

HP BIOSphere

An ecosystem of protections to defend your PC



Attacks on the BIOS can be difficult to detect. Fortunately, the HP BIOSphere ecosystem automates the protection of the BIOS and enables robust PC manageability.

Table of Contents

Why Is BIOS Important?.....	2
HP BIOSphere Helps Defend Your PC.....	3
Automated Protection.....	4
Customizable Safeguards Against Physical Attacks.....	5
Flexible and Customizable Management.....	5
BIOSphere Gen6 Features.....	5
BIOSphere Generations.....	5
Setup Information.....	5
Conclusion.....	6

Why is BIOS Important?

An unsecured BIOS can offer a dangerous amount of access to a hacker and cyber-attacks targeting the BIOS are on the rise. Hackers often gain access to the BIOS via phishing attacks.

Physically present attackers can quickly disassemble the system and establish a direct connection to the non-volatile storage device on the circuit board to inject malware. Malware can also be introduced via unsecured ports.

BIOS level attacks are very difficult to detect because they control the device below the operating system and cannot be removed or modified by anti-virus software. Malware targeting the BIOS can continually supply data and reinstate itself after network defenses deploy. A compromised BIOS can remain hidden, disable other security measures on the PC, and even survive a disk wipe and operating system reinstallation.

HP BIOSphere Helps Defend Your PC

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

HP BIOSphere can help protect against a variety of attacks or corruption, including attacks that target the Master Boot Record (MBR) and GUID Partition Table (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.

Automated Protection

HP BIOSphere Gen6 provides enhanced firmware protection automatically from the moment the PC is first booted up, guarding against malicious attacks and accidental errors that can compromise the BIOS.

HARDWARE ROOT OF TRUST	At every boot, HP Pro and Elite PCs ensure that an authentic BIOS is present before the CPU starts executing code. ¹ (In PCs that also include HP Sure Start ² , corrupted BIOS can self-heal automatically.)
SECURE BOOT	When HP business PCs are manufactured, the Unified Extensible Firmware Interface (UEFI) creates a list of keys that identify trusted hardware, firmware, and operating system loader code. It also creates a list of keys to identify known malware. Secure Boot uses these keys to define and block potential threats before they can attack or infect the PC. For example, Secure Boot can prevent PCs from starting from illegally copied CDs or DVDs that could harm the computer. Secure Boot does not lock out valid recovery discs or Windows [®] discs.
CRITICAL FIRMWARE PROTECTION	HP BIOSphere Gen6 implements NIST 800-147 and ISO/IEC 19678:2015, to make sure the BIOS only gets authentic updates from HP. Other key security standards it implements include draft NIST 800-155, UEFI Secure Boot, and Trusted Computing Group.
MEETS SECURITY STANDARDS	Elements such as the MBR or GPT are protected against corruption or deletion that could render the PC unable to boot.
SIMPLE BIOS UPDATES	HP BIOSphere Gen6 can receive BIOS and Intel [®] ME updates deployed via Windows Update, making it as easy as a standard driver update. ³ Automatic updates can even be scheduled via the network, with customizable dates and times.

Customizable Safeguards 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 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.

PRE-BOOT SECURITY	Prevent unauthorized users from accessing devices with features like Power-on Authentication and HP DriveLock.
PORT CONTROLS	Protect ports against malicious USB drives or attempts to steal data. HP BIOSphere Gen6 allows users to enable/disable individual ports and block the ability to boot from USB. (Many devices now use USB-C® to charge user devices; if disabled, USB-C® will still charge and can be used to power the PC. Available on select HP PCs.)
SECURE ERASE	Permanently erase data from hard disk drives or solid-state drives (SSD) to prevent data theft after disposing of or repurposing old devices. ⁴

Flexible and Customizable Management

HP BIOSphere Gen6 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.

REPLICATED SETUP	For small businesses, Replicated Setup enables users to easily save BIOS settings to a file—such as a USB key—and use them to clone configurations to other machines.
REMOTE BIOS MANAGEMENT	<p>Companies with managed IT can centrally configure and update BIOS settings across a PC fleet in just minutes, using the HP BIOS Configuration Utility.⁵ This script-driven tool provides admins the ability to remotely manage BIOS settings on PCs.</p> <ul style="list-style-type: none">• Read available BIOS settings and their values from a supported desktop, workstation, or notebook computer• Set or reset Setup Password on a supported desktop, workstation, or notebook computer• Replicate BIOS settings across multiple client computers <p>HP BIOSphere settings and passwords can also be managed remotely using the HP Manageability Integration Kit⁷ (MIK) for Microsoft® System Center Configuration Manager (SCCM). The MIK's BIOS Configuration interface allows the IT administrator to define and deploy BIOS settings policies to client computers.</p>

HP BIOSphere Gen6 Features

STANDARDS AND PROTECTIONS	
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 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.
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 SATA hard disk drives, solid state drives (SSD) and NVME 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 if supported by the drive.
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 Gen5 or later.
Port Controls	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 <i>NEW for Gen6</i>	Permanently erases data on hard disk drives, to prepare a system for disposal or redeployment if supported by the drive. HP BIOSphere Gen5: Permanently erases data on SATA hard disk drives, solid state drives (SSD). New for BIOSphere Gen6: HP BIOSphere Gen6 adds support NVME Drives.
Integrated Camera Control <i>NEW for Gen6</i>	F10 Hotkey support for managing camera privacy (toggle on/off).
OTHER	
BIOS Updates via Windows Update	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. Replicated setup with BCU will work with Windows and Linux (if HP Sure Admin8 is disabled).
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. Device Guard requires: BIOS Admin Password, Virtualization, Secure Boot to be enabled. Removeable and Network devices and the Microsoft UEFI CA key will be disabled. The Device Guard BIOS setting simplifies managing these other BIOS settings. Device Guard is 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.
HP Wireless Wakeup	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.
Remote Diagnostics	Allows magic packet configuration to wake up system from sleep standby through WLAN adaptors.
UEFI Wi-Fi <i>NEW for Gen6</i>	UEFI WiFi enables HP select notebook platforms to use WPA2-Personal & select WPA2-Enterprise protocols (EAP-TLS, EAP-TTLS, and EAP-PEAP) to perform secure preboot wireless network connectivity for BIOS update/configuration and OS update/recovery operations. Examples of enabled UEFI WiFi use cases are: preboot network join/authentication, BitLocker Unlock, PXE Boot, OS Recovery, HP Sure Recover, Remote HP PC Hardware Diagnostics, System BIOS Updates, etc. UEFI WiFi has been added to select platforms which are configured with the current generation of Intel CPUs and Intel Wireless LAN Modules. For more details on enabling and configuring UEFI WiFi support please see the whitepaper and for remote management support also see MIK .
UEFI Secure Boot <i>NEW for Gen6</i>	BIOSphere validates the integrity and authenticity of the Operating System before allowing it to start. BIOSphere Gen6 enhances platform security with Secure Boot support, increased to UEFI Class 3 (legacy removal) on platforms with supported CPUs.

HP BIOSphere Generations

HP BIOSphere	2015	<ul style="list-style-type: none"> • Boot block recovery if corrupted or compromised (Sure Start) • Run time monitoring of BIOS code stored in public flash (Sure Start)
HP BIOSphere Gen2	2016	<ul style="list-style-type: none"> • Lock BIOS to disallow BIOS update • Network configuration settings for BIOS update • Intel Trusted Execution Technology (TXT) support • Intel Software Guard Extensions (SGX) support • Power Management control • Boot from Thunderbolt interface • Thunderbolt disable/enable control and configuring security level • Internal speaker, internal microphone, and headphone output enable/disable control • Configure Option ROM Launch Policy
HP BIOSphere Gen3	2017	<ul style="list-style-type: none"> • Windows 10 Device Guard enablement • GUID Partition Table (GPT) protection and recovery • HP Lan/WLAN protection (preventing unauthorized bridging) • HP MAC Address Manager • HP Wireless Wakeup from sleep through WLAN adapter

HP BIOSphere Gen4	2018	<ul style="list-style-type: none"> • Individual USB/SATA port control (enable / disable) • Remote Diagnostics • Combined Intel Management Engine and HP BIOS update • BIOS update via Windows Update • Host-based MAC address over USB-C®
HP BIOSphere Gen5	2019	<ul style="list-style-type: none"> • HP Secure Platform Management (SPM). Options for managing HP Sure Run and HP Sure Recover on applicable platforms. • Enhanced BIOS Authentication Mode (aka HP Sure Admin)
HP BIOSphere Gen6	2020	<ul style="list-style-type: none"> • HP Secure Erase support for NVME drives • HP Privacy Camera – F10 hotkey support for managing camera privacy (on/off) • UEFI WiFi support on HP notebook platforms • UEFI Secure Boot increased to UEFI class 3

Setup Information

HP BIOSphere can help safeguard your PC while saving IT valuable management time. This industry-leading firmware is exclusively available on select HP business PCs.¹

For additional information on the HP Commercial BIOS Setup, please visit our [Setup Guide](#). For additional information on HP features that leverage HP BIOS capabilities, refer to the [HP Security Site](#).

1. HP BIOSphere Gen6 features may vary depending on the platform and configuration.
2. HP Sure Start Gen6 is available on select HP PCs.
3. BIOS updates via Windows Update are available on all HP Elite and HP Pro PCs with Intel® or AMD® 6th generation or higher processors. Intel® ME updates via Windows Update are available on HP Elite and HP Pro PCs with Intel® 11th generation processors.
4. For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method. HP Secure Erase does not support platforms with Intel® Optane™.
5. The HP BIOS Configuration Utility can be downloaded [here](#).
6. Desktop PCs only support password authentication.
7. HP Manageability Integration Kit can be downloaded from [here](#).
8. HP Sure Admin requires Windows 10, HP BIOS, HP Manageability Integration Kit from <http://www.hp.com/go/clientmanagement> and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store. For information on HP Sure Admin, please click [here](#).

Learn more at hp.com/go/computersecurity.

© Copyright 2020 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. AMD and Cezanne are trademarks of Advanced Micro Devices, Inc. USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum. Intel and Thunderbolt are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

