

HP BIOSphere Gen4



keep reinventing

Notre écosystème de micrologiciels de pointe automatise la protection du BIOS et permet une gestion robuste de votre PC.

Une menace croissante

Le BIOS correspond au premier million de lignes de code exécutées par votre PC au démarrage. Il joue un rôle critique en assurant la communication entre le matériel de votre PC et votre système d'exploitation, ce qui rend la sécurité et la facilité de gestion du BIOS de plus en plus importante face aux menaces de sécurité d'aujourd'hui.

HP BIOSphere Gen 4¹ met à profit dix ans de leadership en sécurité du BIOS pour vous offrir un écosystème de protections qui vous aideront à défendre votre PC comprenant protections automatiques, dispositifs de sécurité personnalisables et facilité de gestion pour vous protéger contre les attaques sans interrompre la productivité de vos employés.

La protection commence dans le BIOS

HP BIOSphere Gen4 fournit une protection avancée du micrologiciel et prévient les attaques malveillantes ainsi que les erreurs accidentelles pouvant mettre en danger le BIOS.

- **Confiance à la racine au niveau du matériel**— Les PC HP Pro et HP Elite garantissent que vous démarrez avec un BIOS authentique, à chaque fois. (Dans le PC incluant également HP Sure Start², les BIOS corrompus se réparent automatiquement).
- Assure la protection des éléments critiques du micrologiciel, notamment **Master Boot Record (MBR)** et **GUID Partition Table (GPT)** contre toute corruption ou suppression qui empêcherait le PC de démarrer.
- HP BIOSphere Gen4 respecte les normes **NIST 800-147** et **ISO/IEC 19678:2015** pour garantir que votre BIOS ne reçoive que des mises à jour authentiques de HP.
- Des mises à jour du BIOS aussi faciles que de simples mises à jour de pilotes—HP BIOSphere Gen4 peut recevoir des mises à jour BIOS et Intel[®] ME déployées via Windows Update³.

Protection contre les attaques physiques

De nos jours, le travail sur PC se fait de plus en plus hors du bureau : dans les cafés, aéroports et espaces partagés qui sont plus vulnérables aux attaques physiques.

HP BIOSphere Gen4 comprend des protections puissantes contre les attaques physiques qui sont faciles à configurer et personnaliser et aident les entreprises de toutes tailles à protéger leurs PC et leurs informations sensibles.

- Empêchez les utilisateurs non autorisés d'accéder à vos appareils avec des fonctions de sécurité pré-démarrage telles que l'**Authentification à la mise sous tension** et **HP DriveLock**.
- Protégez vos ports contre les clés USB malveillantes ou les tentatives de voler des données avec des **contrôles de port** — avec HP BIOSphere Gen4, vous pouvez activer/désactiver des ports individuels et bloquer la fonction de démarrage depuis un port USB.
- **Secure Erase4** — Effacez vos données de manière permanente de vos disques durs ou disques SSD pour prévenir toute perte de données après la mise au rebut ou la réaffectation de vos anciens appareils.

Facilité de gestion avancée

HP BIOSphere permet aux services informatiques de configurer et de mettre à jour les paramètres du BIOS de façon centralisée pour tout un parc de PC en quelques minutes – un gain de temps et de travail pour les administrateurs informatiques grâce à une configuration et une gestion simplifiées.

HP BIOS Configuration Utility⁵ est un outil basé sur script qui permet de gérer à distance les paramètres de BIOS d'un PC. De plus, le module HP Manageability Integration Kit pour Microsoft[®] System Center Configuration Manager peut gérer à distance les paramètres et mots de passe HP BIOSphere.

Fonctions supplémentaires et caractéristiques

Normes et protections

Conforme ISO/IEC 19678:2015 (NIST 800-147) et NIST 800-155	HP BIOSphere Gen4 respecte la norme ISO/IEC 19678:2015 (NIST 800-147) pour garantir que votre BIOS ne reçoive que des mises à jour HP authentiques signées numériquement. La protection est renforcée au-delà de ces exigences par une application au niveau du matériel. Prend également en charge les mesures d'intégrité du BIOS spécifiées par NIST 800-155 .
Protection et restauration Master Boot Record (MBR) / GUID Partition Table (GPT)	Assure la protection du Master Boot Record (MBR) et de la GUID Partition Table (GPT) contre toute corruption ou suppression qui empêcherait le PC de démarrer. HP BIOSphere Gen4 peut également sauvegarder et restaurer votre MBR ou GPT en cas de corruption ou de suppression. Les utilisateurs peuvent également verrouiller le Master Boot Record pour empêcher sa modification. Ces fonctions peuvent être activées dans les paramètres du BIOS.
Confiance à la racine au niveau du matériel	Garantie appliquée au niveau du matériel de l'authenticité du BIOS avant l'exécution de code par le processeur au démarrage.
Démarrage sécurisé	Valide l'intégrité et l'authenticité du système d'exploitation avant d'autoriser son démarrage.

Protections configurables

Authentification à la mise sous tension⁶	Assure que seuls des utilisateurs autorisés peuvent démarrer le PC ou accéder au BIOS en exigeant une authentification de l'utilisateur avant le démarrage du système. L'authentification à la mise sous tension prend en charge l'identification par mot de passe ou empreinte digitale ⁶ .
HP DriveLock & HP Automatic DriveLock	Empêche les disques durs des ordinateurs portables de tourner sans autorisation en demandant au BIOS d'identifier l'utilisateur avant de déverrouiller le disque. Pour plus de simplicité, si l'utilisateur utilise déjà l'authentification à la mise sous tension, HP Automatic DriveLock peut assurer un accès rapide et sécurisé sans introduction de mots de passe supplémentaires.
HP One Step Logon	Simplifie votre processus d'ouverture de session en employant vos identifiants Windows pour l'authentification à la mise sous tension. L'authentification unique (Single Sign On) vous offre la protection de l'authentification à la mise sous tension sans que vous ayez à réintroduire vos identifiants pour ouvrir une session Windows. Doit être activé à l'aide de HP Client Security Manager Gen4.
Contrôle des ports	Nouveau dans Gen4 ! Protège contre les accès indésirables en permettant d'activer ou de désactiver des ports USB et périphériques individuels. De nombreux appareils utilisent aujourd'hui les ports USB-C™ pour se charger : si le port USB-C™ est désactivé, il chargera néanmoins les périphériques utilisateurs et pourra être utilisé pour alimenter le PC (disponible sur certains PC HP).
Contrôle des périphériques	Permet aux administrateurs de désactiver individuellement des appareils intégrés tels qu'appareils photo, microphones ou Bluetooth selon les besoins de leur environnement.
HP Secure Erase	Supprime définitivement les données des disques durs pour préparer la mise au rebut ou le redéploiement d'un système.

Autres

Mises à jour du BIOS via Windows Update	Nouveau dans Gen4 ! Met à jour le BIOS et Intel® ME via Windows Update ou le gestionnaire de périphériques, aussi facilement qu'une mise à jour de pilote standard.
Mises à jour du BIOS automatiques via le réseau	Vous permet de planifier vos mises à jour de BIOS automatiques via le réseau. Les dates et heures peuvent être définies dans le menu de configuration F10.
HP LAN-WLAN Protection	Protège le réseau LAN de l'entreprise des accès par passerelle sans fil en désactivant le LAN sans fil ou l'insertion LAN.
Contrôle de la gestion de l'alimentation	Permet de personnaliser la gestion de l'alimentation et le comportement de chargement.
Basculement en heure de pointe	Réduit la consommation d'énergie en basculant automatiquement le système sur l'alimentation par batterie durant les heures de pointe prédéfinies. Doit être activé via HP Power Manager ou à distance via le HP Manageability Integration Kit.

Fonctions d'entreprise et de facilité de gestion

Replicated Setup	Vous permet d'enregistrer facilement vos paramètres de BIOS dans un fichier – par exemple sur une clé USB – et de les utiliser pour cloner des configurations sur d'autres machines.
Activation de Device Guard (pour les utilisateurs de Windows Enterprise uniquement)	Améliore la sécurité du système en prenant en charge les dernières fonctions de protection contre les logiciels malveillants de Windows® 10, y compris Device Guard, qui assure une protection avancée contre les logiciels malveillants en empêchant l'exécution de toute application autre que les applications de confiance. Optimisé pour un déploiement aisé localement ou à distance via le module MIK.
Gestionnaire HP d'adresse MAC	Permet l'utilisation d'une adresse de contrôleur de réseau unique associée à la plate-forme elle-même pour les stations d'accueil câblées et les adaptateurs réseau, que la plate-forme soit sous tension ou hors tension, ce qui a une importance critique pour de nombreux déploiements d'images existants et workflows de gestion à distance. Nouveau dans Gen4 ! Inclut une adresse MAC basée sur hôte via USB-C™. Fonctionne que le PC dans la station d'accueil soit allumé ou éteint. Utilisez l'adresse MAC du système plutôt que celle de la station d'accueil — aide les administrateurs à identifier les systèmes, qu'ils soient ou non placés en station d'accueil. La station d'accueil doit prendre en charge l'adresse MAC basée sur hôte.
HP Wireless Wakeup	Permet à une configuration de paquet magique de réveiller le système d'un état de veille via des adaptateurs WLAN.
Diagnostics à distance	Capacité d'exécuter des diagnostics à distance et d'obtenir des journaux de diagnostic sur un système, même si la fonction de diagnostic n'est pas installée ou s'il n'y a pas d'image sur le disque.

Questions fréquemment posées :

Q : Mon entreprise est en croissance mais n'a pas de service informatique. Puis-je quand même tirer parti de HP BIOSphere Gen4 ?

R : Absolument. HP BIOSphere Gen4 inclut des protections activées par défaut ainsi que des capacités comme l'authentification à la mise sous tension et les contrôles de port qui peuvent facilement être configurées sur chaque PC en appuyant sur F10 au démarrage pour accéder au BIOS.

Q : Quelles plates-formes disposent de HP BIOSphere Gen4 ?

R : HP BIOSphere Gen4 est disponible sur les PC HP Pro et HP Elite (avec processeurs de 8ème génération). Les fonctionnalités varient en fonction de la plateforme et de la configuration.

Q : Contre quel type d'attaque HP BIOSphere Gen4 protège-t-il ?

R : HP BIOSphere Gen4 peut aider à protéger contre diverses attaques ou corruptions, notamment les attaques visant le MBR ou la BPT ; les attaques visant à pénétrer dans le système via une passerelle sans fil non autorisée ; et bien plus, notamment de nouveaux types de logiciels malveillants pouvant être créés à l'avenir pour viser le BIOS.

Il protège également contre les attaques physiques de l'appareil, avec des fonctions comme les mots de passe BIOS, les contrôles de port et HP Secure Erase.

Q : Que se passe-t-il si je dois mettre à jour le BIOS ?

R : HP prend en charge la mise à jour du BIOS par plusieurs méthodes, notamment Windows Update, HP Support Assistant, et la possibilité de configurer des mises à jour automatiques planifiées du BIOS.

Q : Je suis un responsable informatique et je dois configurer les paramètres de BIOS sur plusieurs PC. HP BIOSphere Gen4 peut-il m'aider pour cela ?

R : Oui. Pour les petites entreprises, **Replicated Setup** vous permet d'enregistrer facilement vos paramètres de BIOS dans un fichier – par exemple sur une clé USB – et de les utiliser pour cloner des configurations sur d'autres machines.

Les compagnies recourant à des services de gestion de l'informatique peuvent également mettre en place une configuration de BIOS standardisée sur tous les nouveaux PC à partir d'un emplacement central à l'aide de l'**Utilitaire de configuration de BIOS HP**. Ce processus automatisé ne prend que quelques minutes et permet de réduire les coûts informatiques et d'accroître la productivité.

Les entreprises utilisant Microsoft® System Center Configuration Manager pour gérer leur parc peuvent également configurer les paramètres de BIOS à distance via le HP Manageability Integration Kit Gen2⁷.

Pour en savoir plus : www.hp.com/go/computersecurity

© Copyright 2018. HP Development Company, L.P. Les informations contenues dans ce document peuvent être modifiées à tout moment et sans préavis. Les seules garanties relatives aux produits et services HP sont énoncées dans les déclarations de garantie expresse fournies avec ces produits et services. Aucune information contenue dans le présent document ne peut être interprétée comme constituant une garantie supplémentaire. HP décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document. Microsoft, Windows et le logo Windows sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Intel et Core sont des marques commerciales ou des marques déposées d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans d'autres pays. AMD, Radeon et le logo AMD sont des marques commerciales d'Advanced Micro Devices, Inc. USB Type-C™ et USB-C™ sont des marques commerciales d'USB Implementers Forum.

1. HP BIOSphere Gen4 est disponible sur les plateformes HP Elite et Pro équipées de processeurs Intel ou AMD 8e génération. Les fonctionnalités peuvent varier en fonction de la plateforme et de la configuration.
2. HP Sure Start 4e génération est disponible sur les produits HP Elite et HP Pro 600 équipés des processeurs Intel® 8e génération.
3. Les mises à jour du BIOS via Windows Update sont disponibles sur tous les PC HP Elite et HP Pro avec processeurs Intel ou AMD de 6ème génération ou supérieurs. Les mises à jour Intel ME via Windows Update sont disponibles sur les PC HP Elite et HP Pro avec processeurs Intel de 8ème génération.
4. HP Secure Erase – est utilisé pour les méthodes présentées dans le National Institute of Standards and Technology Special Publication 800-88, méthode de nettoyage « Clear ».
5. L'utilitaire de configuration du BIOS HP peut être téléchargé à l'adresse <http://www.hp.com/go/clientmanagement>.
6. Les PC de bureau ne prennent en charge que l'authentification par mot de passe.
7. HP Manageability Integration Kit peut être téléchargé sur le site <http://www.hp.com/go/clientmanagement>.

