



# **Manuel de supervision des ordinateurs de bureau**

## Business Desktops

Référence : 312947-052

**Septembre 2003**

Ce manuel contient des définitions et des instructions relatives aux fonctions de sécurité et de Supervision intelligente préinstallées sur certains modèles.

© 2003 Hewlett-Packard Development Company, L.P.

HP, Hewlett Packard et le logo Hewlett-Packard sont des marques de Hewlett-Packard Company aux États-Unis et dans d'autres pays.

Compaq et le logo Compaq sont des marques de Hewlett-Packard Development Company, L.P. aux États-Unis et dans d'autres pays.

Microsoft, MS-DOS, Windows et Windows NT sont des marques de la société Microsoft aux États-Unis et dans d'autres pays.

Tous les autres noms de produits mentionnés dans le présent document sont des marques appartenant à leurs détenteurs respectifs.

Hewlett-Packard Company ne saurait être tenu responsable des erreurs ou omissions techniques ou rédactionnelles qui pourraient subsister dans ce document, ni des dommages accidentels ou consécutifs à la fourniture, aux résultats obtenus ou à l'utilisation du présent matériel. Les informations de ce document sont fournies "en l'état" sans garantie d'aucune sorte, y compris et sans limitation, les garanties implicites de qualité marchande et d'aptitude à un usage particulier ; de plus, ces informations sont susceptibles d'être modifiées sans préavis. Les garanties applicables aux produits HP sont énoncées dans les textes de garantie limitée accompagnant ces produits. Aucune partie du présent document ne saurait être interprétée comme constituant un quelconque supplément de garantie.

Ce document contient des informations protégées par des droits d'auteur. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'accord écrit préalable de Hewlett-Packard Company.



**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, autant pour le matériel que pour les informations qu'il contient.

---

## **Manuel de supervision des ordinateurs de bureau**

Business Desktops

Deuxième édition (septembre 2003)

Référence : 312947-052

---

# Table des matières

## Manuel de supervision des ordinateurs de bureau

Configuration initiale et déploiement .....	2
Installation de système à distance .....	3
Mise à jour et supervision des logiciels .....	4
HP Client Manager Software .....	4
Altiris Solutions .....	4
Altiris PC Transplant Pro .....	6
System Software Manager .....	6
Notification préventive des modifications .....	6
ActiveUpdate .....	7
Réécriture de la ROM .....	7
Réécriture de la ROM à distance .....	8
HPQFlash .....	8
Bloc de démarrage ROM FailSafe .....	8
Réplication de la configuration .....	10
Bouton d'alimentation double état .....	19
Site Web .....	20
Composantes et partenaires .....	21
Le suivi et la sécurité du parc .....	21
Sécurité par mot de passe .....	26
Création d'un mot de passe de configuration à l'aide de Computer Setup .....	26
Saisie d'un mot de passe de mise sous tension dans Computer Setup .....	27
Sécurité intégrée .....	32
DriveLock .....	42
Capteur Smart Cover .....	45
Verrou Smart Cover .....	46
Sécurité du secteur d'amorçage principal .....	48
Avant de partitionner ou de formater le disque amorçable actuel .....	50
Dispositif antivol .....	51
Identification des empreintes digitales .....	51

Notification des pannes et récupération .....	51
Système de protection d'unité DPS .....	52
Alimentation avec protection contre les surtensions .....	52
Capteur thermique.....	52

## **Index**

---

# Manuel de supervision des ordinateurs de bureau

La Supervision intelligente HP offre des solutions 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 supervisés. HP détient 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 travaille en étroite collaboration avec les principaux éditeurs de logiciels de supervision, de manière à assurer la compatibilité entre la Supervision intelligente et leurs produits. L'utilitaire Supervision intelligente constitue un élément important de notre engagement à vous offrir des solutions fiables et durables, destinées à vous assister au cours des quatre phases du cycle de vie de l'ordinateur de bureau, à savoir la planification, la mise en œuvre, la supervision et les migrations.

Les caractéristiques essentielles de la supervision sont :

- La configuration initiale et le déploiement
- L'installation à distance du système
- La mise à jour et la supervision des logiciels
- La réécriture de la ROM
- Le suivi et la sécurité du parc
- La notification des pannes et la restauration



La prise en charge de certaines fonctionnalités spécifiques décrites dans ce manuel peut varier d'un modèle d'ordinateur ou d'une version de logiciel à l'autre.

---

## Configuration initiale et déploiement

Les ordinateurs sont livrés avec un ensemble de logiciels système préinstallés. Après une courte opération de décompagnage 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 décompagnage de l'ensemble des logiciels préinstallés.
- Utilisation d'outils de déploiement, tels que Altiris Deployment Solution™, 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. La section PC Deployment du site Internet Solutions and Services à l'adresse (<http://h18000.www1.hp.com/solutions/pcsolutions>) vous donne des informations quant à la méthode de déploiement optimale.

Le CD *Restore Plus!*, l'utilitaire de configuration en ROM (RBSU) 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.

## Installation de système à distance

L'installation de système à distance vous 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 du système est généralement utilisée comme utilitaire d'installation et de configuration du système, et permet d'effectuer 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 en mémoire flash ("[Réécriture de la ROM à distance](#)" page 8).
- Configuration des paramètres du BIOS système.

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

HP et Altiris, Inc. ont collaboré à la réalisation d'outils permettant de faciliter et d'accélérer le déploiement des ordinateurs dans les entreprises et ont réussi à réduire considérablement le coût total de possession des PC HP, ce qui en fait les PC client les plus faciles à superviser en environnement d'entreprise.

## Mise à jour et supervision des logiciels

HP fournit plusieurs outils de supervision et de mise à jour des logiciels sur les ordinateurs de bureau et les stations de travail : Altiris, Altiris PC Transplant Pro, HP Client Manager Software (solution Altiris), System Software Manager, Proactive Change Notification et ActiveUpdate.

### HP Client Manager Software

HP Client Manager (HP CMS) intègre étroitement la technologie HP de Supervision intelligente dans Altiris eXpress pour offrir des fonctions avancées de supervision matérielle des périphériques d'accès HP. Il propose, entre autres :

- Des vues détaillées de l'inventaire matériel pour la gestion des actifs.
- Un suivi de l'état du PC et des diagnostics.
- Une notification proactive des modifications de l'environnement matériel.
- Des rapports accessibles par le Web contenant des détails critiques pour l'entreprise comme, par exemple, des avertissements de surchauffe, des alertes mémoire, etc.
- La mise à niveau à distance des logiciels système, comme les drivers de périphériques et le BIOS de la mémoire morte.
- Le changement à distance de l'ordre d'amorçage.

Pour plus d'informations sur le logiciel HP Client Manager, consultez le site [http://h18000.www1.hp.com/im/client\\_mgr.html](http://h18000.www1.hp.com/im/client_mgr.html).

### Altiris Solutions

Les solutions HP Client Management permettent une supervision centralisée du matériel client HP couvrant tous les aspects du cycle de vie des équipements informatiques.



- Inventaire et gestion du parc
  - ❑ Conformité des licences de logiciels
  - ❑ Suivi des PC et rapports
  - ❑ Contrats de location, définissant le suivi du parc
- Déploiement et migration
  - ❑ Migration vers Microsoft Windows 2000 ou Windows XP édition professionnelle ou familiale
  - ❑ Déploiement du système
  - ❑ Migrations personnelles
- Centre d'assistance et résolution des problèmes
  - ❑ Gestion des tickets du centre d'assistance
  - ❑ Dépannage à distance
  - ❑ Résolution des problèmes à distance
  - ❑ Restauration en cas de sinistre client
- Mise à jour et supervision des logiciels
  - ❑ Supervision régulière des ordinateurs
  - ❑ Déploiement du logiciel système HP
  - ❑ Autorétablissement des applications

Sur certains modèles d'ordinateurs de bureau et de portables, les logiciels préinstallés en usine comprennent un agent de supervision Altiris. Cet agent permet de communiquer avec Altiris Development Solution qui peut alors servir à déployer un nouveau matériel ou effectuer une migration personnalisée vers un nouveau système d'exploitation offrant des assistants faciles à utiliser. Les solutions Altiris se caractérisent par des possibilités de distribution de logiciels simples. Utilisées avec le System Software Manager ou le Client Manager de HP, ces solutions permettent également la mise à niveau du BIOS ROM et des drivers de périphériques à partir d'une console centrale.

Pour plus d'informations, consultez le site  
<http://www.hp.com/go/easydeploy>.

## Altiris PC Transplant Pro

Altiris PC Transplant Pro permet une migration simple qui préserve les anciens paramètres, les préférences et les données des PC en les transférant rapidement dans leur nouvel environnement. En quelques minutes, et non pas en heures ou en jours, les PC fonctionnent et se présentent comme les utilisateurs le souhaitent.

Pour plus d'informations sur l'obtention d'une version d'évaluation de 30 jours entièrement fonctionnelle, consultez le site

<http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

## System Software Manager

System Software Manager (SSM) est un utilitaire qui permet la mise à jour du logiciel système sur plusieurs ordinateurs à la fois. Exécuté sur un PC client, SSM détecte les versions matérielles et logicielles et met à jour les logiciels à partir d'un point central de stockage de fichiers. Les versions de drivers prises en charge par le SSM sont identifiées par une icône spéciale sur le site de téléchargement ou sur le CD Support Software. Pour plus d'informations sur l'utilitaire SSM ou pour le télécharger, consultez le site :

<http://h18000.www1.hp.com/im/ssmwp.html>.

## Notification préventive des modifications

Le programme de notification préventive des modifications utilise le site Web choisi par l'abonné pour :

- Envoyer automatiquement des e-mails de notification indiquant les modifications de matériel et de logiciel pour la plupart des ordinateurs et serveurs professionnels, 60 jours à l'avance.
- Envoyer par courrier électronique, des bulletins, des conseils, des notes de sécurité et des alertes concernent les drivers pour la plupart des ordinateurs et serveurs professionnels.

L'abonné définit lui-même son profil afin de recevoir des informations spécifiques à son environnement informatique. Pour en savoir plus sur le programme de notification préventive et créer un profil personnalisé, consultez le site <http://www.hp.com/go/pcn>.

## ActiveUpdate

ActiveUpdate est une application HP s'exécutant sur un ordinateur client. Sur le système local, ActiveUpdate utilise le profil défini par l'utilisateur pour télécharger proactivement et automatiquement les mises à jour logicielles pour la plupart des ordinateurs et serveurs professionnels. Les mises à jour téléchargées peuvent alors être déployées intelligemment sur les machines auxquelles elles sont destinées grâce aux utilitaires HP Client Manager et System Software Manager.

Pour en savoir plus sur ActiveUpdate, télécharger l'application et créer un profil personnalisé, consultez le site <http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html>.

## Réécriture de la ROM

L'ordinateur est doté d'une mémoire programmable appelée mémoire flash. Si vous définissez un mot de passe de configuration dans l'utilitaire Computer Setup (F10), vous pouvez protéger cette mémoire contre toute mise à jour ou effacement malencontreux. Il est important de protéger ainsi l'intégrité fonctionnelle de l'ordinateur. Si vous souhaitez mettre la mémoire flash à jour, vous pouvez :

- Commander la disquette ROMPaq à jour auprès de HP.
- Télécharger l'image ROMPaq la plus récente depuis le site <http://h18000.www1.hp.com/im/ssmwp.html>.



**ATTENTION :** pour une protection optimale de la ROM, n'oubliez pas de définir un mot de passe de configuration. Le mot de passe de configuration empêche toute mise à jour non autorisée de la ROM. L'utilitaire System Software Manager permet à l'administrateur système de définir le mot de passe de configuration sur un ou plusieurs PC simultanément. Pour plus d'informations, consultez le site <http://h18000.www1.hp.com/im/ssmwp.html>.

---

## Réécriture de la ROM à distance

L'utilitaire Remote ROM Flash permet à l'administrateur système de mettre à jour la ROM d'ordinateurs HP distants à partir d'une console de supervision réseau centralisée. Dans la mesure où l'administrateur système peut effectuer cette tâche à distance sur plusieurs ordinateurs, il obtient un déploiement cohérent et un meilleur contrôle sur les images ROM des PC HP du réseau. Il s'ensuit également une augmentation de la productivité et une diminution du coût d'exploitation.



L'ordinateur doit être en marche ou activé à l'aide de Réveil à distance (Remote Wakeup) pour pouvoir utiliser la fonction de réécriture à distance de la ROM.

Pour de plus amples informations sur la mise à jour à distance de la ROM, veuillez consulter les rubriques HP Client Manager Software ou System Software Manager sur le site <http://h18000.www1.hp.com/im/prodinfo.html>.

## HPQFlash

L'utilitaire HPQFlash permet de mettre à jour ou de restaurer localement la ROM système sur des PC particuliers via un système d'exploitation Windows.

Pour plus d'informations sur l'utilitaire HPQFlash, consultez le site <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html>.

## Bloc de démarrage ROM FailSafe

Le bloc d'amorçage ROM FailSafe permet de restaurer le système dans le cas improbable d'une panne de la ROM, par exemple si une coupure de courant se produisait pendant une mise à niveau de la ROM. Ce bloc d'amorçage est une section de la ROM protégée contre la réécriture qui contrôle la validité de la réécriture de la ROM système à chaque démarrage de l'ordinateur.

- Si la mémoire morte du système est valide, le système démarre normalement.
- Si le test de validité échoue, le bloc de démarrage ROM FailSafe assure une prise en charge suffisante pour démarrer le système à partir d'une disquette ROMPaq, qui programmera une image valide pour la mémoire morte du système.

Si le bloc d'amorçage détecte une ROM système non valide, le voyant d'alimentation du système clignote en rouge 8 fois, à une seconde d'intervalle, puis s'arrête de clignoter pendant deux secondes. L'ordinateur émet en même temps 8 signaux sonores. Un message indiquant le passage au mode de récupération du bloc d'amorçage s'affiche alors à l'écran (certains modèles).

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

1. Si l'unité de disquette contient une disquette, retirez-la et éteignez l'ordinateur.
2. Insérez une disquette ROMPaq dans l'unité de disquette.
3. Mettez le système sous tension.
4. Si aucune disquette ROMPaq n'est détectée, vous devrez en insérer une et redémarrer l'ordinateur.
5. Si un mot de passe de configuration a été défini, le voyant Verr maj s'allume et un message vous demande d'entrer le mot de passe en question.
6. Saisissez le mot de passe de configuration.
7. Si le système démarre à partir de la disquette et reprogramme la mémoire morte avec succès, les trois voyants du clavier s'allument. Une série de signaux sonores allant crescendo indique le succès de l'opération.
8. Retirez la disquette de l'unité de disquette et éteignez l'ordinateur.
9. Remettez l'ordinateur sous tension pour le redémarrer.

Le tableau suivant donne la liste des différentes combinaisons de voyants utilisées par le bloc d'amorçage ROM (dans le cas d'un clavier PS/2), ainsi que leur signification et les opérations à effectuer selon la combinaison.

## Combinaisons des voyants du clavier utilisées par le bloc d'amorçage ROM

Mode Bloc d'amorçage Failsafe	Couleur du voyant du clavier	Clavier activité des voyants	État/Message
Verr num	Vert	Allumé	La disquette ROMPaq est absente, défectueuse ou l'unité n'est pas prête.
Verr maj	Vert	Allumé	Saisissez le mot de passe.
Verr num, Verr maj, Arrêt défil	Vert	Séquence de clignotement d'un voyant à la fois (V, M, AD)	Clavier verrouillé en mode réseau.
Verr num, Verr maj, Arrêt défil	Vert	Allumé	Réussite du bloc de démarrage ROM Flash. Éteignez, puis rallumez l'ordinateur pour le relancer.



Les voyants de diagnostic ne clignotent pas sur les claviers USB.

## Réplication de la configuration

Les procédures ci-dessous 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.



Les deux procédures nécessitent une unité de disquette ou un périphérique USB prenant en charge l'écriture sur mémoire flash, par exemple HP Drive Key.

## Copie sur un seul PC



**ATTENTION** : les paramètres de configuration sont spécifiques à un modèle. Le système de fichiers de l'ordinateur cible peut être altéré si l'ordinateur source est d'un modèle différent. Par exemple, ne copiez pas la configuration d'un ordinateur D510 format compact sur un D510 e-pc.

---

1. Sélectionnez une configuration à copier. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
  2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.
- 



Si vous n'appuyez pas à temps sur la touche **F10**, vous devez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Insérez une disquette ou un périphérique USB à mémoire flash.
4. Cliquez sur **File > Save to Diskette (Fichier > Enregistrer sur disquette)**. Suivez ensuite les instructions à l'écran pour copier la configuration sur le support de votre choix.
5. Éteignez l'ordinateur qui vous désirez configurer et insérez la disquette ou le périphérique USB à mémoire flash.
6. Allumez l'ordinateur à configurer. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.
7. Cliquez sur **File > Restore from Diskette (Fichier > Restaurer à partir d'une disquette)** et suivez les instructions affichées à l'écran.
8. Redémarrez l'ordinateur une fois la configuration terminée.

## Copie sur plusieurs ordinateurs

---



**ATTENTION :** les paramètres de configuration sont spécifiques à un modèle. Le système de fichiers de l'ordinateur cible peut être altéré si l'ordinateur source est d'un modèle différent. Par exemple, ne copiez pas la configuration d'un ordinateur D510 format compact sur un D510 e-pc.

---

Cette méthode demande un peu plus de temps pour préparer la disquette ou le périphérique USB à mémoire flash ; toutefois, la copie de la configuration sur les ordinateurs cibles est nettement plus rapide.

---



Il n'est pas possible de créer une disquette de démarrage sous Windows 2000. La procédure qui suit nécessite soit une disquette amorçable, soit un périphérique USB à mémoire flash amorçable. Si vous ne disposez pas d'un ordinateur exécutant Windows 9x ou Windows XP pour créer une disquette amorçable, vous devrez appliquer la méthode de copie sur un seul PC (voir "[Copie sur un seul PC](#)" page 11).

---

1. Créez une disquette ou un périphérique USB à mémoire flash amorçable. Reportez-vous à "[Disquette amorçable](#)" page 13, "[Périphériques USB à mémoire flash compatibles](#)" page 14 ou "[Périphériques USB à mémoire flash non pris en charge](#)" page 17.
- 



**ATTENTION :** tous les ordinateurs ne peuvent pas être démarrés à partir d'un périphérique USB à mémoire flash. Si l'ordre d'amorçage par défaut de Computer Setup (F10) indique le périphérique USB avant le disque dur, l'ordinateur peut être démarré à partir d'un périphérique USB à mémoire flash. Dans le cas contraire, vous devez utiliser une disquette amorçable.

---

2. Sélectionnez une configuration à copier. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
  3. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.
- 



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---



4. Insérez la disquette ou le périphérique USB à mémoire flash amorçable.
5. Cliquez sur **File > Save to Diskette (Fichier > Enregistrer sur disquette)**. Suivez ensuite les instructions à l'écran pour copier la configuration sur le support de votre choix.
6. Téléchargez un utilitaire BIOS pour la réplication de la configuration (repset.exe) et copiez-le sur la disquette ou le périphérique USB à mémoire flash. Vous trouverez cet utilitaire sur le site <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html>.
7. Sur la disquette ou le périphérique USB de configuration, créez un fichier autoexec.bat contenant les commandes suivantes :  
**repset.exe**
8. Éteignez l'ordinateur à configurer. Insérez la disquette ou le périphérique USB à mémoire flash amorçable et allumez l'ordinateur. L'utilitaire de configuration s'exécutera automatiquement.
9. Redémarrez l'ordinateur une fois la configuration terminée.

## Création d'un support amorçable

### Disquette amorçable

---



La procédure qui suit est destinée à Windows XP édition professionnelle ou familiale Windows 2000 ne prend pas en charge la création de disquettes amorçables.

---

1. Insérez une disquette dans l'unité de disquette.
2. Cliquez sur **Démarrer**, puis sur **Poste de travail**.
3. Cliquez avec le bouton droit sur la lettre de l'unité de disquette et sélectionnez **Formater**.
4. Cochez la case **Créer une disquette de démarrage MS-DOS**, puis cliquez sur le bouton **Démarrer**.

Retournez à la section "[Copie sur plusieurs ordinateurs](#)" page 12.

## Périphériques USB à mémoire flash compatibles

Les périphériques pris en charge, tels que HP Drive Key ou DiskOnKey, ont une image préinstallée qui simplifie la procédure pour les rendre amorçables. Si le périphérique Drive Key utilisé ne contient pas cette image, suivez la procédure présentée plus bas dans cette section (["Périphériques USB à mémoire flash non pris en charge" page 17](#)).



**ATTENTION :** tous les ordinateurs ne peuvent pas être démarrés à partir d'un périphérique USB à mémoire flash. Si l'ordre d'amorçage par défaut de Computer Setup (F10) reprend le périphérique USB figure avant le disque dur, l'ordinateur peut être démarré à partir d'un périphérique USB à mémoire flash. Dans le cas contraire, vous devez utiliser une disquette amorçable.

---

Pour créer un périphérique USB à mémoire flash amorçable, vous devez avoir :

- L'un des systèmes suivants :
  - Ordinateur de bureau Compaq Evo D510 Ultra compact
  - Ordinateur Compaq Evo D510 minitour de format compact
  - Ordinateur HP Compaq Business Desktop d530 ultra compact, compact ou minitour convertible
  - Ordinateur portable Evo N400c, N410c, N600c, N610c, N620c, N800c ou N1000c
  - Ordinateur portable Compaq Presario 1500 ou 2800

Selon leur BIOS, d'autres nouveaux systèmes pourront également prendre en charge l'amorçage à partir d'un périphérique HP Drive Key.



**ATTENTION :** si vous utilisez un ordinateur autre que ceux mentionnés ci-dessus, vérifiez dans l'utilitaire Computer Setup (F10) que le périphérique USB figure avant le disque dur dans l'ordre d'amorçage.

---

- L'un des modules de stockage suivants :
  - HP Drive Key de 16 Mo
  - HP Drive Key de 32 Mo
  - DiskOnKey de 32 Mo

- HP Drive Key de 64 Mo
  - DiskOnKey de 64 Mo
  - HP Drive Key de 128 Mo
  - DiskOnKey de 128 Mo
- Une disquette DOS amorçable contenant les programmes FDISK et SYS. Si vous ne disposez pas du programme SYS, vous pouvez utiliser la commande FORMAT, mais dans ce cas tous les fichiers présents sur le périphérique Drive Key seront effacés.
1. Éteignez l'ordinateur.
  2. Insérez le périphérique Drive Key dans un des ports USB de l'ordinateur et retirez tous les autres périphériques de stockage USB à l'exception des lecteurs de disquette USB.
  3. Insérez une disquette DOS amorçable contenant FDISK.COM et SYS.COM ou FORMAT dans le lecteur de disquette, puis allumez l'ordinateur.
  4. Exécutez FDISK en tapant **FDISK** à la suite de l'invite A:\, puis en appuyant sur Entrée. Si un message vous y invite, cliquez sur **Yes (Y)** pour permettre les disques de grande capacité.
  5. Entrez l'option [**5**] pour afficher les unités de disque du système. Le périphérique Drive Key sera celui dont la taille se rapproche le plus de celle des unités affichées. Il s'agit généralement de la dernière unité de la liste. Notez la lettre de cette unité.  
Unité Drive Key : \_\_\_\_\_



**ATTENTION** : si aucune unité ne correspond au périphérique Drive Key, ne continuez pas. Vous pourriez perdre des données. Vérifiez qu'il ne reste pas d'unité de stockage sur les ports USB. Si vous en trouvez, retirez-les, redémarrez l'ordinateur et continuez à l'étape 4. Si vous n'en trouvez pas, soit le système ne prend pas en charge le périphérique Drive Key, soit celui-ci est défectueux. **NE TENTEZ PAS** de rendre le périphérique Drive Key amorçable.

---

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.

- À l'invite A:\, tapez **SYS x:** où x correspond à la lettre d'unité notée précédemment. Passez à l'étape 13.



**ATTENTION :** assurez-vous d'avoir tapé correctement la lettre d'unité pour le périphérique Drive Key.

---

Une fois les fichiers système transférés, vous revenez à l'invite A:\.

- Copiez tous les fichiers du périphérique Drive Key que vous souhaitez garder dans un répertoire temporaire d'un autre disque (par exemple, le disque dur de l'ordinateur).
- À l'invite A:\, tapez **FORMAT /S X:** où X correspond à la lettre d'unité notée précédemment.



**ATTENTION :** assurez-vous d'avoir tapé correctement la lettre d'unité pour le périphérique Drive Key.

---

La commande FORMAT affiche un ou plusieurs avertissements pour vous demander si vous voulez continuer. Tapez **y** à chaque fois. Le programme FORMAT procède au formatage du périphérique Drive Key, ajoute les fichiers système et vous demande d'entrer un nom de volume.

- Appuyez sur la touche **Entrée** pour aucun nom ou tapez un nom selon vos préférences.
- Recopiez sur le périphérique Drive Key tous les fichiers que vous avez sauvegardés à l'étape.
- Retirez la disquette de l'unité et redémarrez l'ordinateur. L'ordinateur s'amorce sur le périphérique Drive Key en tant qu'unité C.



L'ordre d'amorçage par défaut varie d'un ordinateur à l'autre et peut être modifié dans l'utilitaire Computer Setup (F10).

Si vous avez utilisé une version DOS provenant de Windows 9x, il se peut qu'un logo Windows s'affiche brièvement. Si vous souhaitez le supprimer, ajoutez un fichier de taille zéro nommé LOGI.SYS dans le répertoire principal du périphérique Drive Key.

---

Retournez à la section ["Copie sur plusieurs ordinateurs"](#) page 12.

## Périphériques USB à mémoire flash non pris en charge



**ATTENTION :** tous les ordinateurs ne peuvent pas être démarrés à partir d'un périphérique USB à mémoire flash. Si l'ordre d'amorçage par défaut de Computer Setup (F10) reprend le périphérique USB figure avant le disque dur, l'ordinateur peut être démarré à partir d'un périphérique USB à mémoire flash. Dans le cas contraire, vous devez utiliser une disquette amorçable.

---

Pour créer un périphérique USB à mémoire flash amorçable, vous devez avoir :

- L'un des systèmes suivants :
  - Ordinateur de bureau Compaq Evo D510 Ultra compact
  - Ordinateur Compaq Evo D510 minitour de format compact
  - Ordinateur HP Compaq Business Desktop d530 ultra compact, compact ou minitour convertible
  - Ordinateur portable Evo N400c, N410c, N600c, N610c, N620c, N800c ou N1000c
  - Ordinateur portable Compaq Presario 1500 ou 2800

Selon leur BIOS, d'autres nouveaux systèmes pourront également prendre en charge l'amorçage à partir d'un périphérique USB à mémoire flash.



**ATTENTION :** si vous utilisez un ordinateur autre que ceux mentionnés ci-dessus, vérifiez dans l'utilitaire Computer Setup (F10) que le périphérique USB figure avant le disque dur dans l'ordre d'amorçage.

---

- Une disquette DOS amorçable contenant les programmes FDISK et SYS. Si vous ne disposez pas du programme SYS, vous pouvez utiliser la commande FORMAT, mais dans ce cas tous les fichiers présents sur le périphérique Drive Key seront effacés.
- 1. Si des périphériques SCSI, ATA RAID ou SATA sont connectés à des cartes PCI du système, éteignez l'ordinateur et débranchez son cordon d'alimentation.



**ATTENTION :** le cordon d'alimentation doit être débranché.

---

2. Ouvrez le capot de l'ordinateur et retirez les cartes PCI.
3. Insérez le périphérique Drive Key dans un des ports USB de l'ordinateur et retirez tous les autres périphériques de stockage USB à l'exception des lecteurs de disquette USB. Remettez en place le capot de l'ordinateur.
4. Branchez l'ordinateur et démarrez-le. Dès que le voyant vert du moniteur s'allume, appuyez sur la touche **F10** pour lancer l'utilitaire Computer Setup.
5. Allez dans le menu Advanced/PCI devices (Avancé/Périphériques PCI) et désactivez les contrôleurs IDE et SATA. Lorsque vous désactivez le contrôleur SATA, notez son numéro IRQ. Vous en aurez besoin de ce numéro ultérieurement. Quittez l'utilitaire Computer Setup en confirmant vos changements.  
SATA IRQ : \_\_\_\_\_
6. Insérez une disquette DOS amorçable contenant FDISK.COM et SYS.COM ou FORMAT dans le lecteur de disquette, puis allumez l'ordinateur.
7. Exécutez FDISK et supprimez toute partition présente sur le périphérique USB à mémoire flash. Créez une nouvelle partition et marquez-la comme partition active. Quittez FDISK en appuyant sur la touche **Échap**.
8. Si le système ne redémarre pas automatiquement en quittant FDISK, appuyez sur **Ctrl+Alt+Del** pour redémarrer à partir de la disquette DOS.
9. À l'invite A:\, tapez **FORMAT C: /S** et appuyez sur **Entrée**. Le programme FORMAT procède au formatage du périphérique USB à mémoire flash et vous demande d'entrer un nom de volume.
10. Appuyez sur la touche **Entrée** pour aucun nom ou tapez un nom selon vos préférences.
11. Éteignez l'ordinateur et débranchez son cordon d'alimentation. Ouvrez l'ordinateur et remettez en place les cartes PCI retirées précédemment. Remettez en place le capot de l'ordinateur.
12. Branchez l'ordinateur, retirez la disquette et démarrez-le.
13. Dès que le voyant vert du moniteur s'allume, appuyez sur la touche **F10** pour lancer l'utilitaire Computer Setup.

14. Allez dans le menu Advanced/PCI devices (Avancé/Périphériques PCI) et activez de nouveau les contrôleurs que vous avez désactivé à l'étape 5. Réaffectez le numéro IRQ au contrôleur SATA.
15. Enregistrez vos modifications et quittez. L'ordinateur s'amorce sur le périphérique USB à mémoire flash en tant qu'unité C.



L'ordre d'amorçage par défaut varie d'un ordinateur à l'autre et peut être modifié dans l'utilitaire Computer Setup (F10).

Si vous avez utilisé une version DOS provenant de Windows 9x, il se peut qu'un logo Windows s'affiche brièvement. Si vous souhaitez le supprimer, ajoutez un fichier de taille zéro nommé LOGI.SYS dans le répertoire principal du périphérique Drive Key.

Retournez à la section ["Copie sur plusieurs ordinateurs"](#) page 12.

## Bouton d'alimentation double état

Lorsque l'interface ACPI (Advanced Configuration and Power Interface) est activée sous Windows 2000 et Windows XP édition professionnelle ou familiale, le bouton de mise sous tension peut servir d'interrupteur Marche/Arrêt ou 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 mode où sa consommation électrique est minimale. 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. Sous Windows 2000, cliquez sur le bouton **Démarrer**, puis sélectionnez **Paramètres > Panneau de configuration > Options d'alimentation**.  
Sous Windows XP édition professionnelle ou familiale, cliquez sur le bouton **Démarrer**, puis sélectionnez **Panneau de configuration > Performance et maintenance > Options d'alimentation**.
2. Dans la boîte de dialogue **Propriétés des options d'alimentation**, sélectionnez l'onglet **Paramètres avancés**.
3. Dans le cadre **Bouton d'alimentation**, sélectionnez les options souhaitées.

Lorsque le bouton de mise sous tension est configuré en bouton Suspend, appuyez sur ce bouton pour mettre l'ordinateur en mode d'alimentation faible (Suspend). Appuyez à nouveau sur le bouton pour ramener le système en mode actif. 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 abîmer les données du disque dur.

---

## Site Web

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 personnels for HP computers.

Lorsque vous installez des systèmes d'exploitation nouveaux ou révisés, il est important d'exécuter le logiciel de support 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 périphériques et les utilitaires appropriés afin de garantir la prise en charge correcte et l'exécution de toutes les fonctionnalités.

HP a simplifié la localisation, l'accès, l'évaluation et l'installation du dernier logiciel de support. Vous pouvez télécharger ce logiciel à partir du site <http://www.hp.com/support>.

Ce site contient les derniers drivers de périphériques, 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.



## Composantes et partenaires

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

- Interface de gestion d'ordinateurs de bureau (DMI) 2.0
- WOL (Wake On LAN)
- ACPI
- SMBIOS
- Prise en charge de PXE (Pre-boot Execution)

## Le suivi et la sécurité du parc

Les fonctions de suivi d'inventaire incorporées dans l'ordinateur fournissent les données essentielles d'inventaire qui peuvent être gérées dans HP Insight Manager, HP Client 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 vous permet de choisir l'outil de supervision le mieux adapté à votre environnement et d'exploiter votre 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. Lorsque la puce de sécurité intégrée ProtectTools est installée, l'accès non autorisé aux données n'est pas possible, l'intégrité du système est vérifiée et les utilisateurs tiers qui tentent d'accéder au système sont authentifiés. Les fonctions de sécurité, telles que ProtectTools, le capteur 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.



Protect Tools, le capteur et le verrou Smart Cover sont disponibles en option sur certains modèles.

---

Vous pouvez gérer le paramétrage de sécurité de l'ordinateur HP à l'aide des utilitaires suivants :

- Localement, avec l'utilitaire Computer Setup. Pour en savoir plus et obtenir des instructions sur l'utilisation de Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)* fourni avec l'ordinateur.
- À distance, avec HP Client Manager ou System Software Manager. Ce logiciel permet le déploiement sûr et cohérent, ainsi que le contrôle des paramètres de sécurité à partir d'un simple utilitaire à ligne de commandes.

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).

---

## Présentation des fonctions de sécurité

---

Fonction	But	Mise en place
Contrôle d'amorçage par support amovible	Empêche le démarrage à partir d'unités amovibles (sur certaines unités de disque).	À partir du menu des utilitaires Computer Setup (F10).
Contrôle des interfaces série, parallèle, USB ou infrarouge	Empêche la transmission de données par l'intermédiaire de l'interface série, parallèle, USB (universal serial bus) ou infrarouge intégrée.	À partir du menu des utilitaires Computer Setup (F10).
Mot de passe de démarrage	Interdit l'utilisation de l'ordinateur jusqu'à la saisie du mot de passe. Cela peut s'appliquer à la fois au démarrage initial et au redémarrage du système.	À partir du menu des utilitaires Computer Setup (F10).



Pour plus d'informations sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*.

La prise en charge des options de sécurité peut varier en fonction de la configuration de l'ordinateur.

---

---

**Présentation des fonctions de sécurité (Suite)**


---

<b>Fonction</b>	<b>But</b>	<b>Mise en place</b>
Mot de passe de configuration	Empêche la reconfiguration de l'ordinateur (utilisation de Computer Setup) tant que le mot de passe n'a pas été saisi.	À partir du menu des utilitaires Computer Setup (F10).
Périphérique de sécurité intégré	Empêche tout accès non autorisé aux données en les protégeant par cryptage et mot de passe. Vérifie l'intégrité du système et authentifie les utilisateurs tiers qui tentent d'accéder au système.	À partir du menu des utilitaires Computer Setup (F10).
DriveLock	Empêche tout accès non autorisé aux données stockées sur des disques durs MultiBay. Cette fonctionnalité n'est disponible que sur certains modèles.	À partir du menu des utilitaires Computer Setup (F10).



Pour plus d'informations sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*.


La prise en charge des options de sécurité peut varier en fonction de la configuration de l'ordinateur.

---

---

## Présentation des fonctions de sécurité (Suite)

---

Fonction	But	Mise en place
Capteur Smart Cover	Signale que le capot ou le panneau latéral de l'ordinateur a été retiré. Peut être configuré pour demander la saisie du mot de passe de configuration avant le redémarrage de l'ordinateur, après que le capot ou le panneau latéral ait été retiré. Pour plus d'informations sur cette fonction, reportez-vous au <i>Manuel de référence du matériel</i> figurant sur le CD <i>Documentation Library</i> . Cette fonctionnalité n'est disponible que sur certains modèles.	À partir du menu des utilitaires Computer Setup (F10).
Sécurité du secteur d'amorçage principal	Peut empêcher la modification accidentelle ou malveillante du secteur d'amorçage principal (MBR) du disque d'amorçage actuel et permet de restaurer le "dernier bon MBR connu".	À partir du menu des utilitaires Computer Setup (F10).
Alertes de modification de mémoire	Détectent l'ajout, le déplacement ou le retrait de modules mémoire, et en avertit l'utilisateur et l'administrateur système.	Pour plus d'informations sur l'activation des alertes de modification de mémoire, reportez-vous au guide en ligne <i>Supervision intelligente</i> .
 Pour plus d'informations sur Computer Setup, consultez le <i>Manuel de l'utilitaire Computer Setup (F10)</i> . La prise en charge des options de sécurité peut varier en fonction de la configuration de l'ordinateur.		

---

---

**Présentation des fonctions de sécurité (Suite)**


---

Fonction	But	Mise en place
Étiquette de propriété	Affiche les informations de propriété, définies par l'administrateur, au démarrage du système (protégé par le mot de passe de configuration).	À partir du menu des utilitaires Computer Setup (F10).
Dispositif antivol	Bloque l'accès à l'intérieur de l'ordinateur pour empêcher un changement intempestif de la configuration ou le retrait de composants. Permet également d'attacher l'ordinateur à un objet fixe pour le protéger contre le vol.	Installez un dispositif antivol pour attacher l'ordinateur à un objet fixe.
Boucle antivol	Bloque l'accès à l'intérieur de l'ordinateur pour empêcher un changement intempestif de la configuration ou le retrait de composants.	Installez un verrou dans la boucle de sécurité pour empêcher tout changement indésirable de configuration ou retrait de composant.



Pour plus d'informations sur Computer Setup, consultez le *Manuel de l'utilitaire Computer Setup (F10)*.

La prise en charge des options de sécurité peut varier en fonction de la configuration de l'ordinateur.

---

## Sécurité par mot de passe

Le mot de passe de mise sous tension empêche l'accès non autorisé à l'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. Cela signifie que lorsque l'invite de saisie du mot de passe de mise sous tension s'affiche, vous pouvez saisir le mot de passe de configuration pour 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 le mot de passe de démarrage, même si celui-ci a été défini.

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

Si le système est doté d'un périphérique de sécurité intégré, reportez-vous à "[Sécurité intégrée](#)" page 32.

La création d'un mot de passe de configuration par le biais de l'utilitaire Computer Setup (F10) empêche la reconfiguration de l'ordinateur, à l'aide de ce même utilitaire, tant que le mot de passe n'a pas été saisi.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Sélectionnez **Security (Sécurité)**, puis **Setup Password (Mot de passe de configuration)** et suivez les instructions apparaissant à l'écran.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications et Quitter)**.

## Saisie d'un mot de passe de mise sous tension dans 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 des options de mot de passe (Password Options) dans le menu Security. Ces options comprennent l'invite de mot de passe (Password Prompt) lors du redémarrage à chaud. 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 l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



---

Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Sélectionnez **Security (Sécurité)**, puis **Power-On Password (Mot de passe de démarrage)** et suivez les instructions apparaissant à l'écran.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications et Quitter)**.

## Saisie d'un mot de passe de mise sous tension

Pour saisir un mot de passe de mise sous tension, procédez comme suit :

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 actuel, puis appuyez sur **Entrée**.



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 doté d'un périphérique de sécurité intégré, reportez-vous à "[Sécurité intégrée](#)" page 32.

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

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** 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**.



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 doté d'un périphérique de sécurité intégré, reportez-vous à "[Sécurité intégrée](#)" page 32.

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**. Pour modifier le mot de passe de configuration, exécutez **Computer Setup**.
2. Lorsque l'icône en forme de clé apparaît, saisissez le mot de passe actuel, le caractère de séparation approprié, le nouveau mot de passe, le caractère de séparation approprié, 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**



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

---

3. Appuyez sur **Entrée**.

Le nouveau mot de passe entre en vigueur à la prochaine mise sous tension de l'ordinateur.

---



Pour plus d'informations sur les différents caractères de séparation pouvant être utilisés, reportez-vous à la section "[Caractères de séparation selon les claviers](#)" page 31. Le mot de passe de démarrage et celui de configuration peuvent aussi être modifiés à l'aide des options de sécurité de Computer Setup.

---

## Suppression d'un mot de passe de mise sous tension ou de configuration

Si le système est doté d'un périphérique de sécurité intégré, reportez-vous à "[Sécurité intégrée](#)" page 32.

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**. Pour supprimer le mot de passe de configuration, exécutez **Computer Setup**.
2. Lorsque l'icône en forme de clé apparaît, saisissez le mot de passe actuel suivi du caractère de séparation approprié, comme suit : **mot de passe courant/**
3. Appuyez sur **Entrée**.



Pour plus d'informations sur les différents caractères de séparation pouvant être utilisés, reportez-vous à la section "[Caractères de séparation selon les claviers](#)". Le mot de passe de démarrage et celui de configuration peuvent aussi être modifiés à l'aide des options de sécurité de Computer Setup.

---

## Caractères de séparation selon les claviers

Chaque clavier est conçu pour répondre aux besoins spécifiques de chaque pays. 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	-
BHCSY*	-	Hongrois	-	Espagnol	-
Brésilien	/	Italien	-	Suédois/Finnois	/
Chinois	/	Japonais	/	Suisse	-
Tchèque	-	Coréen	/	Taiïwanais	/
Danois	-	Latino-américain	-	Thaï	/
Français	!	Norvégien	-	Turc	.
Français (Canada)	é	Polonais	-	Anglais (RU)	/
Allemand	-	Portugais	-	Anglais (USA)	/

\* Pour Bosnie-Herzégovine, Croatie, Slovénie et Yougoslavie

## 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 savoir comment effacer des mots de passe.

Si le système est doté d'un périphérique de sécurité intégré, reportez-vous à "[Sécurité intégrée.](#)"

## Sécurité intégrée

La sécurité intégrée ProtectTools se base sur une protection par mot de passe et cryptage pour rehausser le niveau de sécurité des dossiers et fichiers à système de fichiers incorporés (EFS) et pour sécuriser le courrier électronique dans Microsoft Outlook et Outlook Express. ProtectTools est disponible pour certains ordinateurs de bureau à configuration personnalisée (CTO). Il s'adresse aux clients de HP pour lesquels la sécurité des données revêt une importance capitale et qui considèrent que l'accès non autorisé aux données présente beaucoup plus de risques que la perte de données. Dans ProtectTools, quatre mots de passe sont utilisés :

- (F10) Setup – pour lancer l'utilitaire Computer Setup (F10) et activer/désactiver ProtectTools
- Take Ownership (Prise de possession) – ce mot de passe est défini et utilisé par un administrateur système qui accorde les autorisations aux utilisateurs et définit les paramètres de sécurité.
- Emergency Recovery Token (Clé de restauration de secours) – mot de passe défini et utilisé par l'administrateur système et qui permet la restauration en cas de défaillance de l'ordinateur ou de ProtectTools.
- Basic User (Utilisateur) – mot de passe défini par l'utilisateur final.



En cas de perte du mot de passe utilisateur, les données chiffrées ne sont pas récupérables. C'est pourquoi il est plus sûr d'utiliser ProtectTools lorsque les données stockées sur le disque dur de l'utilisateur sont répliquées sur un système général ou régulièrement sauvegardées.

---

La sécurité intégrée ProtectTools consiste à installer (en option) une puce conforme à TCPA 1.1 sur la carte mère de certains ordinateurs de bureau. La puce de sécurité ProtectTools est unique et propre à un ordinateur particulier. Chaque puce exécute les processus de sécurité indépendamment des autres composants de l'ordinateur (processeur, mémoire ou système d'exploitation).

La sécurité intégrée ProtectTools complète et rehausse les fonctions de sécurité prévues dans Microsoft Windows 2000 ou Windows XP édition professionnelle ou familiale. Par exemple, bien que le système d'exploitation puisse coder les fichiers et dossiers locaux sur la base d'un EFS (système de fichiers incorporé), la sécurité intégrée de ProtectTools offre une couche de sécurité supplémentaire en générant des clés de cryptage à partir de la clé principale de la plate-forme (généralement stockée dans un circuit intégré). Ce processus s'appelle généralement "l'emballage" des clés de cryptage. ProtectTools n'empêche pas l'accès par le réseau à un ordinateur non doté d'une puce ProtectTools.

Fonctions essentielles de la sécurité intégrée ProtectTools :

- Authentification de la plate-forme
- Protection du stockage
- Intégrité des données



**ATTENTION :** gardez vos mots de passe en lieu sûr. **Les données codées sont inaccessibles ou irrécupérables sans les mots de passe.**

---

## Définition des mots de passe

### Configuration

Un mot de passe de configuration peut être défini et la sécurité intégrée peut être activée à l'aide de l'utilitaire F10 Setup.

1. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

2. Utilisez les touches Haut et Bas pour sélectionner une langue, puis appuyez sur **Entrée**.
3. Servez-vous des touches Gauche ou Droite pour vous déplacer à l'onglet **Security (Sécurité)**, puis allez à **Setup Password (Mot de passe de configuration)** à l'aide des touches Haut ou Bas. Appuyez sur **Entrée**.

4. Tapez et confirmez un mot de passe. Appuyez sur **F10** pour accepter le mot de passe.



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

5. Utilisez les touches Haut et Bas pour aller dans **Embedded Security Device (Périphérique de sécurité intégré)**. Appuyez sur **Entrée**.
6. Si la boîte de dialogue affiche **Embedded Security Device – Disable**, servez-vous de la flèche gauche ou droite pour obtenir **Embedded Security Device – Enable**. Appuyez sur **F10** pour accepter la modification.



**ATTENTION** : si vous sélectionnez **Reset to Factory Settings – Reset (Rétablir les paramètres d'usine – Restaurer)**, toutes les clés seront effacées et les données chiffrées seront irrécupérables, à moins d'avoir sauvegardé les clés de chiffrement en question (voir "[Prise de possession et clé de restauration de secours](#)"). Ne sélectionnez **Reset (Restaurer)** que si vous y êtes invité dans la procédure de restauration des données codées (voir "[Restauration des données chiffrées](#)" page 37).

7. Utilisez les touches Gauche ou Droite pour aller dans **File (Fichier)**. Utilisez les touches Haut ou Bas pour aller à **Save Changes and Exit (Enregistrer les modifications et Quitter)**. Appuyez sur **Entrée**, puis sur **F10** pour confirmer.

## Prise de possession et clé de restauration de secours

Le mot de passe de prise de possession est requis pour activer ou désactiver le système de sécurité et autoriser l'accès aux utilisateurs. Si le périphérique de sécurité intégrée tombe en panne, le mécanisme de restauration de secours permet à des utilisateurs d'accéder aux données.

1. Dans le cas de Windows XP édition professionnelle ou familiale, cliquez sur **Démarrer > Tous les programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > Embedded Security Initialization Wizard (Assistant d'initialisation de la sécurité intégrée)**.

Dans le cas de Windows 2000, cliquez sur **Démarrer > Programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > Embedded Security Initialization Wizard (Assistant d'initialisation de la sécurité intégrée)**.

2. Cliquez sur **Suivant**.
3. Saisissez et confirmez un mot de passe Take Ownership (prise de possession), puis cliquez sur **Suivant**.



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

---

4. Cliquez sur **Suivant** pour accepter l'emplacement d'archivage de restauration par défaut.
5. Saisissez et confirmez un mot de passe Emergency Recovery Token (clé de restauration d'urgence), puis cliquez sur **Suivant**.
6. Insérez une disquette sur laquelle la clé de restauration de secours sera sauvegardée. Cliquez sur **Parcourir** pour sélectionner l'unité de disquette.



**ATTENTION :** la clé de restauration de secours sert à récupérer les données codées en cas de panne d'ordinateur ou de défaillance de la puce de sécurité intégrée à la carte mère. **Les données codées sont irrécupérables sans cette clé.** (Les données sont également inaccessibles sans le mot de passe utilisateur.) Rangez la disquette dans un endroit sûr.

---

7. Cliquez sur **Save (Enregistrer)** pour accepter l'emplacement et le nom de fichier par défaut, puis cliquez sur **Suivant**.
8. Cliquez sur **Suivant** pour confirmer vos paramètres avant d'initialiser le système de sécurité.



Un message peut vous informer que les fonctions de la sécurité intégrée ne sont pas initialisées. Ne cliquez pas dans la fenêtre de ce message, elle se ferme automatiquement au bout de quelques secondes.

---

9. Cliquez sur **Suivant** pour passer les règles de sécurité locales.
10. Vérifiez que la case Start Embedded Security User Initialization Wizard (Lancer l'Assistant d'initialisation utilisateur) est cochée, puis cliquez sur **Terminer**.

L'Assistant d'initialisation utilisateur démarre automatiquement.

## Utilisateur de base

Le mot de passe de l'utilisateur est créé au cours de l'initialisation utilisateur. Ce mot de passe est requis pour saisir et accéder à des données codées.

---



**ATTENTION** : gardez le mot de passe utilisateur en lieu sûr. **Les données codées sont inaccessibles ou irrécupérables sans ce mot de passe.**

---

1. Si l'Assistant d'initialisation utilisateur n'est pas lancé :

Dans le cas de Windows XP édition professionnelle ou familiale, cliquez sur **Démarrer > Tous les programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > User Initialization Wizard (Assistant d'initialisation utilisateur)**.

Dans le cas de Windows 2000, cliquez sur **Démarrer > Programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > User Initialization Wizard (Assistant d'initialisation utilisateur)**.

2. Cliquez sur **Suivant**.
3. Saisissez et confirmez un mot de passe utilisateur (Basic user), puis cliquez sur **Suivant**.



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

---



4. Cliquez sur **Suivant** pour confirmer.
5. Sélectionnez les fonctions de sécurité appropriées, puis cliquez sur **Suivant**.
6. Cliquez sur le client e-mail approprié pour le sélectionner, puis cliquez sur **Suivant**.
7. Cliquez sur **Suivant** pour appliquer le certificat de cryptage.
8. Cliquez sur **Suivant** pour confirmer.
9. Cliquez sur **Terminer**.
10. Redémarrez l'ordinateur.

## Restauration des données chiffrées

Pour restaurer des données après remplacement de la puce ProtectTools, vous devez disposer de :

- SPEmRecToken.xml – la clé de restauration de secours
- SPEmRecArchive.xml – dossier caché, emplacement par défaut :  
C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Les mots de passe ProtectTools
  - Configuration
  - Prise de possession
  - Clé de restauration d'urgence
  - Utilisateur

1. Redémarrez l'ordinateur.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Saisissez le mot de passe de configuration, puis appuyez sur **Entrée**.

4. Utilisez les touches Haut et Bas pour sélectionner une langue, puis appuyez sur **Entrée**.
5. Servez-vous des touches Gauche ou Droite pour vous déplacer à l'onglet **Security (Sécurité)**, puis allez à **Embedded Security Device (Périphérique de sécurité intégrée)** à l'aide des touches Haut ou Bas. Appuyez sur **Entrée**.
6. Si une seule sélection, **Embedded Security Device – Disable (Périphérique de sécurité intégrée – Désactivé)**, est disponible :
  - a. Utilisez les touches Gauche ou Droite pour activer : **Embedded Security Device – Disable (Périphérique de sécurité intégrée – Activé)**. Appuyez sur **F10** pour accepter la modification.
  - b. Utilisez les touches Gauche ou Droite pour aller dans **File (Fichier)**. Utilisez les touches Haut ou Bas pour aller à **Save Changes and Exit (Enregistrer les modifications et Quitter)**. Appuyez sur **Entrée**, puis sur **F10** pour confirmer.
  - c. Passez à l'étape 1.

Si deux sélections sont disponibles, passez à l'étape 7.

7. Utilisez les touches Haut et Bas pour aller dans **Reset to Factory Settings – Do Not Reset (Rétablir les paramètres d'usine – Ne pas restaurer)**. Appuyez une seule fois sur la touche Gauche ou Droite.

Un message apparaît indiquant que l'exécution de cette action rétablira le périphérique de sécurité intégrée dans sa configuration d'usine si les paramètres sont enregistrés en quittant. Appuyez sur une touche quelconque pour continuer.

Appuyez sur **Entrée**.

8. La sélection présentée est à présent : **Reset to Factory Settings – Reset (Rétablir les paramètres d'usine – Restaurer)**. Appuyez sur **F10** pour accepter la modification.
9. Utilisez les touches Gauche ou Droite pour aller dans **File (Fichier)**. Utilisez les touches Haut ou Bas pour aller à **Save Changes and Exit (Enregistrer les modifications et Quitter)**. Appuyez sur **Entrée**, puis sur **F10** pour confirmer.
10. Redémarrez l'ordinateur.

11. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert.



---

Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

12. Saisissez le mot de passe de configuration, puis appuyez sur **Entrée**.
13. Utilisez les touches Haut et Bas pour sélectionner une langue, puis appuyez sur **Entrée**.
14. Servez-vous des touches Gauche ou Droite pour vous déplacer à l'onglet **Security (Sécurité)**, puis allez à **Embedded Security Device (Périphérique de sécurité intégrée)** à l'aide des touches Haut ou Bas. Appuyez sur **Entrée**.
15. Si la boîte de dialogue affiche **Embedded Security Device – Disable**, servez-vous de la flèche gauche ou droite pour obtenir **Embedded Security Device – Enable**. Appuyez sur **F10**.
16. Utilisez les touches Gauche ou Droite pour aller dans **File (Fichier)**. Utilisez les touches Haut ou Bas pour aller à **Save Changes and Exit (Enregistrer les modifications et Quitter)**. Appuyez sur **Entrée**, puis sur **F10** pour confirmer.
17. Une fois que Windows est lancé :  
  
Dans le cas de Windows XP édition professionnelle ou familiale, cliquez sur **Démarrer > Tous les programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > Embedded Security Initialization Wizard (Assistant d'initialisation de la sécurité intégrée)**.  
  
Dans le cas de Windows 2000, cliquez sur **Démarrer > Programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > Embedded Security Initialization Wizard (Assistant d'initialisation de la sécurité intégrée)**.
18. Cliquez sur **Suivant**.

19. Tapez et confirmez un mot de passe de prise de possession.  
Cliquez sur **Suivant**.



---

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

---

20. Vérifiez que l'option Create a new recovery archive (Créer nouvel archivage de restauration) est sélectionnée. Sous **Recovery archive location (Emplacement d'archivage)**, cliquez sur **Parcourir**.
21. N'acceptez pas le nom de fichier par défaut. Saisissez un autre nom pour éviter de remplacer le fichier d'origine.
22. Cliquez sur **Enregistrer**, puis sur **Suivant**.
23. Saisissez et confirmez un mot de passe Emergency Recovery Token (clé de restauration d'urgence), puis cliquez sur **Suivant**.
24. Insérez une disquette sur laquelle la clé de restauration d'urgence sera sauvegardée. Cliquez sur **Parcourir** pour sélectionner l'unité de disquette.
25. N'acceptez pas le nom de clé par défaut. Saisissez un autre nom pour éviter de remplacer la clé d'origine.
26. Cliquez sur **Enregistrer**, puis sur **Suivant**.
27. Cliquez sur **Suivant** pour confirmer vos paramètres avant d'initialiser le système de sécurité.



---

Un message peut vous informer que la clé de l'utilisateur ne peut pas être chargée. Ne cliquez pas dans la fenêtre de ce message, elle se ferme automatiquement au bout de quelques secondes.

---

28. Cliquez sur **Suivant** pour passer les règles de configuration locales.
29. Décochez la case **Start Embedded Security User Initialization Wizard (Lancer l'Assistant d'initialisation utilisateur)**. Cliquez sur **Terminer**.
30. Cliquez avec le bouton droit sur l'icône ProtectTools dans la barre d'outils et cliquez sur **Initialize Embedded Security restoration (Initialiser la restauration)**.

Cette action lance l'Assistant d'initialisation de la sécurité intégrée HP ProtectTools.

31. Cliquez sur **Suivant**.
32. Insérez la disquette sur laquelle la clé de restauration de secours est enregistrée. Cliquez sur **Parcourir**, puis localisez la clé et double-cliquez dessus pour entrer un nom dans la zone de saisie. Le nom par défaut est A:\SPEmRecToken.xml.
33. Tapez le mot de passe de clé de secours d'origine, puis cliquez sur **Suivant**.
34. Cliquez sur **Parcourir**, puis localisez l'emplacement d'archivage d'origine et double-cliquez dessus pour entrer un nom dans la zone de saisie. Le nom par défaut est C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Cliquez sur **Suivant**.
36. Cliquez sur la machine à restaurer, puis sur **Suivant**.
37. Cliquez sur **Suivant** pour confirmer.
38. Si l'Assistant indique que le système de sécurité a été restauré, passez à l'étape 39.  
  
Si l'Assistant indique que la restauration a échoué, passez à l'étape 10. Vérifiez soigneusement les mots de passe, l'emplacement et le nom de la clé de secours, l'emplacement et le nom d'archivage.
39. Cliquez sur Terminer.
40. Dans le cas de Windows XP édition professionnelle ou familiale, cliquez sur **Démarrer > Tous les programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > User Initialization Wizard (Assistant d'initialisation utilisateur)**.  
  
Dans le cas de Windows 2000, cliquez sur **Démarrer > Programmes > HP ProtectTools Embedded Security Tools (Outils de sécurité intégrée HP ProtectTools) > User Initialization Wizard (Assistant d'initialisation utilisateur)**.
41. Cliquez sur **Suivant**.

42. Cliquez sur **Recover your basic user key (Restaurer la clé de base)**, puis sur **Suivant**.
43. Sélectionnez un utilisateur, saisissez le mot de passe de la clé de secours de cet utilisateur, puis cliquez sur **Suivant**.
44. Cliquez sur **Suivant** pour confirmer vos modifications et accepter l'emplacement des données de restauration.



Les étapes 45 à 49 réinstallent la configuration d'origine pour l'utilisateur de base.

---

45. Sélectionnez les fonctions de sécurité appropriées, puis cliquez sur **Suivant**.
46. Cliquez sur le client e-mail approprié pour le sélectionner, puis cliquez sur **Suivant**.
47. Cliquez sur le certificat de cryptage, puis sur **Suivant** pour l'appliquer.
48. Cliquez sur **Suivant** pour confirmer.
49. Cliquez sur **Terminer**.
50. Redémarrez l'ordinateur.



**ATTENTION** : gardez le mot de passe utilisateur en lieu sûr. **Les données codées sont inaccessibles ou irrécupérables sans ce mot de passe.**

---

## DriveLock

DriveLock est une fonction de sécurité normalisée qui empêche tout accès non autorisé aux données stockées sur des disques durs MultiBay. DriveLock a été implémenté comme une extension de Computer Setup. Cette fonction n'est disponible uniquement lorsque des disques durs prenant en charge DriveLock 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 débloquent 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

L'option DriveLock fait partie du menu Security de l'utilitaire 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 de 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'autotest 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. Il peut utiliser le mot de passe principal ou le mot de passe d'utilisateur. Le nombre de tentatives est limité à deux. Si toutes deux échouent, le POST continue, mais le disque reste inaccessible.

## Applications de DriveLock

La fonction de sécurité DriveLock est surtout utilisée dans les entreprises où un administrateur système fournit aux utilisateurs des disques durs Multibay utilisables sur certains ordinateurs. L'administrateur système est responsable de la configuration du disque dur Multibay, qui comprend notamment la définition du mot de passe DriveLock principal. 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 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 Smart Cover est une combinaison de techniques 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 :

### Niveaux de protection du capteur Smart Cover

Niveau	Paramètre	Description
Niveau 0	Désactivé	Le capteur Smart Cover est inactif (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 le mot de passe de configuration pour pouvoir continuer.



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 l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

3. Sélectionnez **Security (Sécurité)**, puis **Smart Cover**, et suivez les instructions apparaissant à l'écran.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications 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 permet d'empêcher l'accès non autorisé à l'utilitaire Computer Setup.



Le verrou Smart Cover n'est disponible que sur certains modèles.

## Mise en place du verrou Smart Cover

Pour activer et verrouiller le verrou Smart Cover, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

3. Sélectionnez **Security (Sécurité)**, puis **Smart Cover**, et l'option **Locked (Verrouillé)**.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications et Quitter)**.

## Déverrouillage de Smart Cover Lock

1. Mettez l'ordinateur sous tension ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



---

Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Sélectionnez **Security > Smart Cover > Unlocked (Sécurité > Smart Cover > Déverrouillé)**.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications 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. Cette clé vous sera également nécessaire dans les cas suivants :

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



---

**ATTENTION :** la clé Smart Cover FailSafe est un outil spécialisé fourni par HP. N'attendez pas d'avoir besoin de cette clé pour la commander au près d'un Revendeur ou 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 dans la garantie pour appeler le numéro vous concernant.

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

## Sécurité du secteur d'amorçage principal

Le MBR (Master Boot Record) contient les informations nécessaires pour démarrer le système à partir d'un disque et accéder aux données stockées sur ce dernier. La sécurité MBR évite les modifications accidentelles ou malveillantes du MBR, comme celles provoquées par certains virus informatiques ou par l'utilisation erronée de certains utilitaires de disque. Elle permet également de restaurer le "dernier bon MBR" au cas où des modifications du MBR seraient détectées au redémarrage du système.

Pour activer la sécurité MBR, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Sélectionnez **Security (Sécurité) > Master Boot Record Security (Sécurité MBR) > Enabled (Activée)**.
4. Sélectionnez **Security (Sécurité) > Save Master Boot Record (Enregistrement du MBR)**.
5. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications et Quitter)**.

Lorsque la sécurité MBR est activée, le BIOS empêche toute modification du MBR du disque amorçable en cours en mode MS-DOS ou Windows Sans échec.



La plupart des systèmes d'exploitation contrôlent l'accès au MBR du disque amorçable en cours et, par conséquent, le BIOS ne peut empêcher l'ajout de modifications lorsque le système d'exploitation s'exécute.

---

À chaque mise sous tension ou redémarrage de l'ordinateur, le BIOS compare le MBR du disque amorçable actuel au MBR précédemment enregistré. Si des modifications sont détectées et si le disque amorçable actuel est celui à partir duquel le MBR a été précédemment enregistré, le message suivant s'affiche :

1999 – Master Boot Record has changed (Le MBR a été modifié).

Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR.

Dans l'utilitaire Computer Setup, vous devez :

- Enregistrer le MBR du disque amorçable actuel,
- Restaurer le MBR précédemment enregistré, ou
- Désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

Si des modifications sont détectées et si le disque amorçable actuel n'est **pas** le disque à partir duquel le MBR a été précédemment enregistré, le message suivant s'affiche :

2000 – Master Boot Record Hard Drive has changed (Le disque dur du MBR a changé).

Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR.

Dans l'utilitaire Computer Setup, vous devez :

- Enregistrer le MBR du disque amorçable actuel, ou
- Désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

Dans le cas peu probable où le MBR précédemment enregistré aurait été altéré, le message suivant s'affiche :

1998 – Master Boot Record has been lost (Perte du MBR).

Appuyez sur n'importe quelle touche pour accéder au programme Computer Setup et configurer la sécurité MBR.

Dans l'utilitaire Computer Setup, vous devez :

- Enregistrer le MBR du disque amorçable actuel, ou
- Désactiver la fonction de sécurité MBR.

Vous devez connaître le mot de passe de configuration, s'il a été défini.

## Avant de partitionner ou de formater le disque amorçable actuel

Assurez-vous que la sécurité MBR est désactivée avant de modifier le partitionnement ou le formatage du disque amorçable actuel. Divers utilitaires de disque comme FDISK et FORMAT tentent de mettre à jour le MBR. Si la sécurité MBR est activée lorsque vous modifiez le partitionnement ou le formatage du disque, il se peut que vous receviez des messages d'erreur de l'utilitaire de disque ou un avertissement de la sécurité MBR lors de la prochaine mise sous tension de l'ordinateur ou de son redémarrage. Pour désactiver la sécurité MBR, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter > Redémarrer l'ordinateur**.
2. Appuyez sur la touche **F10** dès que le voyant du moniteur devient vert. Appuyez sur **Entrée** pour passer l'écran de titre, si vous le souhaitez.



Si vous n'appuyez pas à temps sur la touche **F10**, vous devrez éteindre l'ordinateur, puis le remettre sous tension et appuyer de nouveau sur la touche **F10** pour accéder à l'utilitaire.

---

3. Sélectionnez **Security (Sécurité) > Master Boot Record Security (Sécurité MBR) > Disabled (Désactivée)**.
4. Avant de quitter, cliquez sur **File > Save Changes and Exit (Fichier > Enregistrer les modifications et Quitter)**.

## Dispositif antivol

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

Vous trouverez une procédure illustrée, dans le *Manuel de référence du matériel* disponible sur le CD *Documentation Library*.

## 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 seules sociétés de pointe disposant d'un système de sécurité très élaboré.



---

La prise en charge de la technologie de reconnaissance des empreintes digitales varie en fonction des modèles.

---

Pour plus d'informations, consultez le site

<http://h18000.www1.hp.com/solutions/security>.

## Notification des pannes et récupération

Les fonctions de notification des pannes et de récupération allient une technologie matérielle et logicielle novatrice qui évite la perte des données essentielles et réduit les temps d'inactivité imprévus.

Lorsqu'une panne survient, l'ordinateur affiche un message d'alerte locale, contenant la description de la panne et la marche à suivre pour y remédier. Vous pouvez ensuite visualiser l'état actuel du système à l'aide de l'utilitaire HP Client Manager. Si l'ordinateur est relié à un réseau supervisé par HP Insight Manager, HP Client Manager ou par d'autres applications de supervision, il envoie également une notification de panne à l'application de supervision du réseau.

## 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 HP. 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 mainteneur peut ensuite utiliser ces informations pour le diagnostic des pannes qui vous ont conduit à exécuter le logiciel DPS. Reportez-vous au *Manuel de résolution des problèmes* pour la procédure d'utilisation du système 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 imprévue. Cette alimentation peut supporter une surtension de 2000 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'alerte en cas de dépassement des limites de température normale, ce qui permet de prendre des mesures avant que les composants internes ne soient endommagés ou que des données ne soient perdues.



---

# Index

## A

accès aux ordinateurs, contrôle 21  
activation du verrou Smart Cover 46  
ActiveUpdate 7  
Adresses Internet, voir Sites Web  
alimentation avec protection contre les  
  surtensions 52  
Altiris 4  
Altiris PC Transplant Pro 6  
annulation d'un mot de passe 31  
avertissement 7  
avertissements  
  protection de la ROM 7

## B

Bloc d'amorçage ROM Failsafe 9  
bouton d'alimentation  
  configuration 19  
  double état 19  
bouton d'alimentation à deux états 19

## C

capteur de température interne 52  
Capteur Smart Cover  
  configuration 45  
  niveaux de protection 45  
caractères de séparation nationaux 31  
caractères de séparation, clavier, national 31  
caractères de séparation, tableau 31  
changement de mot de passe 29

changement de système d'exploitation,  
  informations importantes 20  
clé FailSafe  
  commande 47  
  précautions 47  
clonage de disque 2  
commande de la clé FailSafe 47  
Computer Setup, utilitaires 10  
configuration  
  initiale 2  
  réplication 10  
  saisie du mot de passe 28  
configuration du bouton d'alimentation 19  
contrôle d'accès aux ordinateurs 21

## D

démarrage  
  entrée du mot de passe 28  
désactivation du verrou Smart Cover 47  
DiskOnKey  
  *voir aussi* HP Drive Key  
  amorçable 14 à 19  
dispositif antivol 51  
disque amorçable, informations importantes  
  50  
disque dur, protection 52  
disques durs, outils de diagnostic 52  
Drivelock 42 à 44

## F

formatage du disque, informations  
  importantes 50

## H

HP Client Manager 4

HP Drive Key

*voir aussi* DiskOnKey

amorçable 14 à 19

## I

image logicielle préinstallée 2

informations importantes 50

initiale, configuration 2

installation à distance 3

installation de système à distance, accès à l' 3

## L

logiciel

Bloc d'amorçage ROM Failsafe 9

Computer Setup 10

installation de système à distance 3

intégration 2

mise à jour de plusieurs machines 6

notification des pannes et récupération 51

réécriture de la ROM à distance 8

sécurité MBR 48 à 50

suivi d'inventaire 21

System Software Manager 6

système de protection d'unité 52

logiciel de personnalisation 2

logiciels, récupération 2

## M

mise à jour de la ROM 7

modifications, notification préventive 6

mot de passe

changement 29

configuration 26

ProtectTools 33 à 37

sécurité 26

suppression 30

mot de passe de configuration 28

changement 29

définition 26

ProtectTools 33

suppression 30

mot de passe de démarrage 28

changement 29

suppression 30

mot de passe, annulation 31

Multibay, sécurité 42 à 44

## N

non valide, ROM 9

notification des modifications 6

notification des pannes 51

Notification préventive des modifications 6

## O

outils de clonage, logiciel 2

outils de déploiement, logiciel 2

outils de diagnostic pour disque dur 52

## P

partitionnement du disque

informations importantes 50

périphérique USB à mémoire flash,

amorçable 14 à 19

Preboot Execution Environment (PXE) 3

précautions

clé FailSafe 47

sécurité de verrouillage du capot 46

protection contre les surtensions,

alimentation 52

ProtectTools, sécurité intégrée 32 à 42

PXE (Preboot Execution Environment) 3

## R

reconnaissance des empreintes digitales 51

récupération, logiciels 2

restauration de secours, ProtectTools 37, 42

restauration des données chiffrées 42

restauration des données codées 37

restauration du système 8

**ROM**

- mise à jour 7
- réécriture de la ROM à distance 8

ROM système non valide 9

ROM, tableau des voyants du clavier 10

**S**

saisie du mot de passe de configuration 28

saisie du mot de passe de démarrage 28

sécurité

- capteur Smart Cover 45

- DriveLock 42 à 44

- fonctions, tableau 22

- MBR 48 à 50

- mot de passe 26

- MultiBay 42 à 44

- paramètres, configuration 21

- ProtectTools 32 à 42

- verrou Smart Cover 46, 47

sécurité de verrouillage du capot,  
précautions 46

sécurité intégrée de ProtectTools 32 à 42

Sécurité intégrée ProtectTools

- mots de passe

  - clé de restauration de secours 34

  - configuration 33

  - prise de possession 34

  - utilisateur 36

sécurité intégrée ProtectTools

- restauration de secours 37, 42

sécurité MBR 48 à 50

Sires Web

- réécriture de la ROM à distance 8

Sites Web

- ActiveUpdate 7

- Altiris 5

- Altiris PC Transplant Pro 6

- empreintes digitales, technologie de  
reconnaissance 51

HP Client Manager 4

HPQFlash 8

images ROMPaq 7

Notification préventive de modification 6

réplication de la configuration 13

support logiciel 20

System Software Manager (SSM) 6

technologie de reconnaissance des  
empreintes digitales 51

sites Web

- déploiement de PC 2

- Réécriture de la ROM 7

Smart Cover, capteur 45

Smart Cover, commande de la clé FailSafe 47

Smart Cover, verrou 46, 47

SSM (System Software Manager) 6

suivi d'inventaire 21

support amorçable

- création 13 à 19

- DiskOnKey 14 à 19

- disquette 13

- HP Drive Key 14 à 19

- périphérique USB à mémoire flash 14 à 19

suppression du mot de passe 30

System Software Manager (SSM) 6

système d'exploitation, informations  
importantes 20

système, restauration 8

**T**

température interne de l'ordinateur 52

**U**

URL (sites Web). Voir Sites Web

**V**

verrou Smart Cover

- activation 46

- désactivation 47

voyants du clavier, ROM, tableau 10