HP BIOSphere Gen4

keep reinventing

Our industry leading firmware ecosystem automates the protection of the BIOS and enables robust manageability of your PC.

A Growing Threat

The BIOS is the first million lines of code run by your PC when you turn it on. It plays a critical role, communicating between your PC's hardware and your Operating System, which makes BIOS security and manageability increasingly important in the face of modern security threats.

Building on over a decade of BIOS security leadership, HP BIOSphere Gen 4[1] offers an ecosystem of protections to help defend your PC, including automated protections, customizable safeguards, and easy manageability to protect against attacks without interrupting employee productivity.

Protection Starts in the BIOS

HP BIOSphere Gen4 provides enhanced firmware protection, guarding against malicious attacks and accidental errors that can compromise the BIOS:

- **Hardware root of trust**—HP Pro and HP Elite PCs ensure you start up with an authentic BIOS, every time. (In PCs that also include HP Sure Start[2], corrupted BIOS' self-heal automatically).
- Enables protection of critical firmware elements, including the **Master Boot Record (MBR)** and **GUID Partition Table (GPT)**, against corruption or deletion that could render the PC unable to boot.
- HP BIOSphere Gen4 conforms to **NIST 800-147** and **ISO/IEC 19678:2015** to make sure that your BIOS only gets authentic updates from HP.
- Make BIOS updates as easy as a standard driver update—HP BIOSphere Gen4 can receive BIOS and Intel® ME updates deployed via Windows Update[3].

Guard Against Physical Attacks

Modern workstyles increasingly take PCs out of the office and into cafes, airports, and shared spaces where physical attacks become a greater risk.

HP BIOSphere Gen4 includes powerful protections against physical attacks that are simple to set up and customize, helping businesses of all sizes safeguard their PCs and protect sensitive information.

- Prevent unauthorized users from accessing your devices with pre-boot security features like **Power-on Authentication** and **HP DriveLock**.
- Protect your ports against malicious USB drives or attempts to steal data with **port controls**—with HP BIOSphere Gen4 you can enable/disable individual ports and block the ability to boot from USB.
- **Secure Erase4**—Permanently erase data from hard disk drives or solid state drives (SSD) to prevent data theft after you dispose of or repurpose old devices.

Advanced Manageability

HP BIOSphere allows IT teams to centrally configure and update BIOS settings across a PC fleet in just minutes—saving time and effort for IT administrators with straightforward configuration and management.

HP BIOS Configuration Utility[5] is a script driven tool that provides the ability to manage BIOS settings on PC's remotely. In addition, HP Manageability Integration Kit plug-in for Microsoft® System Center Configuration Manager can remotely manage HP BIOSphere settings and passwords.

Additional Features and Specifications

Standards and Protections

Conforms to ISO/IEC 19678:2015 **(NIST 800-147) and NIST 800-155**	HP BIOSphere Gen4 conforms to ISO/IEC 19678:2015 (NIST 800-147) to make sure that your BIOS only gets authentic, digitally signed updates from HP. It is further strengthened beyond these requirements by including hardware enforcement. Also supports BIOS integrity measurements as specified by **NIST 800-155**.
Master Boot Record (MBR) / GUID Partition Table (GPT) Protection & Recovery	Enables protection of the **Master Boot Record (MBR)** and **GUID Partition Table (GPT)** against corruption or deletion that could render the PC unable to boot. HP BIOSphere Gen4 can also backup and restore your MBR or GPT should it become corrupted or deleted. Users can also lock the Master Boot record to prevent it from being altered. These features can be enabled in the BIOS settings.
Hardware-based root of trust	Hardware-enforced assurance that an authentic BIOS is present before the CPU starts executing code to boot.
Secure Boot	Validates integrity and authenticity of the Operating System before allowing it to start.

Configurable Protections

Power-On Authentication[6]	Ensures that only authorized users can start up the PC or access the BIOS by requiring user authentication prior to system start-up. Power-On Authentication supports passwords or fingerprint identification[6].
HP DriveLock & HP Automatic DriveLock	Prevents notebook hard drives from running without authorization by requiring the BIOS to authenticate the user before the drive is unlocked. For convenience, if the user is already using Power-On Authentication, HP Automatic DriveLock can ensure fast, secure access without entering additional passwords.
HP One Step Logon	Simplifies your log-in process with Power-On Authentication using your Windows Credentials. Single Sign On gives you the protection of Power-On Authentication, without making you re-enter your credentials at the Windows login screen. Must be enabled using HP Client Security Manager Gen4.
Port Controls	**New in Gen4!** Protects against unwanted access with the ability to enable or disable individual USB ports and devices. Many devices now use USB-C™ to charge: if disabled, USB-C™ will still charge user devices and can be used to power the PC (available on select HP PCs).
Device Control	Allows administrators the option to individually disable integrated devices such as cameras, microphones, or Bluetooth as needed in their environment.
HP Secure Erase	Permanently erases data on hard drives to prepare a system for disposal or redeployment.

Other

BIOS Updates via Windows Update	**New in Gen4!** Updates the BIOS and Intel® ME through Windows Update or device manager, as easy as a standard driver update.
Automatic BIOS updates via network	Allows you to schedule automatic BIOS updates via the network. Dates and times are customizable in the F10 setup menu.
HP LAN-WLAN Protection	Protects enterprise LAN from unauthorized wireless bridging access by turning off wireless LAN on LAN insertion.
Power Management control	Allows for customization of power management and charging behavior.
Peak Shift	Reduces power consumption by auto-switching the system to battery power during preset peak hours of the day. Must be enabled via HP Power Manager or remotely via the HP Manageability Integration Kit.

Enterprise and Manageability Features

Replicated Setup	Enables you to easily save BIOS settings to a file—such as a USB key—and use them to clone configurations to other machines.
Device Guard Enablement (for Windows Enterprise users only)	Enhances system security by supporting the latest anti-malware protection features of Windows® 10, including Device Guard, which provides advanced malware protection by blocking anything other than trusted apps from running. Optimized for easy deployment locally or remotely via the MIK plugin.
HP MAC Address Manager	Allows unique network controller address associated with the platform itself to be used for cabled docks & network adapters, regardless of the power state of the platform which is critically important to many IT existing image deployment and remote management workflows. **New in Gen4:** Includes host based MAC address over USB-C™. Works regardless of what power state the notebook is in when the dock is attached. Use the system's MAC address when docked, rather than the dock's address—helps administrators to identify systems, regardless of where they are docked. Dock must support host-based MAC address.
HP Wireless Wakeup	Allows magic packet configuration to wake up system from sleep standby through WLAN adaptors.
Remote Diagnostics	Ability to remotely run and get advanced diagnostics log on a system, even if diagnostics are not installed or there is no image on the drive.

Frequently asked questions:

Q: I have a growing business but no IT department. Can I still benefit from HP BIOSphere Gen4?

A: Absolutely. HP BIOSphere Gen4 includes protections that are enabled by default, as well as capabilities like Power-On Authentication and port controls that can easily be set up on each PC by pressing F10 on start-up to enter the BIOS.

Q: What platforms have HP BIOSphere Gen4?

A: HP BIOSphere Gen4 is available on HP Pro and HP Elite PCs (with 8th Gen processors). Features vary by platform and configuration.

Q: What kind of attacks does HP BIOSphere Gen4 protect against?

A: HP BIOSphere Gen4 can help protect against a variety of attacks or corruption, including attacks that target the MBR or GPT; attacks that attempt to enter through unauthorized wireless bridging; and more, including new types of malware that may be created to target the BIOS in the future.

It can also help protect against physical attacks on the device, with features like BIOS passwords, port controls, and HP Secure Erase.

Q: What happens when I need to update the BIOS?

A: HP supports updating the BIOS through multiple methods, including Windows Update, HP Support Assistant, and with the ability to configure scheduled automatic BIOS updates.

Q: I'm an IT manager and need to configure BIOS settings on multiple PCs. Can HP BIOSphere Gen4 help with this?

A: Yes. For small businesses, **Replicated Setup** enables you to easily save BIOS settings to a file—such as a USB key—and use them to clone configurations to other machines.

Companies with managed IT can also set up a standardized BIOS configuration on all new PCs from one central location, using the **HP BIOS Configuration Utility**. This automated process takes just minutes, resulting in lower IT costs and greater productivity.

Companies using Microsoft® System Center Configuration Manager to manage their fleet can also configure BIOS settings remotely with the HP Manageability Integration Kit Gen2[7].

Learn more at www.hp.com/go/computersecurity

[1] HP BIOSphere Gen4 is available on HP Elite and Pro platforms with 8th Gen Intel or AMD processors. Features may vary by platform and configuration.
[2] HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with Intel® 8th generation processors.
[3] BIOS updates via Windows Update are available on all HP Elite and HP Pro PCs with Intel or AMD 6th gen or higher processors. Intel ME updates via Windows Update are available on HP Elite and HP Pro PCs with Intel 8th gen processors.
[4] HP Secure Erase—For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method.
[5] The HP BIOS Configuration Utility can be downloaded at http://www.hp.com/go/clientmanagement.
[6] Desktop PCs only support password authentication.
[7] HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.