# BIOS Utility Menus

Back to Welcome Page


Main


Security


Advanced


UEFI Drivers

- System Information
- System Diagnostics
- BIOS Event Log
- Update System BIOS

- Change Date and Time
- Set Machine Unique Data
- System IDs

- Replicated Setup
- Save Custom Defaults
- Apply Custom Defaults and Exit
- Apply Factory Defaults and Exit
- Ignore Changes and Exit
- Save Changes and Exit

☐ Suppress POST Errors

Item Specific Help

Security Advanced UEFI Drivers

➡ Show Advanced System Information

Security Advanced UEFI Drivers

➡ Show Basic System Information

Next >>>

Security Advanced UEFI Drivers

➡ Show Basic System Information

<<< Previous Next >>>

Security Advanced UEFI Drivers

➡ Show Basic System Information

<<< Previous

# HP PC Hardware Diagnostics UEFI

Please select a Language.

English

Cestina

Dansk

Deutsch

Nederlands

Espanol

eesti keel

Suomi

Francais

Hrvatski

Magyar

BIOS Event Log

- View BIOS Event Log
- Export to USB Key
- Clear BIOS Event Log on Next Boot

Item Specific Help

Help

View BIOS Event Log

Date Time Description

---

No event have been logged

Help

Item Specific Help

# Export to USB Key

The file cannot be accessed. Please insert a USB storage device and try again.

OK

Main | Security | Advanced | UEFI Drivers

HP Computer Setup

Update System BIOS

| | |
|---|---|
| Current System BIOS Version: | S22 Ver. 80.30.00 |
| Current BIOS Release Date: | 03/09/2020 |
| Installation Date of Current BIOS: | 03/31/2020 |
| Most Recent Update Check: | Never Checked |

---

➡ Check HP.com for BIOS Updates 1

☐ Lock BIOS Version 2

☐ Native OS Firmware Update Service

BIOS Rollback Policy: Unrestricted Rollback to older BIOS 3

➡ Minimum BIOS version

☐ Allow BIOS Updates Using a Network 4

➡ BIOS Update Preferences 5

➡ Network Configuration Settings 6

➡ Update System and Supported Device Firmware Using Local Media

Help

Item Specific Help

1. **Check HP.com for BIOS Updates**
   Checks for the latest BIOS release revision on the network, and lets the user decide whether to download the BIOS image and update System.

2. **Lock BIOS Version**
   If not selected, then BIOS updates are allowed, if selected then updates to BIOS are not allowed.

3. *Click on the field to see the options.*

4. **Allow BIOS Updates Using a Network**
   Enable/Disable automatic BIOS updates through the network in a scheduled basis.

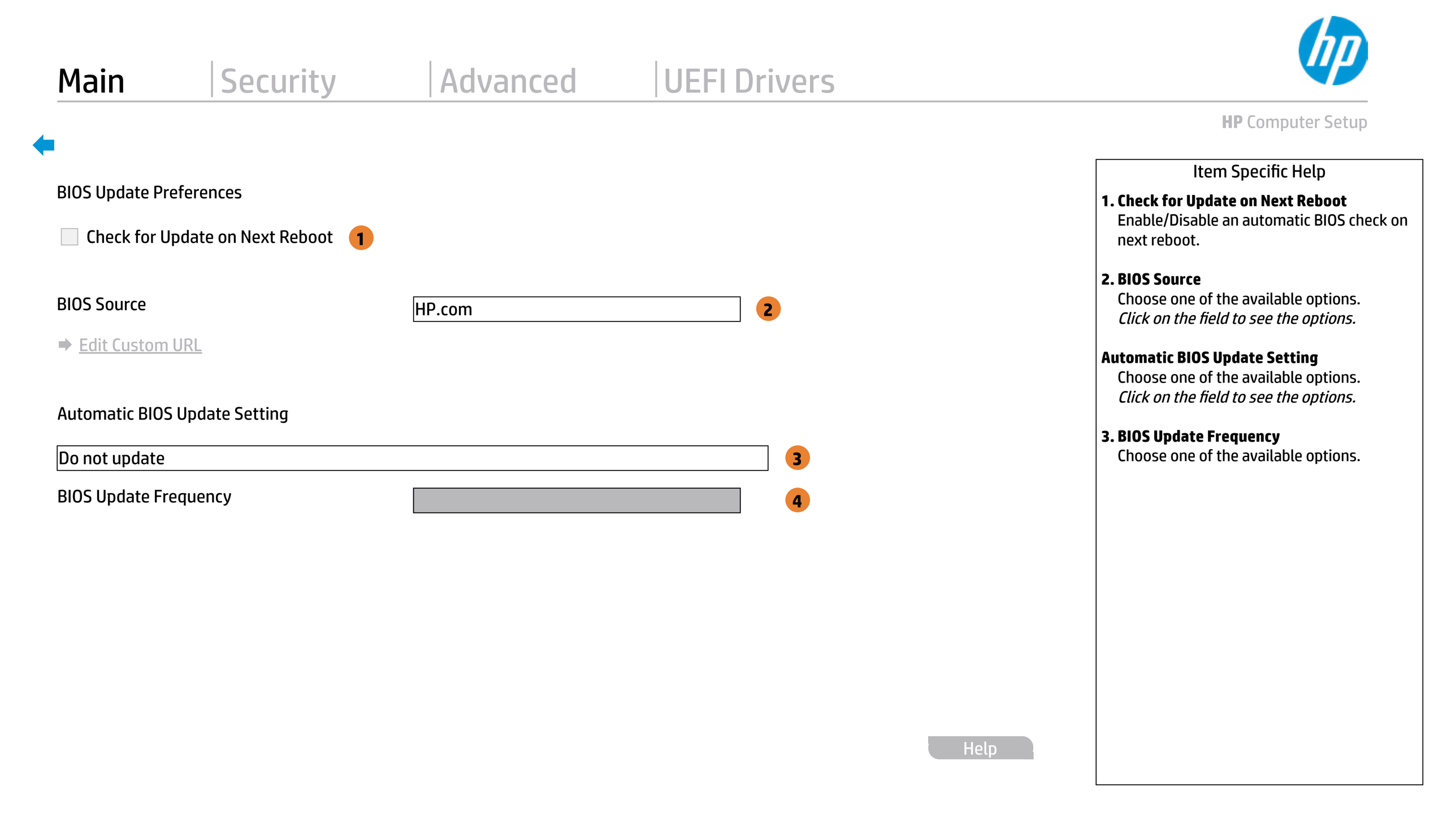
5. **BIOS Update Preferences**
   Sets the configurations to perform BIOS updates through the network.

6. **Network Configuration Settings**
   Configure network settings to be used for download and upload.

# Network BIOS Update

MS Windows Bitlocker Drive Encryption (BDE) may be enabled on your system.
HP requires that BDE be suspended temporarily before the BIOS is flashed and
that you obtain your BDE recovery password or recovery PIN before suspending BDE.
After the BIOS is updated, BDE can be resumed.

Continue Cancel


Main
Security
Advanced
UEFI Drivers
HP Computer Setup
BIOS Update Preferences
Check for Update on Next Reboot
1
BIOS Source
HP.com
2
Edit Custom URL
Automatic BIOS Update Setting
Do not update
3
BIOS Update Frequency
4
Help
Item Specific Help
1. Check for Update on Next Reboot
Enable/Disable an automatic BIOS check on next reboot.
2. BIOS Source
Choose one of the available options.
Click on the field to see the options.
Automatic BIOS Update Setting
Choose one of the available options.
Click on the field to see the options.
3. BIOS Update Frequency
Choose one of the available options.

Main | Security | Advanced | UEFI Drivers

HP Computer Setup

Network Configuration Settings

- [ ] Proxy Server 1
- Edit Proxy Server
- Test Network Connection 2

IPv4 Configuration — Automatic 3

- IPv4 Address
- IPv4 Subnet Mask
- IPv4 Gateway

DNS Configuration — Automatic 4

- DNS Addresses

Data transfer timeout — 100 5

- [ ] Force HTTP no-cache 6

Help

Item Specific Help

1. **Proxy Server**
   Enable/Disable the use of a proxy server.

2. **Edit Proxy Server**
   Specify the Proxy Server Address and the Port Number through the common-use <server>:<port> notation.

3. **Test Network Connection**
   Check the network connection using current BIOS update configuration.
   *Click on the field to see the options.*

4. **IPv4 Configuration**
   Setup for static IPv4 address.
   *Click on the field to see the options.*

5. **DNS Configuration**
   Configure a list of DNS addresses.

6. **Force HTTP no-cache**
   Disable HTTP caching.

Change Date And Time

| | |
|---|---|
| Set Date (MM/DD/YYYY) | 09 / 24 / 2019 |
| Set Time (HH:MM): | 02 : 56 |

Item Specific Help

Help

Main | Security | Advanced | UEFI Drivers

HP Computer Setup

- Feature Byte
- Build ID
- Serial Number
- SKU Number
- Product Family
- System Board CT Number
- Product Name

Item Specific Help

Help

Feature Byte

Current Setting: 3E3X476J6S6b7B7H7M7Q7T7W7maBapaqaubhdUdpdqfNfPhKjhk8.Qn

Build ID

Current Setting: 20WWQ6AT6av#SABA#DABA

Press the space key followed by the enter key to clear current setting

Serial Number

Current Setting: 8CC014047R

Press the space key followed by the enter key to clear current setting

SKU Number

Current Setting: F93PVT#070

Press the space key followed by the enter key to clear current setting

Product Family

Current Setting: 103C_53307F HP ProDesk

Press the space key followed by the enter key to clear current setting

System Board CT Number

Current Setting: PJLHVX48JDI019

Press the space key followed by the enter key to clear current setting

Product Name

Current Setting: HP EliteDesk 800

Press the space key followed by the enter key to clear current setting

System IDs

- Asset Tracking Number
- Ownership Tag

Item Specific Help

Help

Asset Tracking Number

Current Setting: 8CC014047R

Press the space key followed by the enter key to clear current setting

Ownership Tag

Current Setting:

Press the space key followed by the enter key to clear current setting

Replicated Setup

- Backup current settings to USB device
- Restore current settings from USB device

Item Specific Help

Help

Administrator Tools

- ➡ Create BIOS Administrator Password 1
- ➡ Create POST Power-On Password
- ➡ Password Policies
- ➡ Administrator Authentication Policies
- ☐ Fingerprint Reset on Reboot

Security Configuration

- ➡ TPM Embedded Security
- ➡ BIOS Sure Start
- ➡ Secure Boot Configuration
- ➡ Secure Platform Management (SPM)
- ☐ Physical Presence Interface 2
- ➡ Smart Cover

Intel Software Guard Extension (SGX) [Sofware control] 3

Utilities

- ➡ Hard Drive Utilities

Absolute® Persistence Module Current State

Activation Status : Inactive

Absolute® Persistence Module Permanent Disable : No

- ☐ System Management Command
- ➡ Restore Security Settings to Factory Defaults

Item Specific Help

**1. Create BIOS Administrator Password**
The Administrator password controls access to the following features:

- Setup Menu (F10)
- 3rd Party Option ROM Management (F3)
- Update System ROM
- WMI Commands that change system settings
- BIOS Configuration Utility (BCU)
- Alternative Power-On Password

**2. Physical Presence Interface**
When this feature is set to “Enable”, then the user is notified on system power up when changes are made to system security policy, and the user must manually agree to those changes before the change is confirmed

**3. Intel Software Guard Extensions (SGX)**
Enable/Disable Software Guard Extensions (SGX)

# BIOS Administrator Password

Enter BIOS Administrator Password

# POST Power-On Password

Enter POST Power-On Password

TPM Embedded Security

| | |
|---|---|
| TPM Specification Version | 2.0 |
| TPM Device | Available (1) |
| TPM State (2) | |
| Clear TPM | No |
| TPM Activation Policy | Allow user to reject |

Item Specific Help

**1. TPM Device**
Exposes the integrated Trusted Platform Module (TPM) for use.
*Click on the field to see the options.*

**TPM State**
Enables the integrated Trusted Platform Module (TPM).

BIOS Sure Start

- [ ] Verify Boot Block on every boot

BIOS Data Recovery Policy: Automatic

- [x] Dynamic Runtime Scanning of Boot Block
- [ ] Sure Start BIOS Settings Protection 1
- [x] Sure Start Secure Boot Keys Protection
- [x] Enhanced HP Firmware Runtime Intrusion Prevention and Detection 2

Sure Start Security Even Policy: Log Event Only 3

Sure Start Security Event Boot Notification: Time out after 15 seconds

## Item Specific Help

**1. Sure Start BIOS Settings Protection**

When enabled, HP Sure Start will lock all critical BIOS settings and provide enhanced protection for these settings via the HP Sure Start non-volatile (flash) memory

- The BIOS administrator credentials must be set to enable this setting
- See HP Sure Start documentation for details on which BIOS settings are protected

**2. Enhanced HP Firmware Runtime Intrusion Prevention and Detection**

Enables monitoring of HP system firmware executing out of main memory while the user Operating System is running.

Any anomalies detected in HP System firmware that is active while the user operating system is running will result in a Sure Start Security Event being generated.

*Click on the field to see the options.*

**3. Sure Start Security Event Policy**

This setting controls HP Sure Start behavior upon identifying a critical security event (any modification to HP firmware) during OS runtime.

- Log event only - HP Sure Start will log all critical security events m the HP Sure Start Audit log within the HP Sure Start non-volatile (flash) memory
- Log Event and notify user: In addition to logging all critical security events. HP Sure Start will notify the user within thr operating system that a critical event has occurred
- Log Event and power off system: In addition to logging all critical events. HP Sure Start will power off the system upon detecting a HP Sure Start Security Event. Due to the potential for data loss, use of this setting is only recommended in situations where security integrity of the system is a higher priority than the risk of potential data loss

Secure Boot Configuration

- [ ] Secure Boot

Secure Boot Key Management

- [x] Import Custom Secure Boot Keys
- [x] Clear Secure Boot keys
- [ ] Reset Secure Boot keys to factory defaults
- [x] Enable MS UEFI CA key

Access to the above settings requires Sure Start Secure Boot Keys Protection to be disabled

Ready BIOS for Device Guard Use: Do Nothing

Requires BIOS Administrator credentials to be configured and Secure Boot to be enabled.

Item Specific Help

Smart Cover

Cover Removal Sensor: Disable

Item Specific Help

Secure Platform Management (SPM)

NOTE: Some actions may not be selectable due to a pending password change.

SPM

SPM Current State: Not provisioned

➡ Unprovision SPM

HP Sure run

HP Sure Run Current State: Inactive

➡ Deactivate HP Sure Run

Enhanced BIOS Authentication Mode (EBAM)

EBAM Current State: Disabled

➡ Disable EBAM

Local Access Key: Not Present

➡ Clear EBAM Local Access Key(s) and Reboot

Item Specific Help

1. **Create BIOS Administrator Password**
   The Administrator password controls access to the following features:
   - Setup Menu (F10)
   - 3rd Party Option ROM Management (F3)
   - Update System ROM
   - WMI Commands that change system settings
   - BIOS Configuration Utility (BCU)
   - Alternative Power-On Password

2. **Physical Presence Interface**
   When this feature is set to “Enable”, then the user is notified on system power up when changes are made to system security policy, and the user must manually agree to those changes before the change is confirmed

3. **Intel Software Guard Extensions (SGX)**
   Enable/Disable Software Guard Extensions (SGX)

Hard Drive Utilities

Save/Restore MBR of the system hard drive is only available with drives that have a Master Boot Record.

- [ ] Save/Restore GPT of System Hard Drive 1

Boot Sector (MBR/GPT) Recovery Policy | Local user control

➡ DriveLock/Automatic DriveLock

➡ Secure Erase

- [ ] Allow OPAL Hard Drive SID Authentication

Help

Item Specific Help

1. **Save/Restore GPT of System Hard Drive**
   Enabling this feature will save the GUID Partition table (GPT) of the system Hard Drive. If the GPT is subsequently changed the user will he prompted to choose whether to restore GPT.

Select a Drive

➡ SATA 0: WDC WD10SPZX-60Z10T0 1

Help

Item Specific Help

**1. SATA 0: WDC WD10SPZX-60Z10T0**
Set HDD Password

DriveLock Security Options

The hard drive’s security state cannot be changed.

Cycle power to manage DriveLock on this drive.

Item Specific Help

Help

# Set DriveLock Password

Please exercise caution when using DriveLock.
Losing the passwords will render a drive premanently unusable.

Please be aware these settings take place immediately: save not necessary.

Enter DriveLock Master Password.

Select a Drive

SATA 0: WDC WD10SPZX-60Z10T0 (Drive is Locked)

Item Specific Help

Help

# BIOS Administrator Password

Enter BIOS Administrator Password

- Display Language
- Scheduled Power-On

- Boot Options
- HP Sure Recover
- System Options
- Built-In Device Options
- Port Options 1
- Power Management Options
- Remote Management Options
- Electronic Labels

Remote HP PC Hardware Diagnostics

- Settings 2
- Execute Remote HP PC Harware Diagnostics 3

Item Specific Help

1. **Port Options**
   Enable/Disable Port Settings

2. **Settings**
   Set the configuration for Remote HP PC Hardware Diagnostics, including the URLs used for download and upload, the scheduled execution frequency, etc.

3. **Execute Remote HP PC Harware Diagnostics**

Main | Security | Advanced | UEFI Drivers

HP Computer Setup

Display Language

| | |
|---|---|
| Select Language | English |
| Select Keyboard Layout | English |

Item Specific Help

Scheduled Power-On

- [ ] Sunday
- [ ] Monday
- [ ] Tuesday
- [ ] Wednesday
- [ ] Thursday
- [ ] Friday
- [ ] Saturday

| | |
|---|---|
| Hour | 0 |
| Minute | 0 |

Item Specific Help

Boot Options

Startup Delay (sec.) 0

- [ ] Fast Boot
- [ ] USB Storage Boot
- [ ] Network (PXE) Boot

After Power Loss Power Off (1)

- [ ] Prompt on Memory Size Change
- [ ] Prompt on Fixed Storage Change
- [ ] Audio Alerts During Boot
- [ ] NumLock on at boot
- [ ] UEFI Boot Order

---

M.2 SSD 1: Windows Boot Manager
USB:
NETWORK BOOT: IPV4 Network - Intel(R) Ethernet Connection (11) I219-LM
NETWORK BOOT: IPV6 Network - Intel(R) Ethernet Connection (11) I219-LM

---

Item Specific Help

1. **After Power Loss**
   Determine the system's state after power is lost to the unit.

HP Sure Recover

- [ ] HP Sure Recover 1
- [ ] Recover from Network 2
- [ ] Recover after Boot Failure 3

Recover Agent

URL: ftp://ftp.hp.com/pub/pcbios/CPR

Username:

Provisioning Version: 0

Recovery Image

URL:

Username:

Provisioning Version: 0

OS Recovery Image Version:

OS Recovery Driver Version:

Item Specific Help

1. **HP Sure Recover**
   If this setting is enabled, the system firmware will honor local and remote requests to reinstall the OS. If it is disabled, all requests to reinstall the OS will be ignored.

2. **Recover from Network**
   If this setting is enabled, the system firmware will obtain the recovery agent from the network. Otherwise, the system firmware will obtain the recovery agent from a local drive.

3. **Recover after Boot Failure**
   If this setting is enabled and no bootable UEFI OS is found, the system firmware will launch HP Sure Recover.

System Options

- [ ] Configure Storage Controller for RAID
- [ ] Configure Storage Controller for Intel Optane
- [ ] Turbo-Boost
- [ ] Hyperthreading 1
- [ ] Virtualization Technology (VTx)
- [ ] Virtualization Technology for Directed I/O (VTd)
- [ ] DMA Protection

Pre-boot DMA protection: Thunderbolt Only

- [ ] M.2 SSD 1
- [ ] M.2 SSD 2
- [ ] M.2 WLAN/BT

Power Button Override: disable

- [ ] USB Type-C Connector System Software Interface (UCSI) 2
- [ ] HP Application Driver
- [ ] Intel Dynamic Tuning 3

Item Specific Help

1. **Hyperthreading**
   Permits the user to control the processor capability

2. **USB Type-C Connector System Software Interface (UCSI)**
   The UCSI option should be disabled if booting a Microsoft Windows 10 version before 1709 to avoid system stability issues.

3. **Intel Dynamic Tuning**
   Previously called “Dynamic Platform and Thermal Framework (DPTF)”

## Built-In Device Options

| | |
|---|---|
| Embedded LAN Controller | |
| Wake On LAN | Disabled |
| Dust Filter | |
| Dust Filter Reminder (Days) | |
| Video memory size | 32 MB |
| Audio Device | |
| Microphone | Enable |
| Internal Speakers | |
| Increase Idle Fan Speed(%) | 0 |
| M.2 USB / Bluetooth | |
| LAN/WLAN Auto Switching | |
| Wake on WLAN | |

Item Specific Help

Port Options

- [ ] Serial Port A

I/O Address A: Auto

- [ ] Front USB Ports 1
- [ ] Front USB Port 1
- [ ] Front USB Port 2
- [ ] Front USB Port 3
- [ ] Rear USB Ports 2
- [ ] Rear USB Port 1
- [ ] Rear USB Port 2
- [ ] Rear USB Port 3
- [ ] Rear USB Port 4
- [ ] USB Option Port
- [ ] USB Legacy Port Charging 3
- [ ] Front USB Type-C Downstream Charging
- [ ] SATA 0 4

Restrict USB Devices: Allow all USB Devices

Item Specific Help

1. **Front USB Ports**
   Hides the front USB ports from the OS

2. **Rear USB Ports**
   Hides the rear USB ports from the OS

3. **USB Legacy Port Charging**
   Enable USB Charging port for charging capability when system Hibernate/Shutdown

4. **SATA 0**
   Hides the SATA port from the OS

Power Management Options

- [ ] Runtime Power Management 1
- [ ] Extended Idle Power States 2
- [ ] S5 Maximum Power Savings 3
- [ ] SATA Power Management
- [ ] PCI Express Power Management 4
- [ ] Power On from Keyboard Ports 5
- [ ] Unique Sleep State Blink Rates

Item Specific Help

1. **Runtime Power Management**
   Enables Runtime Power Management.

2. **Extended Idle Power States**
   Increases the OS's Idle Power Savings.

3. **S5 Maximum Power Savings**
   Enabling this feature reduces the power of this system as much as possible in the S5 state. Power is removed from the wake up circuitry, the expansion slots and any management features while in SB.

4. **PCI Express Power Management**
   Enabling this option permits the PCI Express links to use Active State Power Management (ASPM) to enter low power states while not in use.

5. **Power On from Keyboard Ports**
   To wake up system from Hibernate/Shutdown via keyboard

Remote Management Options

- [ ] Intel Management Engine (ME) 1
- [ ] Intel Active Management Technology (AMT) 2
- [ ] USB Key Provisioning Support
- [ ] USB Redirection Support

Unconfigure AMT on next boot: Apply 3

SOL Terminal Emulation Mode: ANSI

- [ ] Show unconfigure ME Confirmation Prompt
- [ ] Verbose Boot Messages
- [ ] Watchdog Timer 4
  - OS Watchdog Timer (min.): 5
  - BIOS Watchdog Timer (min.): 5

CIRA Timeout (min.): 1 min 5

## Item Specific Help

1. **Intel Management Engine (ME)**
   Enabled by default. [Help Icon] = “This option allows for a user to disable the Intel Management Engine, which disables Intel Active Management Technology and all underlying Intel ME technologies. This option also disables ME functions that allow for ME firmware updates. It is suggested to periodically enable this option to update ME firmware, as the ME firmware may contains platform stability fixes.

2. **Intel Active Management Technology (AMT)**
   This option allows for a user to enable Intel Active Management Technology, which is tied to all ME-regulated remote management functions. Disabling AMT will still allow for ME firmware updates, which are recommended for receiving platform stability fixes.

3. **Unconfigure AMT on next boot**
   Perform AMT/ME unconfigure without password operation.

4. **Watchdog Timer**
   Enable/Disable WatchDog Timer.

5. **CIRA Timeout (min.)**
   Set CIRA Timeout (Minutes).

Remote HP PC Hardware Diagnostics

| | |
|---|---|
| Diagnostics Download URL | HP.com 1 |
| ➡ Custom Download Address | |
| Diagnostics Logs Upload URL | |
| ➡ Custom Upload Address 2 | |
| ➡ Username 3 | |
| ➡ Password 4 | |
| Scheduled Execution | Disable |
| Frequency | Daily 5 |
| Execute On Next Boot | Disable 6 |
| ➡ Last Execution Result | |

Item Specific Help

1. **Diagnostics Download URL**
   Select between HP server URL and a custom server URL.

2. **Custom Upload Address**
   Configure a URL for diagnostics logs upload.

3. **Username**
   Configure the username for uploading diagnostics logs to the server, if authentication is required.

4. **Password**
   Configure the password for uploading diagnostics logs to the server, if authentication is required.

5. **Frequency**
   Select the frequency for scheduled execution of Remote HP PC Hardware Diagnostics.

6. **Execute On Next Boot**
   Enable/disable the execution on next boot. The flag will be disabled after the diagnostics have run.

# Custom Upload URL

There is no Custom Upload URL configured.
Type a new Custom Upload URL and press ENTER to save.
Press ESC to CANCEL

# Custom Server Username

There is no Username configured.
Type a new Username and press ENTER to save.
Press ESC to CANCEL

# Custom Server Password

There is no Upload Server Password configured.
Type a new Upload Server Password and press ENTER to save.
Press ESC to CANCEL



This will restart the system into the 3rd Party Option ROM Management application. You can get to this application directly by pressing F3 during startup.

➡ 3rd Party Option ROM Management

Item Specific Help