Manuel de supervision des ordinateurs de bureau

HP Business PC

Manuel de supervision des ordinateurs de bureau

HP Business PC

Quatrième édition (septembre 2009)

Référence : 581009-051

A propos de ce livre

Le présent manuel fournit des définitions et des instructions pour l'utilisation des fonctions de sécurité et de supervision préinstallées sur certains modèles.

⚠ **AVERTISSEMENT !** Le non-respect de ces instructions expose l'utilisateur à des risques potentiellement très graves.

△ **ATTENTION :** Le non-respect de ces instructions présente des risques, tant pour le matériel que pour les informations qu'il contient.

REMARQUE : Le texte ainsi défini fournit des informations importantes supplémentaires.

Sommaire

1 Présentation de la gestion des ordinateurs de bureau

La suite HP Client Management Solutions offre des fonctionnalités normalisées pour la supervision et le contrôle des ordinateurs de bureau, des stations de travail et des ordinateurs portables dans un environnement réseau. HP fut le pionnier de la supervision des ordinateurs de bureau en produisant dès 1995 les tout premiers ordinateurs personnels entièrement supervisables. HP est détenteur d'un brevet couvrant cette technologie de supervision. Depuis, HP est devenu un leader du marché en matière de développement de normes et d'infrastructures nécessaires pour déployer, configurer et superviser efficacement des ordinateurs de bureau, des stations de travail et des ordinateurs portables. HP développe ses propres logiciels de supervision et travaille en étroite collaboration avec les principaux éditeurs de logiciels de supervision, de manière à assurer la compatibilité entre HP Client Management Solutions et ces produits. HP Client Management Solutions constitue un élément important de notre engagement à vous offrir des solutions pour vous assister dans la réduction du coût total de propriété et de maintenance des PC dans leur cycle de vie.

Voici les principales possibilités et fonctionnalités de la supervision des ordinateurs de bureau :

- Configuration et mise en œuvre initiales
- Installation à distance de système
- Mise à jour et gestion des logiciels
- Réécriture de la ROM
- Configuration des options du matériel
- Suivi d'inventaire et sécurité
- Notification des pannes et dépannage

REMARQUE : La prise en charge des fonctions spécifiques décrites dans ce manuel peut varier selon les modèles ou la version du logiciel.

2 Configuration et mise en œuvre initiales

Les ordinateurs HP sont livrés avec un ensemble de logiciels système préinstallés. Après une courte opération de décompactage des logiciels, l'ordinateur est prêt à fonctionner.

Vous préférerez peut-être remplacer les logiciels préinstallés par un ensemble personnalisé de logiciels système et d'applications. Il existe plusieurs méthodes de mise en œuvre d'un ensemble personnalisé de logiciels. Celles-ci comprennent :

- Installation d'applications logicielles supplémentaires après le décompactage de l'ensemble des logiciels préinstallés.
- Utilisation d'outils de déploiement de logiciels, tels que HP Client Automation Standard Edition ou HP Client Automation Enterprise Edition (basé sur la technologie Radia), pour remplacer les logiciels préinstallés par un ensemble personnalisé de logiciels.
- Application d'un procédé de clonage de disque permettant de copier le contenu d'un disque dur vers un autre.

La méthode de mise en œuvre la plus performante pour vous dépend de votre environnement et de vos procédés informatiques.

L'utilitaire de configuration ROM et le matériel compatible ACPI vous apportent une aide supplémentaire dans la récupération de logiciels système, la gestion de la configuration et la résolution des problèmes, ainsi que dans la gestion de l'alimentation.

HP Client Automation Agent

L'agent de supervision utilisé par HP Client Automation Standard Edition et Enterprise Edition est préchargé sur l'ordinateur. Une fois installé, ce logiciel permet de communiquer avec la console de supervision HP.

Pour installer HP Client Automation Agent :

1. Cliquez sur **Démarrer**.
2. Cliquez sur **Tous les programmes**.
3. Cliquez sur **HP Manageability**.
4. Cliquez sur le fichier Lisez-moi **Readme HP Management Agent** correspondant à la langue de votre choix.
5. Consultez et suivez les instructions fournies dans le fichier Readme (Lisez-moi) pour installer HP Client Automation Agent.

HP Client Automation Agent est un composant d'infrastructure clé pour l'activation de toutes les solutions HP Client Automation. Pour en savoir plus sur les autres composants d'infrastructure requis pour l'implémentation des solutions de gestion de la configuration HP, consultez l'adresse http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) est une solution gratuite développée par Symantec pour tous les modèles d'ordinateurs de bureau, de portables, de stations de travail et d'ordinateurs HP Blade pris en charge par HP. HPCM intègre des outils HP spécifiques comme System Software Manager, HP Instant Support Professional Edition (l'édition professionnelle d'assistance instantanée HP) et HP Client Management Interface qui permettent d'activer un modèle centralisé pour la gestion, le suivi et le contrôle de tout matériel pris en charge par HP.

HP Client Manager 7.0 possède un nouveau portail utilisé comme guichet unique où l'administrateur peut exécuter les tâches de gestion suivantes :

- Inventaire
- Alertes
- Gestion du BIOS
- Mises à jour des pilotes
- Exécuter HP Instant Support Health Scan and Diagnostics
- Exécuter des tâches Embedded Security
- Afficher la tendance des états d'alerte HP Health Alert Trend pour les 3 à 6 derniers mois
- Afficher la compatibilité générale des ordinateurs pris en charge avec HP Instant Support Health Scan and Diagnostics
- Afficher le récapitulatif des ordinateurs HP : une analyse des différents ordinateurs de bureau, portables, stations de travail et ordinateurs HP Blade pris en charge par HP
- Afficher les alertes : inventaire, seuil, état du matériel
- Rapports
- Tâches administratives pour mettre à jour des outils HP spécifiques

HPCM peut être téléchargé à l'adresse http://www.symantec.com/business/theme.jsp en cliquant sur **HP Client Manager** sous **Strategic Partner Products** (Produits partenaires stratégiques). Vous pouvez obtenir une licence permanente gratuite à partir de la page de téléchargement.

Les vidéos HPCM « Comment » sont aussi publiées sur le site http://www.symantec.com/connect. Recherchez **HP Client Manager 7.0** pour afficher les vidéos décrivant les étapes de différentes tâches dans HPCM.

3 Installation à distance de système

L'installation à distance de système permet de démarrer et de configurer le système à partir du logiciel et des informations se trouvant sur un serveur réseau en initiant la fonction PXE (Preboot Execution Environment). La fonction d'installation à distance de système est généralement employée comme utilitaire d'installation et de configuration de système et peut être utilisée pour exécuter les tâches suivantes :

- Formatage d’un disque dur
- Déploiement d’une image logicielle sur un ou plusieurs nouveaux PC
- Mise à jour à distance du BIOS système par réécriture de la ROM (Réécriture à distance de la ROM à la page 14)

REMARQUE : Des fonctions permettent d’écrire le BIOS système à partir du système d’exploitation Microsoft Windows.

- Configuration des paramètres du BIOS système

Pour initialiser l’installation à distance de système, appuyez sur F12 lorsque le message **F12=Network Service Boot** (Amorçage de maintenance réseau) apparaît dans l’angle inférieur droit de l’écran de logo HP au démarrage de l’ordinateur. Suivez les instructions affichées à l’écran pour continuer l’opération. L’ordre d’amorçage par défaut est un paramètre du BIOS qui peut être modifié de manière à toujours tenter un amorçage PXE.

4 Mise à jour et gestion des logiciels

HP fournit différents outils de supervision et de mise à jour du logiciel sur les ordinateurs de bureau, les stations de travail et les ordinateurs portables :

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter Edition, Standard Edition et Enterprise Edition
- HP Client Manager from Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- PC de marque Intel vPro avec Active Management Technology
- Verdiem Surveyor
- HP Product Change Notification
- HP Subscriber’s Choice

HP Client Management Interface

Quels que soient les outils de supervision système utilisés par votre service informatique, la gestion de vos actifs matériels et logiciels est importante pour maintenir des coûts informatiques bas et vos activités agiles. L’administrateur informatique peut accéder à HP Client Management Interface en écrivant des scripts simples et en intégrant ceux-ci dans la solution de gestion de leur choix.

Grâce à l'interface HP CMI (HP Client Management Interface), les nouveaux ordinateurs d'entreprise HP s'intègrent en toute transparence dans votre environnement informatique géré. HP CMI fournit une interface qui simplifie l'intégration des ordinateurs d'entreprise HP avec les outils de supervision système répandus de l'industrie (y compris Microsoft Systems Management Server, IBM Tivoli Software et HP Operations) et avec les applications de gestion développées en interne. En utilisant HP CMI, les applications et outils de supervision de systèmes peuvent demander un inventaire en profondeur des clients, recevoir des informations d'état et gérer des paramètres du BIOS système en communiquant directement avec l'ordinateur client, ce qui supprime le besoin d'un logiciel d'agent ou de connecteur pour atteindre l'intégration.

HP Client Management Interface est basé sur des normes industrielles qui incluent Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management

BIOS (SMBIOS) et Advanced Configuration and Power Interface (ACPI). HP CMI est une technologie de fondation utilisée dans HP Client Management Solutions. Grâce à HP CMI, HP vous permet de choisir la manière dont vous souhaitez gérer vos ordinateurs clients HP.

Une utilisation de HP Client Management Interface en conjonction avec un logiciel de supervision de système permet de réaliser les opérations suivantes :

- Demande en profondeur d'informations d'inventaire de client – Capturez des informations détaillées sur les processeurs, disques durs, mémoire, BIOS, drivers, y compris informations de capteur (telles que vitesse de ventilateur, tension et température).
- Réception d'informations d'état – Abonnez-vous à une vaste gamme d'alertes matérielles de client (telles que surchauffe, arrêt de ventilateur et modifications de configuration matérielle) à envoyer à la console de gestion du système, à une application ou à l'ordinateur client local. Les alertes sont envoyées en temps réel lorsqu'elles sont déclenchées par des événements matériels.
- Gestion des paramètres du BIOS système – Réalisez à distance des fonctions F10, y compris configuration et modification des mots de passe du BIOS et de la séquence de démarrage de l'ordinateur, à partir de votre console de gestion du système sur tout système client sans devoir visiter chaque machine.

Pour plus d'informations sur HP Client Management Interface, consultez le site http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager est une interface conviviale gratuite qui permet de trouver et de télécharger des mises à jour logicielles pour les modèles de PC clients HP de votre environnement. En spécifiant vos modèles, votre système d'exploitation et votre langue, vous pouvez rapidement trouver, trier et sélectionner les softpaqs dont vous avez besoin. Pour télécharger HP SoftPaq Download Manager, consultez l'adresse http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) est un utilitaire gratuit qui automatise le déploiement distant de drivers de périphérique et de mises à jour du BIOS pour vos PC d'entreprise HP en réseau. Lorsque SSM est exécuté, il détermine silencieusement (sans interaction de l'utilisateur) les niveaux de révision des drivers et du BIOS installées sur chaque système client en réseau et compare cet inventaire aux SoftPaqs logiciels système qui ont été testés et stockés dans un magasin de fichiers central. Le SSM procède ensuite automatiquement à la mise à jour des logiciels système des PC en réseau dont le niveau de révision est inférieur à celui des fichiers centralisés. Étant donné que la distribution des mises à jour SoftPaqs est uniquement autorisée aux modèles clients appropriés, les administrateurs peuvent utiliser efficacement le SSM en toute confiance pour maintenir les logiciels système à jour.

Le logiciel SSM s'intègre dans des outils de distribution des logiciels d'entreprise, tels que la suite HP Client Automation Solutions, HP Client Manager from Symantec et Microsoft SMS (Systems Management Server). À l'aide de SSM, vous pouvez distribuer vos propres mises à jour ou des mises à jour tierces, qui ont été rassemblées dans le format SSM prêt à l'emploi.

Vous pouvez télécharger le logiciel SSM gratuitement à partir du site http://www.hp.com/go/ssm.

REMARQUE : Le logiciel SSM ne prend pas actuellement en charge la réécriture à distance de la ROM sur les systèmes où la fonction Windows BitLocker Drive Encryption est activée et qui utilisent les mesures TPM pour protéger les clés BitLocker. En effet, l'écriture du BIOS annulerait la signature créée sur la plate-forme par BitLocker. Désactivez BitLocker à partir de Group Policy afin d'écrire le BIOS système.

Vous pouvez activer la prise en charge de BitLocker sans les mesures TPM du BIOS afin d'éviter l'invalidation des clés BitLocker. HP vous recommande de conserver une sauvegarde sécurisée des identités BitLocker en cas de récupération en urgence.

HP ProtectTools Security Manager

Le logiciel HP ProtectTools Security fournit des fonctions de sécurité destinées à aider à protéger l'ordinateur, les réseaux et les données critiques contre les accès non autorisés. Les fonctions de sécurité accrue du BIOS sont fournies par les modules logiciels suivants et sont accessibles à partir de HP ProtectTools Security Manager :

HP ProtectTools Security Manager est la console unique par laquelle il est possible d'accéder à tous les autres modules.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

HP ProtectTools offre deux versions qui peuvent être utilisées : HP ProtectTools Security Manager et HP ProtectTools Administrative Console. La version administrateur et la version utilisateur sont disponibles dans le menu **Démarrer** > **Tous les programmes**.

Les modules logiciels disponibles pour votre ordinateur peuvent varier en fonction de votre modèle. Embedded Security for HP ProtectTools n'est par exemple disponible que sur les ordinateurs dotés de la puce de sécurité intégrée TPM (Trusted Platform Module).

Les modules logiciels HP ProtectTools peuvent être préinstallés, préchargés ou téléchargés sur le site Web HP. Pour certains ordinateurs d'entreprise HP Pro, HP ProtectTools est disponible séparément. Pour plus d'informations, consultez le site http://www.hp.com/products/security.

HP Client Automation Starter Edition et Standard Edition

HP Client Automation est une solution de supervision de matériels et de logiciels destinée aux environnements Windows Vista, Windows XP et HP Thin Client ; elle est simple d'utilisation et rapide à

déployer et constitue une base robuste pour les exigences futures. Cette solution est disponible en deux éditions :

- L'édition Starter est un produit gratuit destiné à la supervision des ordinateurs de bureau, ordinateurs portables et stations de travail HP, qui fournit un inventaire des matériels et logiciels, une commande à distance, une surveillance d'alertes HP, des mises à jour de BIOS et de pilote HP, une intégration avec HP Protect Tools et une prise en charge supplémentaire pour Intel AMT. Cette édition prend également en charge le déploiement et la supervision de machines HP Thin Client.
- L'édition Standard, disponible à la vente, inclut toutes les fonctionnalités disponibles dans l'édition Starter et ajoute le déploiement et la migration Windows, des fonctions de gestion de correctifs, la distribution de logiciels, ainsi que le suivi de l'utilisation de logiciels.

HP Client Automation Starter Edition et Standard Edition fournissent un chemin de migration vers HP Client Automation Enterprise Edition (basé sur la technologie Radia) pour la supervision automatisée d'environnements informatiques volumineux, hétérogènes et en constant changement.

Pour plus d'informations sur les solutions HP Client Automation, consultez le site http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition est une solution basée sur les stratégies, qui permet aux administrateurs d'inventorier, de déployer, de corriger et de superviser en continu des logiciels et un contenu parmi des plates-formes clientes hétérogènes. Grâce à ce logiciel, le professionnel informatique peut :

- Automatiser le processus entier de supervision du cycle de vie à partir de la découverte, du déploiement et de la gestion continue via la migration et la mise au rebut
- Déployer automatiquement et superviser en continu une pile intégrale de logiciels (systèmes d’exploitation, applications, correctifs, paramètres et contenu) vers un état souhaité
- Superviser des logiciels sur virtuellement tout périphérique, notamment des ordinateurs de bureau, des postes de travail ou des ordinateurs portables, dans une infrastructure hétérogène ou autonome
- Superviser des logiciels sur la plupart des systèmes d’exploitation

Grâce à une supervision continue de la configuration, les clients HP peuvent constater d’étonnantes économies des coûts informatiques, une livraison accélérée des logiciels et du contenu sur le marché, ainsi qu’une productivité et une satisfaction accrues.

Pour plus d'informations sur les solutions HP Client Automation, consultez le site http://www.hp.com/go/client.

HP Client Manager from Symantec

HP Client Manager from Symantec, développé avec Altiris, est disponible gratuitement pour tous les modèles d'ordinateurs de bureau, de portables et de stations de travail pris en charge par HP. Intégré dans HP Client Manager, l'utilitaire SSM permet de suivre, de surveiller et de gérer tous les aspects matériels des systèmes clients HP.

Utilisez HP Client Manager from Symantec pour :

- Obtenir des informations précieuses sur le matériel, comme le processeur, la mémoire vidéo et les paramètres de sécurité
- Surveiller l'état du système pour prévenir l'apparition de problèmes
- Acquérir et installer automatiquement des drivers et mises à jour de BIOS sans visite de chaque PC
- Configurer à distance des paramètres de BIOS et de sécurité
- Automatiser les procédures de résolution rapide des problèmes matériels

Une étroite intégration avec les outils HP Instant Support réduit le temps de résolution des problèmes matériels.

- Diagnostics – exécutez et affichez à distance des rapports sur les modèles d'ordinateurs de bureau, de portables et de stations de travail HP
- Analyse d'état du système – recherchez des problèmes matériels connus éventuels dans votre base installée de systèmes clients HP
- Discussion active – connectez-vous à l'assistance technique HP pour résoudre des problèmes
- Base de connaissances HP – lien vers des informations d'expert
- Processus automatisé de collecte et de livraison de SoftPaq pour résolution rapide de problèmes matériels
- Identification, inventaire et initialisation de systèmes avec la puce de sécurité intégrée dans HP ProtectTools
- Option d'alertes d'état à afficher localement sur le système client
- Rapport d'informations d'inventaire de base pour clients non-HP
- Mettre en place et configurer la puce de sécurité TPM
- Planifier de façon centralisée une sauvegarde et récupération client
- Ajouter une prise en charge pour la gestion d'Intel AMT

Pour plus d'informations sur le logiciel HP Client Manager from Symantec, visitez le site http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite est une solution de gestion des systèmes facile à utiliser. Elle permet de gérer pendant toute leur durée de vie les logiciels des ordinateurs d'entreprise, des ordinateurs portables et des stations de travail. Client Management Suite comprend les produits Altiris suivants :

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution

- Application Management Solution
- Carbon Copy Solution

Pour plus d'informations sur la suite Altiris Client Management Suite, consultez le site http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

HP Client Catalog permet aux professionnels informatiques d'utiliser des produits Microsoft pour automatiser le déploiement de mises à jour logicielles HP (Softpaqs) sur des PC d'entreprise HP. Le fichier de catalogue contient des informations de plate-forme détaillées sur les ordinateurs d'entreprise, les ordinateurs portables et les stations de travail HP. Il peut être utilisé en relation avec l'inventaire personnalisé et les fonctionnalités de mise à jour des produits Microsoft pour fournir des mises à jour de pilote et de correctif automatisées pour les ordinateurs clients HP gérés.

Voici quelques-uns des produits Microsoft pris en charge par HP Client Catalog :

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 V2

Pour plus d'informations sur HP Client Catalog for SMS, consultez le site http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Technologie de gestion à distance

Parmi les modèles, vous trouverez la technologie vPro et la technologie standard. Les deux technologies proposent une recherche, une guérison et une protection améliorées des actifs informatiques en réseau. Ces deux technologies permettent de gérer des PC que le système soit actif ou inactif et même si le système d'exploitation est bloqué.

Il existe trois formes de gestion à distance disponibles sur les ordinateurs de bureau : Alert Standard Format (ASF), Intel Active Management Technology (AMT) et Desktop and mobile Architecture for Systems Hardware (DASH).

Les fonctions de technologie de gestion à distance comprennent :

- Recherche réseau
- Informations d’inventaire matériel
- Surveillance de l’état de la plate-forme
- Gestion de l’alimentation – mise sous et hors tension
- Diagnostics et réparation distants
    - Redirection de la console texte : permet de contrôler la console à distance pendant la phase de démarrage de l’ordinateur
    - Redirection du support : permet le démarrage du système à partir d’une unité de démarrage, d’un disque ou d’une image ISO distants (deux variantes existent : la redirection IDE-Redirect (IDE-R) sur les plate-formes AMT et la redirection USB Media Redirection)

- Isolement basé sur le matériel et récupération – limitation ou blocage de l'accès réseau des PC, en cas de détection d'activité de type virale
- Suivi et vérification des évènements de la plate-forme
- Portail de gestion du serveur Web intégré pour l'accès à distance et la configuration
- Technologies de gestion à distance intégrées aux partenaires de gestion de la console HP

REMARQUE : Toutes les fonctions ci-dessus ne sont pas disponibles sur toutes les plate-formes.

Configuration du ME (Management Engine) d'Intel

REMARQUE : Pour obtenir une présentation de la technologie Intel vPro, consultez le site http://www.intel.com/vpro.

Pour obtenir des informations spécifiques à HP sur la technologie Intel vPro, consultez les livres blancs sur le site http://www.hp.com/support. Sélectionnez votre pays/région et votre langue, activez l'option **Accéder aux informations techniques pour la résolution de problèmes de support**, entrez le numéro de modèle de votre ordinateur, puis appuyez sur Entrée. Dans la catégorie **Resources** (Ressources), cliquez sur **Manuals (guides, supplements, addendums, etc.)** (Manuels [guides, suppléments, addendums, etc.]). Sous **Quick jump to manuals by category** (Atteindre rapidement les manuels par catégorie), cliquez sur **White papers** (Livres blancs).

Les technologies de gestion disponibles incluent :

- AMT (DASH 1.0 inclus)
- ASF
- DASH 1.1 (utilisation d'une carte d'interface réseau Broadcom)

Les technologies ASF et AMT ne peuvent pas être configurées en même temps, mais toutes deux sont prises en charge.

Pour configurer des systèmes Intel vPro pour AMT ou ASF :

1. Allumez l'ordinateur ou redémarrez-le. Sous Microsoft Windows, cliquez sur **Démarrer** > **Arrêter l'ordinateur** > **Redémarrer**.
2. Dès que l'ordinateur se met sous tension, appuyez sur la combinaison de touches Ctrl+P avant que l'ordinateur ne démarre le système d'exploitation.

   REMARQUE : Si vous n'appuyez pas sur les touches Ctrl+P au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur les touches Ctrl+P avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

Cette combinaison permet d'accéder à l'utilitaire de configuration MEBx (Management Engine BIOS Execution) d'Intel. Cet utilitaire permet à l'utilisateur de configurer divers aspects de la technologie de gestion. Vous trouverez ci-après quelques-unes des options de configuration :

- Main Menu (Menu principal)
  - Intel® ME Configuration (Configuration ME Intel®)
  - Intel® AMT Configuration (Configuration AMT Intel®)
  - Change Intel® ME Password (Modifier le mot de passe ME Intel®)
  - Exit (Quitter)
- Intel® ME Platform Configuration (Configuration de plate-forme ME Intel®)
  - Intel® ME State Control (Contrôle d'état ME Intel®) (activer/désactiver)
  - Intel® ME Firmware Local Update (Mise à jour locale du microprogramme ME Intel®) (activer/désactiver)
  - Intel® ME Features Control (Contrôle des fonctions ME Intel®)
  - Intel® ME Power Control (Contrôle d'alimentation ME Intel®)
- Intel® AMT Configuration (Configuration AMT Intel®)
  - Host Name (Nom d'hôte)
  - TCP/IP
  - Provision Model (Modèle d'approvisionnement) (Enterprise, SMB)
  - Setup and Configuration (Installation et configuration)
  - Un-Provision (Annulation d'approvisionnement)
  - SOL/IDE-R (activer/désactiver)
  - Password Policy (Stratégie de mot de passe)
  - Secure Firmware Update (Mise à jour sécurisée du microprogramme) (activer/désactiver)
  - Set PRTC (Définir PRTC)
  - Idle Timeout (Délai d'attente avant inactivité)
- Change Intel® ME Password (Modifier le mot de passe ME Intel®) (HP recommande vivement de modifier ce mot de passe. Le mot de passe par défaut est **admin**.)

Afin de gérer à distance des systèmes AMT, l'administrateur doit utiliser une console distante qui prend en charge AMT. Des consoles de gestion d'entreprise sont disponibles auprès de certains fournisseurs, comme HP, Altiris et Microsoft SMS. En mode SMB, le client fournit une interface de navigateur Web. Pour accéder à cette fonction, ouvrez un navigateur à partir de tout autre système sur le réseau, puis entrez `http://nom_hôte:16992` où `nom_hôte` est le nom attribué au système. Vous pouvez également utiliser l'adresse IP à la place du nom d'hôte.

Pour configurer les systèmes avec une carte d'interface réseau Broadcom compatible DASH :

Consultez la documentation la plus récente sur le site http://www.hp.com sous **Support et dépannage**, puis sélectionnez votre modèle. Sélectionnez ensuite **Manuels**, puis les **Livres blancs** concernant DASH ou la carte d'interface réseau Broadcom.

Verdiem Surveyor

Verdiem Surveyor est une solution logicielle permettant de gérer les coûts électriques du PC. Surveyor calcule et rapporte l'électricité consommée par chaque PC. Il permet également de contrôler les paramètres d'alimentation du PC, permettant ainsi aux administrateurs de mettre aisément en œuvre des stratégies d'économie d'énergie sur l'ensemble des réseaux. Un HP SoftPaq contenant l'agent Surveyor peut être téléchargé sur le site Web de support HP et installé sur des modèles d'ordinateurs de bureau pris en charge. Des licences Surveyor pour gérer les PC peuvent être achetées auprès de votre représentant HP.

HP Proactive Change Notification

Le programme de notification proactive de modifications utilise un site Web sécurisé permettant, de manière proactive et automatique, d'effectuer les opérations suivantes :

- Recevoir des avis électroniques de modification de matériel et de logiciels sur la plupart des ordinateurs et des serveurs professionnels, jusqu'à 60 jours à l'avance.
- Recevoir des avis électroniques à la clientèle, des bulletins de sécurité et des alertes de drivers pour la plupart des ordinateurs et des serveurs professionnels.

Vous pouvez définir votre propre profil de manière à ne recevoir que des informations relatives à un environnement informatique spécifique. Pour en savoir plus sur le programme de notification proactive de modifications et créer un profil personnalisé, consultez le site http://h30046.www3.hp.com/subhub.php.

Subscriber's Choice

Le service Subscriber's Choice HP est un service personnalisé.

Sur la base de votre profil, HP vous fournira des conseils personnalisés sur les produits, les articles vedettes et les alertes/notifications sur les drivers et l'assistance.

Dans le cas de ces alertes/notifications, vous recevez des messages électroniques vous indiquant que vous pouvez télécharger les informations auxquelles vous êtes abonné. Pour en savoir plus sur le service Subscriber's Choice et créer votre profil personnel, consultez le site http://h30046.www3.hp.com/subhub.php.

Solutions retirées

Deux logiciels, Altiris Local Recovery et Dantz Retrospect, ne seront plus fournis dorénavant avec les ordinateurs d'entreprise, les ordinateurs portables et les stations de travail HP.

5 Réécriture de la ROM

Le BIOS de l'ordinateur est stocké sur une mémoire ROM flash programmable (mémoire morte). En définissant un mot de passe de configuration dans l'utilitaire Computer Setup (F10), vous pouvez protéger la mémoire ROM pour qu'elle ne soit pas mise à jour ou écrasée par inadvertance. Il est important de garantir l'intégrité de fonctionnement de l'ordinateur. Si vous devez ou souhaitez mettre le BIOS à niveau, vous pouvez télécharger les images BIOS les plus récentes à partir de la page HP Support et pilotes, http://www.hp.com/support/files.

△ **ATTENTION :** Pour obtenir une protection optimale de la mémoire ROM, créez un mot de passe de configuration. Le mot de passe de configuration empêche les mises à niveau non autorisées de la mémoire ROM. System Software Manager permet à l'administrateur système de définir le mot de passe pour un ou plusieurs ordinateurs simultanément. Pour plus d'informations, consultez le site http://www.hp.com/go/ssm.

Réécriture à distance de la ROM

La fonction de réécriture à distance de la ROM permet une mise à niveau en toute sécurité le BIOS d'ordinateurs HP distants, directement depuis la console de supervision réseau centralisée. L'exécution à distance de cette tâche sur plusieurs ordinateurs permet une mise en œuvre efficace et un meilleur contrôle des images de BIOS de PC HP par le réseau. Cela permet également une augmentation de la productivité et une baisse du coût de possession.

REMARQUE : Le logiciel SSM ne prend pas actuellement en charge la réécriture à distance de la ROM sur les systèmes où la fonction Windows BitLocker Drive Encryption est activée et qui utilisent les mesures TPM pour protéger les clés BitLocker. En effet, l'écriture du BIOS annulerait la signature créée sur la plate-forme par BitLocker. Désactivez BitLocker à partir de Group Policy afin d'écrire le BIOS système.

L'ordinateur doit être en marche ou activé à l'aide de la fonction de réveil à distance pour pouvoir utiliser la fonction de réécriture ROM à distance.

Pour plus d'informations sur la réécriture à distance de la ROM, consultez le logiciel HP Client Manager Software ou System Software Manager à l'adresse http://www.hp.com/go/ssm/.

HPQFlash

L'utilitaire HPQFlash permet de mettre à jour ou de restaurer localement le BIOS système de PC individuels à partir d'un système d'exploitation Windows.

Pour plus d'informations sur l'utilitaire HPQFlash, visitez le site http://www.hp.com/support/files et entrez le numéro de modèle de l'ordinateur lorsque vous y êtes invité.

6 Mode de récupération d’urgence de bloc d’amorçage

Le mode de récupération d’urgence du bloc d’amorçage permet de restaurer le système dans le cas improbable d’une panne de ROM flash, par exemple si une coupure de courant se produisait pendant une mise à niveau de la ROM. Ceci rendrait le BIOS système inutilisable. Le bloc d’amorçage (Boot Block) est une section protégée de la mémoire morte qui contient le code qui contrôle la validité de l’image du BIOS système, chaque fois que le système est mis sous tension.

- Si l’image du BIOS système est valide, le système démarre normalement.
- Si l’image n’est pas valide, un BIOS de bloc d’amorçage failsafe offre une prise en charge suffisante pour rechercher les fichiers d’image du BIOS sur les supports amovibles. Si un fichier d’image du BIOS approprié est trouvé, il est automatiqument inscrit dans la ROM.

Si une image de BIOS système non valide est détectée, le voyant d’alimentation du système clignote en rouge 8 fois, à une seconde d’intervalle. Simultanément, le haut-parleur émet 8 bips. Si la partie de la ROM système contenant l’image ROM d’option vidéo n’est pas corrompue, le **mode de récupération d’urgence du bloc d’amorçage** s’affiche à l’écran.

Pour restaurer le système après son passage au mode de récupération d’urgence du bloc d’amorçage, procédez comme suit :

1. Éteignez l’alimentation.
2. Insérez une un CD ou un périphérique USB à mémoire flash contenant le fichier d’image de BIOS souhaité dans le répertoire racine.

   REMARQUE : Le support doit être formaté à l’aide du système de fichiers FAT12, FAT16 ou FAT32.

3. Allumez l’ordinateur.

   Si aucune image du BIOS appropriée n’est trouvée, vous êtes invité à insérer un support contenant un fichier d’image du BIOS.

   Si le système reprogramme la ROM avec succès, il se met automatiquement hors tension.

4. Retirez le support amovible utilisé pour mettre à niveau le BIOS.
5. Mettez l’ordinateur sous tension pour le redémarrer.

REMARQUE : BitLocker empêche Windows Vista de démarrer lorsqu’un CD contenant le fichier image du BIOS file est situé dans une unité optique. Si BitLocker est activé, retirez ce CD avant de tenter de démarrer vers Windows Vista.

7 Réplication de la configuration

Les procédures suivantes permettent à un administrateur de copier facilement la configuration d'un ordinateur sur d'autres ordinateurs du même modèle. Ceci permet une configuration plus rapide et plus cohérente de plusieurs ordinateurs.

REMARQUE : Les deux procédures nécessitent une unité de disquette ou un lecteur flash USB.

REMARQUE : System Software Manager (SSM) peut être utilisé pour répliquer les informations de configuration de l'ordinateur à partir du système d'exploitation Microsoft Windows. Pour plus d'informations, consultez le Manuel de l'utilisateur SSM à l'adresse http://www.hp.com/go/ssm.

Copie vers un ordinateur unique

ATTENTION : Une configuration d'installation est spécifique au modèle. Une corruption du système de fichiers peut se produire si les ordinateurs source et cible ne sont pas du même modèle. Par exemple, ne copiez pas la configuration d'installation d'un PC dc7xxx vers un PC dx7xxx.

1. Sélectionnez une configuration d'installation à copier. Éteignez l'ordinateur. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Arrêter l'ordinateur**.
2. Si vous utilisez un périphérique USB à mémoire flash, insérez-le maintenant.
3. Allumez l'ordinateur.
4. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.
5. Si vous utilisez une disquette, insérez-la maintenant.
6. Cliquez sur **Fichier** > **Replicated Setup** (Installation répliquée) > **Save to Removable Media** (Enregistrer sur support amovible). Pour créer la disquette de configuration ou le périphérique USB à mémoire flash, suivez les instructions à l'écran.
7. Mettez hors tension l'ordinateur à configurer, puis insérez la disquette de configuration ou le périphérique USB à mémoire flash.
8. Mettez sous tension l'ordinateur à configurer.
9. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

10. Cliquez sur **Fichier** > **Replicated Setup** (Installation répliquée) > **Restore from Removable Media** (Restaurer à partir du support amovible), puis suivez les instructions à l'écran.

11. Une fois la configuration terminée, redémarrez l'ordinateur.

Copie vers plusieurs ordinateurs

△ **ATTENTION :** Une configuration d'installation est spécifique au modèle. Une corruption du système de fichiers peut se produire si les ordinateurs source et cible ne sont pas du même modèle. Par exemple, ne copiez pas la configuration d'installation d'un PC dc7xxx vers un PC dx7xxx.

Cette méthode prend un peu plus de temps pour préparer la disquette de configuration ou le périphérique USB à mémoire flash, mais la copie de la configuration vers les ordinateurs cible est bien plus rapide.

REMARQUE : Une disquette amorçable est requise pour cette procédure ou pour créer un périphérique USB à mémoire flash amorçable. Si Windows XP n'est pas disponible pour créer une disquette amorçable, utilisez la méthode de copie vers un ordinateur unique à la place (voir la section Copie vers un ordinateur unique à la page 16).

1. Créez une disquette ou un périphérique USB à mémoire flash amorçable. Reportez-vous à la section Périphérique USB à mémoire flash compatible à la page 18 ou Périphérique USB à mémoire flash non pris en charge à la page 19.

   △ **ATTENTION :** Tous les ordinateurs ne sont pas capables de démarrer à partir d'un périphérique USB à mémoire flash. Si le périphérique USB figure avant le disque dur dans l'ordre d'amorçage par défaut de Computer Setup (F10), alors vous pouvez démarrer l'ordinateur à partir d'un périphérique USB à mémoire flash. Sinon, vous devez utiliser une disquette amorçable.

2. Sélectionnez une configuration d'installation à copier. Éteignez l'ordinateur. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Arrêter l'ordinateur**.

3. Si vous utilisez un périphérique USB à mémoire flash, insérez-le maintenant.

4. Allumez l'ordinateur.

5. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

6. Si vous utilisez une disquette, insérez-la maintenant.

7. Cliquez sur **Fichier** > **Replicated Setup** (Installation répliquée) > **Save to Removable Media** (Enregistrer sur support amovible). Pour créer la disquette de configuration ou le périphérique USB à mémoire flash, suivez les instructions à l'écran.

8. Téléchargez un utilitaire BIOS pour la réplication de la configuration (repset.exe) et copiez-le sur la disquette de configuration ou le périphérique USB à mémoire flash. Pour obtenir cet utilitaire, visitez le site http://welcome.hp.com/country/us/en/support.html et entrez le numéro de modèle de l'ordinateur.

9. Sur la disquette de configuration ou le périphérique USB à mémoire flash, créez un fichier autoexec.bat contenant la commande suivante :

```
repset.exe
```

10. Mettez hors tension l'ordinateur à configurer. Insérez la disquette de configuration ou le périphérique USB à mémoire flash, puis mettez l'ordinateur sous tension. L'utilitaire de configuration s'exécute automatiquement.

11. Une fois la configuration terminée, redémarrez l'ordinateur.

Création d'un périphérique d'amorçage

Périphérique USB à mémoire flash compatible

Les périphériques pris en charge disposent d'une image préinstallée pour simplifier le processus les rendant amorçables. Tous les périphériques USB à mémoire flash HP ou Compaq et la plupart des autres comportent cette image préinstallée. Si le périphérique USB utilisé ne possède pas cette image, suivez la procédure décrite plus loin dans cette section (voir Périphérique USB à mémoire flash non pris en charge à la page 19).

Pour créer un périphérique d'amorçage USB à mémoire flash, vous devez avoir :

- un périphérique USB à mémoire flash pris en charge
- une disquette DOS amorçable avec les programmes FDISK et SYS (si SYS n'est pas disponible, FORMAT peut être utilisé, mais tous les fichiers existants sur le périphérique USB à mémoire flash seront perdus)
- un PC amorçable à partir d'un périphérique USB à mémoire flash

△ **ATTENTION :** Certains PC plus anciens peuvent ne pas démarrer à partir d'un périphérique USB à mémoire flash. Si le périphérique USB figure avant le disque dur dans l'ordre d'amorçage par défaut de Computer Setup (F10), vous pouvez démarrer l'ordinateur à partir d'un périphérique USB à mémoire flash. Sinon, vous devez utiliser une disquette amorçable.

1. Éteignez l'ordinateur.

2. Insérez le périphérique USB à mémoire flash dans un des ports USB de l'ordinateur, puis retirez tous les autres périphériques de stockage USB à l'exception des unités de disquette USB.

3. Insérez une disquette DOS amorçable contenant FDISK.COM et SYS.COM ou FORMAT.COM, puis allumez l'ordinateur.

4. Exécutez FDISK à partir de l'invite **A:** en tapant `FDISK` et en appuyant sur la touche Entrée. Si vous y êtes invité, cliquez sur **Yes** (**Y**) pour activer la prise en charge de disque de grande taille.

5. Entrez le choix [`5`] pour afficher les unités de disque du système. Le périphérique USB à mémoire flash sera l'unité dont la taille s'approche le plus de celle des unités affichées. Habituellement, il s'agit de la dernière unité de la liste. Notez la lettre de cette unité.

   Périphérique USB à mémoire flash : _____

   △ **ATTENTION :** Si aucune unité ne correspond au périphérique USB à mémoire flash, ne continuez pas. Vous pourriez perdre des données. Vérifiez si d'autres périphériques de stockage sont connectés aux ports USB. Si vous en trouvez, déconnectez-les, redémarrez l'ordinateur et continuez à l'étape 4. Si vous n'en trouvez pas, soit le système ne prend pas en charge les périphériques USB à mémoire flash, soit le périphérique USB utilisé est défectueux. NE tentez PAS de rendre amorçable le périphérique USB connecté.

6. Quittez FDISK en appuyant sur la touche Échap pour revenir à l'invite **A:**.
7. Si votre disquette DOS contient SYS.COM, passez à l'étape 8, sinon passez à l'étape 9.
8. À l'invite **A:**, entrez `SYS x:` où x représente la lettre d'unité notée ci-dessus.

△ **ATTENTION :** Assurez-vous d'avoir entré la lettre d'unité correcte pour le périphérique USB à mémoire flash.

Une fois les fichiers système transférés, SYS revient à l'invite **A:**. Passez à l'étape 13.

9. Copiez tous les fichiers à conserver du périphérique USB à mémoire flash vers un répertoire temporaire sur une autre unité (par exemple, le disque dur interne du système).
10. À l'invite **A:**, entrez `FORMAT /S X:` où `X` représente la lettre d'unité notée ci-dessus.

△ **ATTENTION :** Assurez-vous d'avoir entré la lettre d'unité correcte pour le périphérique USB à mémoire flash.

FORMAT affiche un ou plusieurs messages et vous demande à chaque fois si vous voulez continuer. Entrez `Y` à chaque fois. FORMAT formate le périphérique USB à mémoire flash, ajoute les fichiers système et vous demande d'entrer un nom de volume.

11. Appuyez sur Entrée si vous ne désirez pas de nom de volume ou entrez le nom de votre choix.
12. Recopiez sur votre périphérique USB tous les fichiers sauvegardés à l'étape 9.
13. Retirez la disquette et redémarrez l'ordinateur. L'ordinateur s'amorcera sur le périphérique USB à mémoire flash comme unité C.

REMARQUE : L'ordre d'amorçage par défaut varie d'un ordinateur à l'autre et peut être changé à l'aide de l'utilitaire Computer Setup (F10).

Si vous utilisez une version DOS d'un système d'exploitation Windows 9x, un écran de logo Windows peut s'afficher brièvement. Si vous ne souhaitez pas voir cet écran, ajoutez un fichier de taille zéro nommé LOGO.SYS dans le répertoire racine du périphérique USB à mémoire flash.

Revenez à la section Copie vers plusieurs ordinateurs à la page 17.

Périphérique USB à mémoire flash non pris en charge

Pour créer un périphérique d'amorçage USB à mémoire flash, vous devez avoir :

- un périphérique USB à mémoire flash
- une disquette DOS amorçable avec les programmes FDISK et SYS (si SYS n'est pas disponible, FORMAT peut être utilisé, mais tous les fichiers existants sur le périphérique USB à mémoire flash seront perdus)
- un PC amorçable à partir d'un périphérique USB à mémoire flash

△ **ATTENTION :** Certains PC plus anciens peuvent ne pas démarrer à partir d'un périphérique USB à mémoire flash. Si le périphérique USB figure avant le disque dur dans l'ordre d'amorçage par défaut de Computer Setup (F10), vous pouvez démarrer l'ordinateur à partir d'un périphérique USB à mémoire flash. Sinon, vous devez utiliser une disquette amorçable.

1. Si le système est doté de cartes PCI auxquelles sont connectés des unités de disque SCSI, RAID ATA ou SATA, éteignez l'ordinateur et débranchez le cordon d'alimentation.

   △ **ATTENTION :** Le cordon d'alimentation doit être débranché.

2. Ouvrez l'ordinateur et retirez les cartes PCI.
3. Insérez le périphérique USB à mémoire flash dans un des ports USB de l'ordinateur, puis retirez tous les autres périphériques de stockage USB à l'exception des unités de disquette USB. Fermez l'ordinateur.
4. Branchez l'ordinateur et mettez-le en marche.
5. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

6. Utilisez la commande **Advanced** (Avancé) > **PCI Devices** (Périphériques PCI) pour désactiver les contrôleurs PATA et SATA. Lors de la désactivation du contrôleur SATA, notez l'IRQ à laquelle le contrôleur est affecté. Vous devrez ultérieurement lui réaffecter cette IRQ. Quittez Computer Setup en confirmant vos modifications.

   IRQ SATA : _____

7. Insérez une disquette DOS amorçable contenant FDISK.COM et SYS.COM ou FORMAT.COM, puis allumez l'ordinateur.
8. Exécutez FDISK et supprimez toute partition du périphérique USB à mémoire flash. Créez une nouvelle partition et définissez-la comme partition active. Quittez FDISK en appuyant sur la touche Échap.
9. Si le système ne redémarre pas automatiquement à la sortie de FDISK, appuyez sur les touches Ctrl+Alt+Suppr pour redémarrer à partir de la disquette DOS.
10. À l'invite **A:**, entrez `FORMAT C: /S` et appuyez sur la touche Entrée. FORMAT formate le périphérique USB à mémoire flash, ajoute les fichiers système et vous demande d'entrer un nom de volume.
11. Appuyez sur Entrée si vous ne désirez pas de nom de volume ou entrez le nom de votre choix.
12. Éteignez l'ordinateur et débranchez le cordon d'alimentation. Ouvrez l'ordinateur et réinstallez les cartes PCI précédemment enlevées. Fermez l'ordinateur.
13. Retirez la disquette, branchez l'ordinateur et mettez-le en marche.
14. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

15. Utilisez la commande **Advanced** (Avancé) > **PCI Devices** (Périphériques PCI) et réactivez les contrôleurs PATA et SATA que vous avez désactivés à l'étape 6. Replacez le contrôleur SATA sur son IRQ d'origine.

16. Enregistrez vos modifications et quittez Computer Setup. L'ordinateur s'amorcera sur le périphérique USB à mémoire flash comme unité C.

REMARQUE : L'ordre de démarrage par défaut peut varier d'un ordinateur à l'autre et peut être modifié dans l'utilitaire Computer Setup (F10). Pour consulter les instructions, reportez-vous au *Manuel de l'utilitaire Computer Setup (F10)* .

Si vous utilisez une version DOS d'un système d'exploitation Windows 9x, un écran de logo Windows peut s'afficher brièvement. Si vous ne souhaitez pas voir cet écran, ajoutez un fichier de taille zéro nommé LOGO.SYS dans le répertoire racine du périphérique USB à mémoire flash.

Revenez à la section Copie vers plusieurs ordinateurs à la page 17.

8 Interrupteur d'alimentation double état

Lorsque l'interface de configuration avancée et d'économie d'énergie est activée, le bouton de mise sous tension peut servir soit de bouton marche/arrêt, soit de bouton de mise en veille. La fonction de mise en veille ne met pas l'ordinateur hors tension, mais le fait passer dans un état à faible consommation électrique. Cela vous permet d'arrêter le système sans fermer les applications et de reprendre rapidement votre travail où vous l'aviez laissé sans perdre de données.

Pour reconfigurer le bouton de mise sous tension, procédez comme suit :

1. Cliquez sur le bouton **Démarrer**, puis sélectionnez **Panneau de configuration** > **Options d'alimentation**.
2. Dans les **Propriétés des options d'alimentation**, sélectionnez l'onglet **Avancé**.
3. Dans la section **Bouton d'alimentation**, sélectionnez **Mettre en veille**.

Lorsque le bouton d'alimentation est configuré pour la mise en veille, le fait d'appuyer sur ce bouton met l'ordinateur dans un mode de fonctionnement à très faible consommation. Appuyez de nouveau sur le bouton pour ramener rapidement le système à son fonctionnement normal. Pour couper complètement l'alimentation de l'ordinateur, appuyez sur le bouton de mise sous tension pendant quatre secondes.

△ **ATTENTION :** N'éteignez l'ordinateur avec le bouton d'alimentation que si le système ne répond plus ; le fait d'éteindre l'ordinateur sans interaction avec le système d'exploitation peut provoquer une perte de données ou altérer les données du disque dur.

9 Support du site Web HP

Les ingénieurs HP ont procédé à des tests rigoureux et au débogage des logiciels mis au point par HP et d'autres éditeurs. Ils ont également développé un logiciel spécifique de prise en charge de système d'exploitation afin de garantir les performances, la compatibilité et la fiabilité des ordinateurs HP.

Lorsque vous installez des systèmes d'exploitation nouveaux ou révisés, il est important d'exécuter le logiciel de prise en charge conçu pour ce système d'exploitation. Si vous prévoyez d'utiliser une version de Microsoft Windows différente de celle fournie avec l'ordinateur, vous devez d'abord installer les drivers de périphérique et les utilitaires appropriés afin de garantir la prise en charge correcte et l'exécution de toutes les fonctionnalités.

HP a simplifié les tâches de localisation, d'accès, d'évaluation et d'installation des derniers logiciels de support. Vous pouvez télécharger le logiciel à l'adresse http://www.hp.com/support.

Ce site contient les derniers drivers de périphérique, utilitaires et images de ROM flash dont vous avez besoin pour exécuter le système d'exploitation Microsoft Windows le plus récent sur l'ordinateur HP.

10 Normes industrielles

Les solutions de supervision HP s’intègrent dans d’autres applications de supervision, car elles s’appuient sur des normes établies telles que :

- WBEM (Web-Based Enterprise Management)
- WMI (Windows Management Interface)
- WOL (Wake On LAN)
- ACPI (Advanced Configuration and Power Interface)
- SMBIOS (System Management BIOS)
- Prise en charge de PXE (Pre-boot Execution Environment)

11 Suivi d’inventaire et sécurité

Les fonctions de suivi d’inventaire incorporées dans l’ordinateur fournissent les données essentielles d’inventaire qui peuvent être gérées dans les logiciels HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager ou autre application de supervision des systèmes. L’intégration automatique qui se fait en continu entre les fonctions de suivi d’inventaire et ces produits permet de choisir l’outil de supervision le mieux adapté à l’environnement et d’exploiter l’investissement dans des outils existants.

HP propose en outre différentes solutions permettant de sécuriser l'accès aux éléments et aux données essentiels de l'ordinateur. Lorsqu'il est installé, l'utilitaire HP Embedded Security for ProtectTools empêche l'accès non autorisé aux données, vérifie l'intégrité du système et authentifie les tiers qui tentent d'y accéder. (Pour plus d'informations, reportez-vous au manuel *HP ProtectTools Security Manager Guide* sur le site http://www.hp.com/products/security.) Les fonctions de sécurité, telles que HP Embedded Security for ProtectTools, le capteur Smart Cover et le verrou Smart Cover, disponibles sur certains modèles, empêchent tout accès non autorisé aux composants internes de l'ordinateur. En désactivant les ports parallèles, de série ou USB ou en désactivant la capacité d'amorçage des supports amovibles, vous pouvez protéger vos données importantes. Les alertes de modification de mémoire et de capteur Smart Cover peuvent être transmises automatiquement aux applications de supervision, afin d'émettre des messages proactifs en cas de manipulation des composants internes de l'ordinateur.

REMARQUE : HP Embedded Security for ProtectTools, le capteur Smart Cover et le verrou Smart Cover sont disponibles en option sur certains modèles.

Vous pouvez gérer les paramètres de sécurité de l’ordinateur HP à l’aide des utilitaires suivants :

- En local, avec l’utilitaire Computer Setup. Pour obtenir des informations supplémentaires et des instructions sur l’utilisation de l’utilitaire Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)* fourni avec l’ordinateur.
- A distance, avec HP Client Manager from Symantec, HP Client Automation ou System Software Manager. Ce logiciel permet le déploiement sûr et cohérent, ainsi que le contrôle des paramètres de sécurité.

Les sections et le tableau suivants décrivent les fonctions locales de supervision de la sécurité de l’ordinateur offertes par l’utilitaire Computer Setup (F10).

Tableau 11-1 Sommaire des fonctions de sécurité

Option	Description
Mot de passe de configuration	Permet de définir et d'activer un mot de passe de configuration (administrateur). **REMARQUE :** Si le mot de passe de configuration est défini, il est nécessaire de modifier les options Computer Setup, de réécrire la ROM et de modifier certains paramètres Plug-and-Play sous Windows.

Tableau 11-1 Sommaire des fonctions de sécurité (suite)

Mot de passe de mise sous tension	Permet de définir et d'activer un mot de passe de mise sous tension. L'invite de mot de passe de mise sous tension s'affiche après un cycle de mise hors puis sous tension. Si l'utilisateur n'entre pas le mot de passe de mise sous tension correct, l'unité ne démarre pas. **REMARQUE :** Ce mot de passe ne s'affiche pas lors de démarrages à chaud, tels que Ctrl+Alt+Suppr ou **Restart from Windows** (Redémarrage à partir de Windows) à moins qu'il ne soit activé dans les **Password Options** (Options de mot de passe) (voir ci-dessous).
Options de mot de passe (Cette sélection apparaît uniquement si un mot de passe de mise sous tension ou de configuration a été défini.)	Permet de : • Verrouiller des ressources héritées (s'affiche si un mot de passe de configuration est défini) • Activer/Désactiver le mode de serveur réseau (s'affiche si un mot de passe de mise sous tension est défini) • Spécifier si le mot de passe est obligatoire pour un redémarrage à chaud (Ctrl+Alt+Suppr) (s'affiche si un mot de passe de mise sous tension est défini) • Activer/Désactiver le mode de parcours de configuration (s'affiche si un mot de passe de configuration est défini) (permet d'afficher, mais non de modifier, les options de configuration F10 sans entrer de mot de passe de configuration) • Activer/Désactiver le mot de passe strict (apparaît si un mot de passe de mise sous tension est défini) ; lorsqu'il est activé, contourne le cavalier de mot de passe embarqué pour désactiver le mot de passe de mise sous tension Pour plus d'informations, consultez le *Manuel de supervision des ordinateurs de bureau*.
Smart Cover (certains modèles)	Permet de : • Verrouiller/déverrouiller le verrou Smart Cover. • Régler le capteur de retrait du capot sur Disable/Notify User/Setup Password (Désactiver/Avertir l'utilisateur/Mot de passe de configuration) **REMARQUE :** *Notify User* avertit l'utilisateur si le capteur a détecté le retrait du capot. *Setup Password* nécessite que le mot de passe de configuration soit entré pour démarrer l'ordinateur si le capteur détecte que le capot a été retiré. Cette fonction n'est prise en charge que sur certains modèles.
Device Security (Sécurité des unités de disque)	Permet de définir l'option Device Available/Device Hidden (Périphérique disponible/masqué) pour : • Ports série • Port parallèle • Ports USB arrière • Ports USB avant • Ports USB internes • Système audio • Contrôleurs réseau (certains modèles) • Ancienne disquette : • Périphérique de sécurité intégré (certains modèles) • SATA0 • SATA1 (certains modèles) • SATA2 (certains modèles)

Tableau 11-1 Sommaire des fonctions de sécurité (suite)

	• SATA3 (certains modèles) • eSATA (certains modèles)
LoJack for HP ProtectTools	Permet de commander, gérer et assurer le suivi à distance de l'ordinateur. Une fois qu'il est activé, LoJack Pro for HP ProtectTools est configuré à partir du centre d'assistance Absolute Software Customer Center. A partir du centre d'assistance, l'administrateur peut configurer LoJack for HP ProtectTools pour surveiller ou gérer l'ordinateur. Si le système est déplacé ou volé, le centre d'assistance peut aider les autorités locales à localiser et récupérer l'ordinateur. S'il est configuré, LoJack Pro peut continuer à fonctionner même si le disque dur est effacé ou remplacé.
Network Service Boot (Démarrage des services réseau)	Active ou désactive la capacité de l'ordinateur de démarrer à partir d'un système d'exploitation installé sur un serveur du réseau. (Fonction disponible uniquement sur les cartes réseau ; le contrôleur réseau doit être une carte d'extension PCI ou être intégré sur la carte mère.)
System ID (ID du système)	Permet de définir les options suivantes : • Étiquette d'inventaire (identifiant de 18 octets), un numéro d'identification de propriété affecté à l'ordinateur par votre société. • Étiquette de propriété (identifiant de 80 octets) affichée pendant l'autotest POST. • Le numéro de série du châssis ou numéro UUID (Universal Unique Identifier) si le numéro actuel n'est pas valide. Le numéro UUID ne peut être mis à jour que si le numéro de châssis actuel est correct. (Ces numéros d'identification sont habituellement définis en usine et permettent d'identifier le système de façon unique.) • Les paramètres régionaux de clavier (par exemple, Anglais ou Français) pour la saisie des ID système.
DriveLock Security (Sécurité DriveLock)	Permet d'attribuer ou de modifier un mot de passe maître ou utilisateur aux disques durs. Lorsque cette fonction est activée, l'utilisateur est invité à entrer l'un des mots de passe DriveLock lors du POST. Le disque dur reste inaccessible tant que l'un des mots de passe n'est pas correctement entré lors d'une procédure de démarrage à froid. **REMARQUE :** Cette option n'apparaît que si au moins un disque dur offrant la fonction DriveLock est relié à votre système.
Setup Security Level (Niveau de sécurité de configuration)	Fournit une méthode permettant aux utilisateurs finaux d'avoir un accès limité pour modifier les options de configuration spécifiées, sans devoir connaître le mot de passe de configuration. Cette fonction permet à l'administrateur de protéger les options de configuration essentielles, tout en autorisant à l'utilisateur de visualiser les paramètres système et de configurer des options non essentielles. L'administrateur spécifie des droits d'accès sur des options de configuration individuelles via le menu Setup Security Level (Niveau de sécurité de configuration). Par défaut, toutes les options de configuration se voient attribuer un mot de passe de configuration, indiquant que l'utilisateur doit entrer le mot de passe de configuration correct durant le processus POST pour apporter des modifications aux options. L'administrateur peut définir des éléments individuels sur Aucun, indiquant que l'utilisateur peut apporter des modifications aux options spécifiées si l'accès à la configuration est effectué avec un mot de passe non valide. Le choix Aucun est remplacé par Mot de passe de mise sous tension si un mot de passe de mise sous tension est défini. **REMARQUE :** Le mode de parcours de configuration (Setup Browse Mode) doit être activé pour que l'utilisateur puisse accéder à la configuration sans connaître le mot de passe de configuration.
System Security (Sécurité du système) (certains modèles : ces options dépendent du matériel)	Data Execution Prevention (Prévention contre l'exécution de données) (certains modèles) (activer/désactiver) : permet de protéger l'ordinateur contre certaines failles de sécurité des systèmes d'exploitation. Virtualization Technology (Technologie de virtualisation) (certains modèles) (activer/désactiver) : contrôle les fonctions de virtualisation du processeur. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. Virtualization Technology Directed I/O (Technologie de virtualisation de l'architecture Directed I/O) (certains modèles) (activer/désactiver) : contrôle les fonctions de remappage DMA de la

Tableau 11-1 Sommaire des fonctions de sécurité (suite)

	virtualisation du chipset. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. Trusted Execution Technology (Technologie d'exécution sécurisée) (certains modèles) (activer/désactiver) : contrôle les fonctions sous-jacentes du processeur et du chipset, indispensables pour prendre en charge un appareil virtuel. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. Pour activer cette fonction, vous devez activer les fonctions suivantes : • Prise en charge du périphérique de sécurité intégré • Technologie de virtualisation • Technologie de virtualisation de l'architecture Directed I/O Embedded Security Device Support (Prise en charge du périphérique de sécurité intégré) (certains modèles) (activer/désactiver) : permet d'activer et de désactiver le périphérique de sécurité intégré. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. **REMARQUE :** Pour configurer le périphérique de sécurité intégré, vous devez définir un mot de passe de configuration. • Reset to Factory Settings (Restaurer les paramètres usine) (certains modèles) (ne pas restaurer/restaurer) : la restauration des paramètres usine par défaut efface toutes les clés de sécurité. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. **ATTENTION :** Le périphérique de sécurité intégré est un élément stratégique de nombreux schémas de sécurité. L'effacement des clés de sécurité permet d'empêcher l'accès aux données protégées par le périphérique de sécurité intégré. Sélectionner Reset to Factory Settings (Restaurer les paramètres usine) peut entraîner une perte significative de données. • Reset authentication credentials (Réinitialiser les informations d'authentification) (certains modèles) (ne pas réinitialiser/réinitialiser) : la sélection de ce paramètre permet de prendre en charge et de supprimer les informations d'authentification du périphérique de sécurité intégré. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. OS management of Embedded Security Device (Gestion du périphérique de sécurité intégré par le système d'exploitation) (certains modèles) (activer/désactiver) : cette option permet à l'utilisateur de limiter le contrôle du système d'exploitation du périphérique de sécurité intégré. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. Cette option permet à l'utilisateur de limiter le contrôle du système d'exploitation du périphérique de sécurité intégré. • Reset of Embedded Security Device though OS (Réinitialisation du périphérique de sécurité intégré via le système d'exploitation) (certains modèles) (activer/désactiver) : cette option permet à l'utilisateur de limiter la capacité du système d'exploitation à restaurer les paramètres usine du périphérique de sécurité intégré. La modification de ce paramètre requiert de mettre l'ordinateur hors tension, puis à nouveau sous tension. **REMARQUE :** Pour activer cette option, vous devez définir un mot de passe de configuration. PAVP (certains modèles) (désactivé/min/max) : l'option PAVP active le chemin vidéo audio protégé du chipset. Ceci peut permettre d'afficher certains éléments de contenu haute définition protégés et dont la lecture serait, sans cette option, interdite. Sélectionnez la définition Max pour attribuer 96 Mo de mémoire système exclusive pour l'option PAVP.

Sécurité par mot de passe

Le mot de passe de mise sous tension empêche l'accès non autorisé à votre ordinateur en demandant la saisie d'un mot de passe pour accéder aux applications ou aux données, chaque fois que l'ordinateur

est allumé ou redémarré. Le mot de passe de configuration empêche l'accès non autorisé à Computer Setup et peut aussi être utilisé à la place du mot de passe de mise sous tension. C'est-à-dire que, lorsque l'invite de saisie du mot de passe de mise sous tension s'affiche, la saisie du mot de passe de configuration vous permettra d'accéder à l'ordinateur.

La création d'un mot de passe de configuration à l'échelle du réseau est aussi possible, ce qui permet à l'administrateur système d'accéder à tous les systèmes du réseau pour effectuer des opérations de maintenance sans avoir besoin de connaître votre mot de passe de mise sous tension, même si celui-ci a été défini.

REMARQUE : System Software Manager (SSM) peut être utilisé pour créer et gérer les mots de passe BIOS à partir du système d'exploitation Microsoft Windows. Pour plus d'informations, consultez le Manuel de l'utilisateur SSM à l'adresse http://www.hp.com/go/ssm.

REMARQUE : Avec HP Client Management Interface (HP CMI), vous accédez aux paramètres de gestion BIOS, notamment aux mots de passe BIOS à partir du système d'exploitation Windows. Pour plus d'informations, consultez les Livres blancs techniques HP Client Management Interface à l'adresse http://www.hp.com/go/hpcmi.

Création d'un mot de passe de configuration à l'aide de Computer Setup

Si le système est équipé d'un périphérique de sécurité intégré, reportez-vous au manuel *HP ProtectTools Security Manager* à l'adresse http://www.hp.com. Créer un mot de passe de configuration dans Computer Setup empêche la reconfiguration de l'ordinateur (utilisation de l'utilitaire Computer Setup (F10) jusqu'à ce que le mot de passe soit saisi.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Sélectionnez **Sécurité**, puis **Mot de passe** de configuration et suivez les instructions affichées à l'écran.
4. Avant de quitter, sélectionnez **Fichier** > **Enregistrer et quitter**.

Création d'un mot de passe de mise sous tension à l'aide de Computer Setup

La création d'un mot de passe de mise sous tension par le biais de l'utilitaire Computer Setup bloque l'accès à l'ordinateur, lors de sa mise sous tension, jusqu'à la saisie du mot de passe. Lorsqu'un mot de passe de mise sous tension est défini, Computer Setup présente la fonction **Options de mot de passe** dans le menu **Sécurité**. Les options de mot de passe incluent **Password Prompt on Warm**

Boot (Invite de mot de passe de mise sous tension). Si l'invite de mot de passe de mise sous tension est activée, le mot de passe doit également être entré lors du redémarrage de l'ordinateur.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Sélectionnez **Sécurité**, puis **Mot de passe de mise sous tension**, puis suivez les instructions qui s'affichent à l'écran.
4. Avant de quitter, sélectionnez **Fichier** > **Enregistrer et quitter**.

Saisie d'un mot de passe de mise sous tension

Pour saisir un mot de passe de mise sous tension, procédez comme indiqué ci-dessous :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer l'ordinateur**.
2. Lorsque l'icône en forme de clé apparaît à l'écran, saisissez le mot de passe courant, puis appuyez sur la touche Entrée.

REMARQUE : Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

Si vous saisissez le mot de passe de manière incorrecte, une icône représentant une clé brisée apparaît à l'écran. Essayez une nouvelle fois. Après trois tentatives infructueuses, vous devez éteindre l'ordinateur, puis le remettre en marche avant de pouvoir continuer.

Saisie du mot de passe de configuration

Si le système est équipé d'un périphérique de sécurité intégré, reportez-vous au manuel *HP ProtectTools Security Manager* à l'adresse http://www.hp.com.

Si un mot de passe de configuration a été défini sur l'ordinateur, un message vous invite à l'entrer à chaque exécution de l'utilitaire Computer Setup.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Lorsque l'icône en forme de clé apparaît à l'écran, saisissez le mot de passe de configuration, puis appuyez sur la touche Entrée.

REMARQUE : Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

Si vous saisissez le mot de passe de manière incorrecte, une icône représentant une clé brisée apparaît à l'écran. Essayez une nouvelle fois. Après trois tentatives infructueuses, vous devez éteindre l'ordinateur, puis le remettre en marche avant de pouvoir continuer.

Changement d'un mot de passe de mise sous tension ou de configuration

Si le système est équipé d'un périphérique de sécurité intégré, reportez-vous au manuel *HP ProtectTools Security Manager* à l'adresse http://www.hp.com.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer l'ordinateur**.
2. Pour modifier le mot de passe de mise sous tension, passez à l'étape 3.

   Pour modifier le mot de passe de configuration, dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.
3. Lorsque l'icône en forme de clé apparaît, saisissez le mot de passe actuel, une barre oblique (/) ou un autre caractère de séparation, le nouveau mot de passe, une barre oblique (/) ou un autre caractère de séparation, et encore une fois le nouveau mot de passe, selon le schéma suivant :
   `mot de passe courant/nouveau mot de passe/nouveau mot de passe`

   REMARQUE : Entrez le mot de passe avec soin. Pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.
4. Appuyez sur Entrée.

Le nouveau mot de passe prend effet à la prochaine mise sous tension de l'ordinateur.

REMARQUE : Pour plus d'informations sur les différents caractères de séparation, reportez-vous au tableau Caractères de séparation selon les claviers à la page 32. Le mot de passe de mise sous tension et celui de configuration peuvent aussi être modifiés à l'aide des options de Sécurité dans Computer Setup.

Suppression d’un mot de passe de mise sous tension ou de configuration

Si le système est équipé d’un périphérique de sécurité intégré, reportez-vous au manuel *HP ProtectTools Security Manager* à l’adresse http://www.hp.com.

1. Allumez l’ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer l’ordinateur**.
2. Pour supprimer le mot de passe de mise sous tension, passez à l’étape 3.

   Pour supprimer le mot de passe de configuration, dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Lorsque l’icône en forme de clé apparaît, entrez le mot de passe courant, une barre oblique (/) ou un autre caractère de séparation, comme suit : `mot de passe courant/`
4. Appuyez sur Entrée.

REMARQUE : Pour plus d’informations sur les différents caractères de séparation, reportez-vous au tableau Caractères de séparation selon les claviers à la page 32. Le mot de passe de mise sous tension et celui de configuration peuvent aussi être modifiés à l’aide des options de Sécurité dans Computer Setup.

Caractères de séparation selon les claviers

Chaque clavier est conçu pour répondre aux besoins spécifiques à chaque pays/région. La syntaxe et les touches que vous utilisez pour changer ou supprimer un mot de passe dépendent du clavier utilisé avec l’ordinateur.

Caractères de séparation selon les claviers

/	Arabe	-	Grec	/	Russe
=	Belge	.	Hébreu	-	Slovaque
-	BHCMSS*	-	Hongrois	-	Espagnol
/	Brésilien	-	Italien	/	Suédois/Finnois
/	Chinois	/	Japonais	-	Suisse
-	Tchèque	/	Corée	/	Taïwanais
-	Danois	-	Latino-américain	/	Thaï
!	Français	-	Norvégien	.	Turc
é	Français (Canada)	-	Polonais	/	Anglais (USA)
-	Allemand	-	Portugais		

* Pour Bosnie-Herzégovine, Croatie, Monténégro, Serbie et Slovénie

Annulation des mots de passe

Si vous oubliez le mot de passe, vous ne pouvez pas accéder à l'ordinateur. Reportez-vous au *Manuel de résolution des problèmes* pour connaître la procédure d'effacement des mots de passe.

Si le système est équipé d'un périphérique de sécurité intégré, reportez-vous au manuel *HP ProtectTools Security Manager* à l'adresse http://www.hp.com.

DriveLock

DriveLock est une fonction de sécurité normalisée qui empêche tout accès non autorisé aux données stockées sur des disques durs ATA. Elle a été implémentée comme une extension de Computer Setup. Cette fonction est uniquement disponible si des disques durs prenant en charge le jeu de commandes ATA Security sont détectés. DriveLock s'adresse aux clients de HP pour lesquels la sécurité des données revêt une importance capitale. Pour eux, le coût du disque dur et la perte des données qu'il contient sont futiles par rapport au drame que représenterait l'accès non autorisé à ces données. Pour établir un compromis entre ce niveau de sécurité extrême et la nécessité de pouvoir remplacer un mot de passe oublié, HP utilise un schéma de sécurité à deux mots de passe dans la mise en oeuvre DriveLock. L'un d'eux est défini et utilisé par l'administrateur du système tandis que l'autre est généralement défini et employé par l'utilisateur final. Si ces deux mots de passe sont oubliés, il n'y a plus aucun moyen de débloquer le disque. C'est pourquoi il est plus sûr d'utiliser DriveLock lorsque les données stockées sur le disque dur sont répliquées sur un système général d'entreprise ou régulièrement sauvegardées. En cas de perte des deux mots de passe utilisés par DriveLock, le disque dur est inutilisable. Les utilisateurs qui ne correspondent pas au profil défini plus haut ne peuvent pas se permettre de prendre ce risque. En revanche, les clients qui présentent ce profil ne courent pas un gros danger compte tenu de la nature des données stockées sur le disque dur.

Utilisation de DriveLock

Lorsque un ou plusieurs disques durs prenant en charge le jeu de commandes ATA Security sont détectés, l'option DriveLock apparaît dans le menu Sécurité de Computer Setup. L'utilisateur peut choisir de définir le mot de passe principal ou d'activer DriveLock. Pour activer DriveLock, vous devez fournir un mot de passe d'utilisateur. Dans la mesure où la configuration initiale de DriveLock est généralement effectuée par un administrateur système, il convient de commencer par définir le mot de passe principal. HP encourage les administrateurs système à définir un mot de passe principal, qu'ils envisagent ou non d'activer DriveLock. De cette manière, si le disque dur venait à être verrouillé, l'administrateur serait en mesure de modifier les paramètres DriveLock. Une fois le mot de passe principal défini, l'administrateur système peut activer DriveLock ou laisser cette option désactivée.

Si le disque dur est verrouillé, l'auto-test de mise sous tension (POST) exige un mot de passe pour le déverrouiller. Si un mot de passe de mise sous tension est défini et s'il correspond au mot de passe d'utilisateur, POST n'invite pas l'utilisateur à entrer une seconde fois son mot de passe. Dans le cas contraire, l'utilisateur est invité à entrer un mot de passe DriveLock. Sur un démarrage à froid, le mot de passe principal ou le mot de passe d'utilisateur peut être utilisé. Sur un démarrage à chaud, entrez le même mot de passe que celui utilisé pour déverrouiller le disque durant le démarrage à froid précédent. Le nombre de tentatives est limité à deux. Sur un démarrage à froid, si toutes deux échouent, POST continue, mais le disque reste inaccessible. Sur un démarrage à chaud ou un redémarrage de Windows, si toutes deux échouent, POST s'arrête et l'utilisateur doit mettre l'ordinateur hors puis sous tension.

Applications de DriveLock

La fonction de sécurité DriveLock est surtout utilisée dans les entreprises. L'administrateur système est responsable de la configuration du disque dur, qui comprend notamment la définition du mot de passe

DriveLock principal et d'un mot de passe d'utilisateur temporaire. Si l'utilisateur oublie son mot de passe ou si un autre employé récupère l'équipement, le mot de passe principal permet de redéfinir le mot de passe d'utilisateur et d'accéder à nouveau au disque dur.

HP recommande aux administrateurs système d'entreprise qui choisissent d'activer DriveLock de mettre au point une stratégie commune pour la définition et la gestion des mots de passe principaux. Cela permet d'éviter les situations où un employé définit les deux mots de passe DriveLock (intentionnellement ou non) avant de quitter l'entreprise. Dans un tel scénario, le disque dur devient inutilisable et doit être remplacé. De même, s'ils ne définissent pas de mot de passe principal, les administrateurs système risquent de se retrouver dans l'incapacité d'accéder à un disque dur afin d'y effectuer les opérations d'administration habituelles, notamment de vérifier qu'il ne contient pas de logiciels non autorisés, et de procéder au contrôle d'inventaire et à la maintenance.

Aux utilisateurs dont les contraintes de sécurité sont moins sévères, HP recommande de ne pas activer DriveLock. Il s'agit notamment des particuliers ou des employés qui ne gèrent pas de données confidentielles sur leur disque dur. Pour ces personnes, la perte d'un disque dur due à l'oubli des deux mots de passe est bien plus grave comparée à la valeur des données. L'accès à Computer Setup et à DriveLock peut être limité à l'aide d'un mot de passe de configuration. En spécifiant un mot de passe de configuration qu'il ne communique pas aux utilisateurs, l'administrateur peut empêcher ces derniers d'activer DriveLock.

Capteur Smart Cover

Disponible sur certains modèles seulement, le capteur de retrait du capot est une combinaison de technologie matérielle et logicielle qui vous avertit lorsque le capot ou le panneau latéral de l'ordinateur est retiré. Il existe trois niveaux de protection, décrits dans le tableau suivant :

Tableau 11-2 Niveaux de protection du capteur Smart Cover

Niveau	Paramètre	Description
Niveau 0	Désactivé	Le capteur Smart Cover est inactif (option par défaut).
Niveau 1	Avertir utilisateur	Au redémarrage de l'ordinateur, affichage d'un message signalant que le capot ou que le panneau latéral de l'ordinateur a été retiré.
Niveau 2	Mot de passe de configuration	Au redémarrage de l'ordinateur, affichage d'un message signalant que le capot ou que le panneau latéral de l'ordinateur a été retiré. Vous devez saisir votre mot de passe de configuration pour pouvoir continuer.

REMARQUE : Ces paramètres peuvent être modifiés à l'aide de Computer Setup. Pour plus d'informations sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*.

Configuration du niveau de protection du capteur Smart Cover

Pour définir le niveau de protection du capteur Smart Cover, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Sélectionnez **Sécurité** > **Smart Cover** > **Cover Removal Sensor** (Capteur de retrait du capot), puis sélectionnez le niveau de sécurité souhaité.
4. Avant de quitter, sélectionnez **Fichier** > **Enregistrer et quitter**.

Verrou Smart Cover

Le verrou Smart Cover est un dispositif de verrouillage contrôlé par logiciel, présent sur certains ordinateurs HP. Ce système empêche tout accès non autorisé aux composants internes de l'ordinateur. Les ordinateurs sont livrés avec le verrou en position déverrouillée.

△ **ATTENTION :** Pour obtenir une sécurité Cover Lock optimale, créez un mot de passe de configuration. Le mot de passe de configuration empêche l'accès non autorisé à l'utilitaire Computer Setup.

REMARQUE : Le verrou Smart Cover est disponible en option sur certains modèles.

Mise en place du verrou Smart Cover

Pour activer et mettre en place le verrou Smart Cover, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Sélectionnez **Sécurité** > **Smart Cover** > **Cover Lock** (Verrou du capot) > **Lock option** (Option de verrou).
4. Avant de quitter, sélectionnez **Fichier** > **Enregistrer et quitter**.

Désactivation du verrou Smart Cover

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer** > **Arrêter** > **Redémarrer**.
2. Dès que l'ordinateur est mis sous tension, appuyez sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à la configuration de l'ordinateur (Computer Setup). Appuyez sur Entrée pour ignorer l'écran de titre, si vous le souhaitez.

   REMARQUE : Si vous n'appuyez pas sur la touche F10 au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche F10 avant que l'ordinateur ne démarre le système d'exploitation pour accéder à l'utilitaire.

3. Sélectionnez **Sécurité** > **Smart Cover** > **Cover Lock** (Verrou du capot) > **Unlock** (Déverrouiller).
4. Avant de quitter, sélectionnez **Fichier** > **Enregistrer et quitter**.

Utilisation de la clé Smart Cover FailSafe

Si vous activez le verrou Smart Cover et que vous ne pouvez pas entrer le mot de passe pour le désactiver, vous aurez besoin d'une clé Smart Cover FailSafe pour ouvrir le capot de l'ordinateur. La clé vous sera également nécessaire en cas de :

- Coupure de courant
- Panne au démarrage
- Défaillance d'un composant (processeur ou alimentation, par exemple)
- Oubli d'un mot de passe

△ **ATTENTION :** La clé Smart Cover FailSafe est un outil spécialisé fourni par HP. Pour parer à toute éventualité, commandez cette clé avant d'en avoir besoin en vous adressant à un revendeur ou un mainteneur agréé.

Pour vous procurer la clé FailSafe, suivez l'une de ces suggestions :

- Adressez-vous à un revendeur ou un mainteneur agréé HP.
- Consultez la liste des numéros de téléphone indiqués dans le document de garantie pour appeler le numéro vous concernant.

Pour plus d'informations sur l'utilisation de la clé Smart Cover FailSafe, consultez le *Manuel de référence du matériel*.

Dispositif antivol

Le panneau arrière de l'ordinateur (certains modèles) est prévu pour recevoir un dispositif antivol permettant d'attacher physiquement l'ordinateur à un poste de travail.

Pour obtenir des instructions illustrées, consultez le *Manuel de référence du matériel*.

Identification des empreintes digitales

Tout en dispensant l'utilisateur de saisir des mots de passe, la technologie de reconnaissance des empreintes digitales élaborée par HP renforce la sécurité du réseau, simplifie la procédure de connexion et réduit les coûts relatifs à la gestion des réseaux d'entreprise. Son coût abordable ne la réserve désormais plus aux seuls organismes de pointe disposant d'un système de sécurité très élaboré.

REMARQUE : La prise en charge de la technologie d'identification des empreintes digitales varie en fonction des modèles.

Notification des pannes et récupération

Les fonctions de notification des pannes et de dépannage allient une technologie innovante, matérielle et logicielle, pour éviter la perte de vos données essentielles et réduire les temps d'inactivité imprévus.

Si l'ordinateur est connecté à un réseau supervisé par le logiciel HP Client Manager, cet ordinateur signale toute panne à l'application de supervision du réseau. Le logiciel HP Client Manager permet également de programmer des diagnostics à distance pour qu'ils s'exécutent automatiquement sur tous les PC supervisés et obtenir un rapport sur les tests qui ont échoués.

Système de protection d'unité DPS

Le système de protection d'unité DPS (Drive Protection System) est un outil de diagnostic intégré aux disques durs installés sur certains ordinateurs. Le DPS est conçu pour aider au diagnostic des problèmes pouvant conduire à un remplacement du disque dur non pris en charge par la garantie.

Lors de la construction des ordinateurs HP, chaque disque dur installé est testé avec le système DPS, et un enregistrement permanent des informations clés est écrit sur le disque. À chaque test DPS, les résultats sont inscrits sur le disque dur. Le fournisseur de services peut ensuite utiliser ces informations pour le diagnostic des pannes vous ayant conduit à exécuter le logiciel DPS. Reportez-vous au *Manuel de résolution des problèmes* pour connaître la procédure d'utilisation de DPS.

Alimentation avec protection contre les surtensions

Un système intégré de protection contre les surtensions assure une plus grande fiabilité de l'ordinateur en cas de surtension imprévisible. Cette alimentation peut supporter une surtension de 2 000 volts sans temps d'arrêt du système, ni de perte de données.

Capteur thermique

Le capteur thermique est une fonction matérielle et logicielle qui contrôle la température interne de l'ordinateur. Cette fonction affiche un message d'avertissement en cas de dépassement de la plage normale de températures, ce qui permet de prendre des mesures avant que les composants internes ne soient endommagés ou que des données ne soient perdues.

△ **ATTENTION :** Une situation de température élevée peut endommager le système ou causer la perte de données.

Index