

# HP BIOSphere Gen4



keep reinventing

Il nostro ecosistema firmware leader di settore consente di automatizzare la protezione del BIOS e garantisce una gestibilità avanzata del PC.

## Una minaccia in costante crescita

Il BIOS è composto dal primo milione di righe di codice che il PC esegue quando viene acceso. Svolge un ruolo essenziale di comunicazione tra l'hardware del PC e il sistema operativo, e per questo la sicurezza e la gestibilità del BIOS sono sempre più importanti alla luce delle moderne minacce alla sicurezza.

Frutto di una leadership decennale nella protezione del BIOS, HP BIOSphere Gen 4<sup>1</sup> contribuisce a difendere il PC grazie a un ecosistema di strumenti automatizzati e personalizzabili e a soluzioni di gestione che permettono di proteggere il sistema dagli attacchi senza ridurre la produttività.

## La protezione comincia dal BIOS

HP BIOSphere Gen4 offre protezione avanzata del firmware contro attacchi dannosi ed errori accidentali che possono compromettere il BIOS:

- **Root of Trust basato su hardware:** i PC HP Pro e HP Elite garantiscono sempre l'avvio di un BIOS originale. (Nei PC che includono anche HP Sure Start<sup>2</sup>, il BIOS danneggiato è in grado di ripararsi automaticamente).
- Consente la protezione di elementi critici del firmware, tra cui il **Master Boot Record (MBR)** e il **GUID Partition Table (GPT)**, contro guasti e cancellazioni che potrebbero impedire l'avvio del PC.
- HP BIOSphere Gen4 è conforme agli standard **NIST 800-147** e **ISO/IEC 19678:2015** per consentire la ricezione solo di aggiornamenti del BIOS originali HP.
- Gli aggiornamenti del BIOS sono semplici come quelli di un driver: HP BIOSphere Gen4 può ricevere aggiornamenti BIOS e Intel® ME tramite Windows Update<sup>3</sup>.

## Protezione contro gli attacchi fisici

Lo stile di lavoro moderno porta ad utilizzare sempre più spesso il PC lontano dall'ufficio, nei caffè, negli aeroporti o negli spazi condivisi dove gli attacchi fisici possono essere sempre in agguato.

HP BIOSphere Gen4 include robuste protezioni contro gli attacchi fisici che possono essere configurate e personalizzate in tutta semplicità, per aiutare le aziende a salvaguardare i PC di loro proprietà e le informazioni sensibili in essi contenute.

- Gli utenti non autorizzati non possono accedere ai vostri dispositivi, grazie a funzionalità di sicurezza pre-avvio quali l'**autenticazione all'avvio** e **HP DriveLock**.
- Protezione contro le unità USB dannose o i tentativi di furto dei dati grazie al **controllo delle porte**: con HP BIOSphere Gen4 è possibile abilitare/disabilitare le singole porte ed escludere la possibilità di avvio da USB.
- **Secure Erase4**: eliminazione permanente dei dati da unità disco rigido o unità a stato solido (SSD) per impedire il furto dei dati dopo lo smaltimento o la riconversione di dispositivi.

## Gestibilità avanzata

HP BIOSphere consente ai team IT di configurare e aggiornare in modo centralizzato le impostazioni del BIOS per un intero parco PC, semplificando così la gestione da parte degli amministratori IT.

HP BIOS Configuration Utility<sup>5</sup> è uno strumento basato su script che consente di gestire in remoto le impostazioni del BIOS sui PC. Inoltre, il plug-in HP Manageability Integration Kit per Microsoft® System Center Configuration Manager può gestire in remoto le impostazioni e le password di HP BIOSphere.

## Funzionalità aggiuntive e specifiche

### Standard e protezioni

<b>Conforme a ISO/IEC 19678:2015 (NIST 800-147) e NIST 800-155</b>	HP BIOSphere Gen4 è conforme allo standard ISO/IEC 19678:2015 (NIST 800-147) per garantire che il BIOS riceva solo aggiornamenti originali e con firma elettronica di HP. Viene inoltre ulteriormente rafforzato oltre tali requisiti grazie all'applicazione tramite hardware. Supporta anche le misurazioni dell'integrità del BIOS secondo la specifica <b>NIST 800-155</b> .
<b>Protezione e ripristino Master Boot Record (MBR) / GUID Partition Table (GPT)</b>	Consente la protezione di <b>Master Boot Record (MBR)</b> e <b>GUID Partition Table (GPT)</b> contro guasti e cancellazioni che potrebbero impedire l'avvio del PC. HP BIOSphere Gen4 può anche effettuare il backup e il ripristino di MBR o GPT nel caso di guasti o cancellazioni. Inoltre gli utenti possono bloccare il Master Boot Record per impedire che venga modificato. Questa funzionalità può essere abilitata nelle impostazioni del BIOS.
<b>Root of trust basato su hardware</b>	L'applicazione tramite hardware garantisce la presenza di un BIOS originale prima che la CPU cominci ad eseguire il codice dell'avvio.
<b>Avvio sicuro</b>	Convalida l'integrità e l'autenticità del sistema operativo prima di consentirne l'avvio.

### Protezioni configurabili

<b>Autenticazione all'avvio<sup>6</sup></b>	Garantisce che solo gli utenti autorizzati possano avviare il PC o accedere al BIOS richiedendo l'autenticazione dell'utente prima dell'avvio del sistema. L'autenticazione all'avvio supporta l'identificazione mediante password o impronte digitali <sup>6</sup> .
<b>HP DriveLock e HP Automatic DriveLock</b>	Impedisce il funzionamento dell'unità disco rigido del notebook in mancanza di autorizzazione, richiedendo al BIOS di autenticare l'utente prima di sbloccare l'unità. Per praticità, se l'utente utilizza già l'autenticazione all'avvio, HP Automatic DriveLock può consentire l'accesso rapido e sicuro senza l'aggiunta di ulteriori password.
<b>HP One Step Logon</b>	Semplifica il processo di accesso con autenticazione all'avvio utilizzando le credenziali Windows dell'utente. Il single sign-on offre la protezione dell'autenticazione all'avvio, senza la necessità di inserire nuovamente le proprie credenziali alla schermata di accesso di Windows. Deve essere abilitato mediante HP Client Security Manager Gen4.
<b>Controlli delle porte</b>	<b>Novità in Gen4!</b> Protezione contro gli accessi non autorizzati con la possibilità di abilitare o disabilitare singole porte USB e dispositivi. Molti dispositivi ora utilizzano USB-C™ per la ricarica: anche se disabilitata, la tecnologia USB-C™ ricarica comunque i dispositivi utente e può essere utilizzata per alimentare il PC (disponibile su alcuni PC HP).
<b>Controllo dei dispositivi</b>	Consente agli amministratori di scegliere i singoli dispositivi integrati da disabilitare, ad esempio videocamere, microfoni o Bluetooth, in base all'ambiente.
<b>HP Secure Erase</b>	Consente di eliminare in modo permanente i dati sull'unità disco rigido per preparare un sistema per lo smaltimento o la riconversione.

### Altro

<b>Aggiornamenti del BIOS tramite Windows Update</b>	<b>Novità in Gen4!</b> Gli aggiornamenti del BIOS e di Intel® ME vengono distribuiti mediante Windows Update o Device Manager, con una semplicità paragonabile all'aggiornamento di un driver standard.
<b>Aggiornamenti automatici del BIOS tramite rete</b>	Consente di programmare gli aggiornamenti automatici del BIOS tramite rete. La data e l'ora sono personalizzabili nel menu di configurazione premendo F10.
<b>Protezione HP LAN-WLAN</b>	Protegge la LAN aziendale dall'accesso bridging wireless disattivando la LAN wireless all'inserimento della LAN.
<b>Controllo della gestione energetica</b>	Consente di personalizzare la gestione energetica e il comportamento di ricarica.
<b>Peak Shift</b>	Riduce il consumo energetico commutando automaticamente il sistema sull'alimentazione a batteria durante le ore di picco della giornata. Deve essere abilitato tramite HP Power Manager o in remoto tramite HP Manageability Integration Kit.

### Funzionalità di gestibilità e aziendali

<b>Replicated Setup</b>	Consente di salvare con facilità le impostazioni del BIOS in un file, ad esempio su una chiavetta USB, e di utilizzarle per clonare le configurazioni su altre macchine.
<b>Device Guard Enablement (solo per utenti Windows Enterprise)</b>	Aumenta la sicurezza del sistema grazie al supporto delle più recenti funzionalità di protezione anti-malware di Windows® 10, incluso Device Guard, che offre protezione avanzata contro i malware bloccando l'esecuzione di qualunque applicazione che non sia affidabile. Ottimizzata per semplificare l'implementazione in locale o in remoto tramite il plug-in MK.
<b>HP MAC Address Manager</b>	Consente di utilizzare l'indirizzo univoco del controller di rete associato alla piattaforma per le dock cablate e le schede di rete, indipendentemente dallo stato di alimentazione della piattaforma. Si tratta di una funzionalità particolarmente importante per molte operazioni IT critiche di gestione da remoto e di implementazione delle immagini di sistema. <b>Novità in Gen4:</b> include indirizzo MAC basato su host tramite USB-C™. Funziona indipendentemente dallo stato di alimentazione del notebook quando collegato alla docking station. Utilizza l'indirizzo MAC di sistema, invece dell'indirizzo della docking station, e facilita quindi l'identificazione dei sistemi stessi. La docking station deve supportare l'indirizzo MAC basato su host.
<b>HP Wireless Wakeup</b>	Consente alla configurazione magic packet di "risvegliare" il sistema dallo stato di standby mediante adattatori WLAN.
<b>Diagnostica in remoto</b>	Possibilità di eseguire in remoto ed ottenere un log di diagnostica avanzata su un sistema anche se non dispone di strumenti di diagnostica installati o se non c'è un'immagine di sistema installata.

## Domande frequenti:

**D: La mia azienda è in crescita ma non dispone di un reparto IT. Posso comunque trarre vantaggio da HP BIOSphere Gen4?**

R: Certamente. HP BIOSphere Gen4 include protezioni abilitate per impostazione predefinita, nonché funzionalità quali autenticazione all'avvio e controlli delle porte che possono essere facilmente configurate su qualunque PC premendo F10 all'avvio per accedere al BIOS.

**D: Su quali piattaforme è disponibile HP BIOSphere Gen4?**

R: HP BIOSphere Gen4 è disponibile sui PC HP Pro e HP Elite (con processori di ottava generazione). Le funzionalità possono variare a seconda della piattaforma e delle configurazioni.

**D: Da che tipo di attacchi offre protezione HP BIOSphere Gen4?**

R: HP BIOSphere Gen4 offre protezione contro vari tipi di attacchi o guasti, inclusi gli attacchi mirati contro MBR o GPT, attacchi che tentano l'accesso mediante bridging wireless non autorizzato e altri ancora, incluse nuove tipologie di malware che, in futuro, potrebbero venire create per attaccare il BIOS.

Può anche offrire protezione contro gli attacchi fisici al dispositivo, con funzionalità quali le password per il BIOS, i controlli delle porte e HP Secure Erase.

**D: Cosa accade quando il BIOS deve essere aggiornato?**

R: HP supporta l'aggiornamento del BIOS con vari metodi, tra cui Windows Update e HP Support Assistant, e con la possibilità di configurare la programmazione degli aggiornamenti automatici del BIOS.

**D: Sono un responsabile IT e devo configurare le impostazioni del BIOS su più PC. HP BIOSphere Gen4 può aiutarmi?**

R: Sì. Per le piccole aziende, **Replicated Setup** consente di salvare con facilità le impostazioni del BIOS in un file, ad esempio su una chiavetta USB, e di utilizzarle per clonare le configurazioni su altre macchine.

Le aziende che dispongono di un reparto IT gestito possono impostare una configurazione del BIOS standardizzata su tutti i nuovi PC da una postazione centrale, utilizzando **HP BIOS Configuration Utility**. Questo processo automatizzato richiede solo pochi minuti, con un notevole risparmio sui costi IT e una maggiore produttività.

Le aziende che utilizzano Microsoft® System Center Configuration Manager per gestire il proprio parco dispositivi possono configurare le impostazioni del BIOS anche in remoto con HP Manageability Integration Kit Gen2<sup>7</sup>.

Scoprite di più su [www.hp.com/go/computersecurity](http://www.hp.com/go/computersecurity)

---

© Copyright 2018. HP Development Company, L.P. Le informazioni qui contenute possono subire variazioni senza preavviso. Le uniche garanzie sui prodotti e sui servizi HP sono esposte nelle dichiarazioni di garanzia esplicita che accompagnano i suddetti prodotti e servizi. Nulla di quanto qui contenuto può essere interpretato come garanzia aggiuntiva. HP declina ogni responsabilità per errori tecnici o editoriali od omissioni qui contenuti. Microsoft, Windows e il logo Windows sono marchi registrati o marchi di proprietà di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Intel e Core sono marchi registrati o marchi di proprietà di Intel Corporation o di sue consociate negli Stati Uniti e/o in altri Paesi. AMD, Radeon e il logo AMD sono marchi registrati di Advanced Micro Devices, Inc. USB Type-C™ e USB-C™ sono marchi registrati di USB Implementers Forum.

1. HP BIOSphere Gen4 è disponibile su piattaforme HP Elite e Pro con processori Intel o AMD di ottava generazione. Le funzionalità possono variare a seconda della piattaforma e delle configurazioni.
2. HP Sure Start Gen4 è disponibile per i prodotti HP Elite e HP Pro 600 dotati di processori Intel® di ottava generazione.
3. Gli aggiornamenti del BIOS tramite Windows Update sono disponibili su tutti i PC HP Elite e HP Pro con processori Intel o AMD di sesta generazione o versioni successive. Gli aggiornamenti di Intel ME tramite Windows Update sono disponibili sui PC HP Elite e HP Pro con processori Intel di ottava generazione.
4. HP Secure Erase è conforme ai metodi indicati nella National Institute of Standards and Technology Special Publication 800-88, metodo di pulizia "Clear".
5. HP BIOS Configuration Utility può essere scaricata da <http://www.hp.com/go/clientmanagement>.
6. I PC desktop supportano solo l'autenticazione tramite password.
7. HP Manageability Integration Kit può essere scaricato da <http://www.hp.com/go/clientmanagement>.

