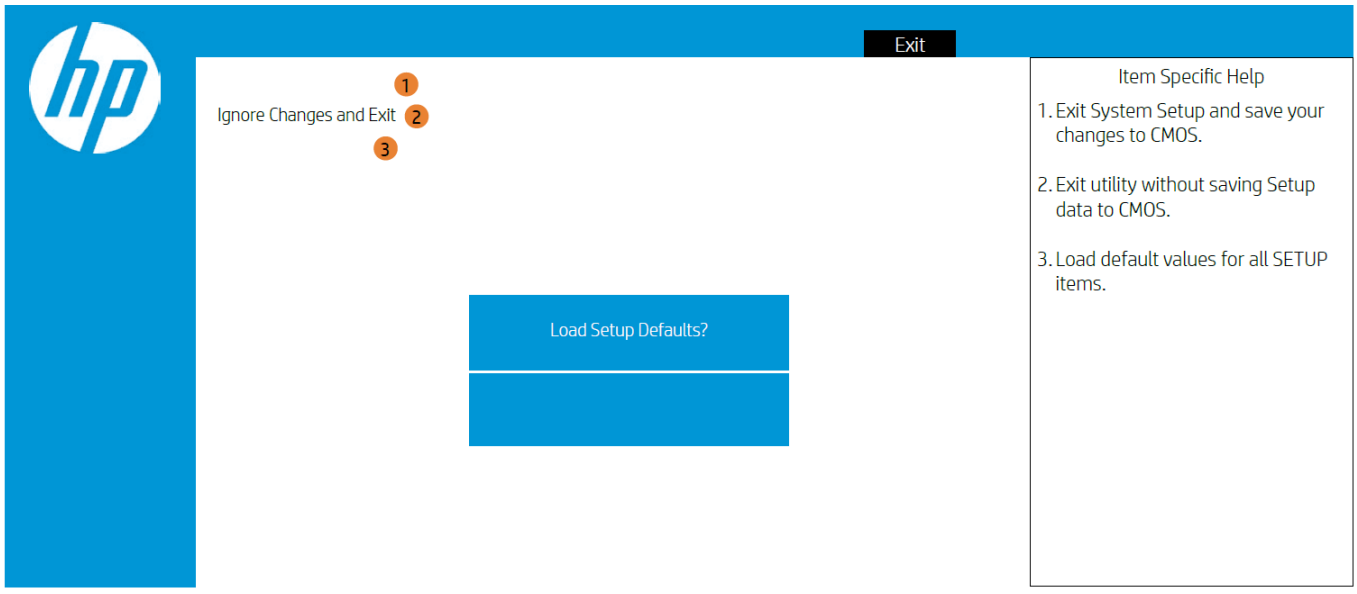

Boot Options
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Legacy Support
Platform Key
Enrolled MSFT
Pending Action
None
Load HP Factory Default Keys
Load MSFT Debug Policy Keys
UEFI Boot Order
► OS Boot Manager
Internal CD/DVD ROM Drive
Legacy Boot Order
► Internal Hard Drive
Internal CD/DVD ROM Drive
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
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Legacy Support
Platform Key
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
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
Post Hotkey Delay (sec)
USB Boot
Network Boot
Network Boot Protocol
Legacy Support
Platform Key
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
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





Download PDF: HP M01 Series Desktop User Manual

References

- User Manual