# ProtectTools
## Manuel de l’utilisateur

© Copyright 2007 Hewlett-Packard Development Company, L.P.

Microsoft et Windows sont des marques déposées de Microsoft Corporation aux États-Unis. Intel est une marque commerciale ou une marque déposée d'Intel Corporation ou de ses filiales aux États-Unis et dans d'autres pays/régions. AMD, le logo AMD Arrow et les combinaisons de ceux-ci sont des marques commerciales d'Advanced Micro Devices, Inc. Bluetooth est une marque détenue par son propriétaire et utilisée sous licence par Hewlett-Packard Company. Java est une marque déposée aux États-Unis de Sun Microsystems, Inc. SD Logo est une marque détenue par son propriétaire.

Les informations de ce document sont susceptibles d'être modifiées sans préavis. Les garanties applicables aux produits et services HP sont énoncées dans les textes de garantie accompagnant ces produits et services. Aucune partie du présent document ne saurait être interprétée comme constituant un quelconque supplément de garantie. HP ne peut être tenu responsable des erreurs ou omissions techniques ou de rédaction de ce document.

Première édition : juillet 2007

Référence du document : 451271-051

# Sommaire

# 1 Introduction à la sécurité

Le logiciel HP ProtectTools Security Manager fournit des fonctions de sécurité conçues pour empêcher tout accès non autorisé à l'ordinateur, aux réseaux et aux données critiques. Des fonctionnalités évoluées de sécurité sont proposées dans les modules logiciels suivants :

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools

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

Les modules logiciels HP ProtectTools peuvent être préinstallés, préchargés ou téléchargés sur le site Web HP. Pour plus d'informations, consultez le site http://www.hp.com.

**REMARQUE :** Les instructions contenues dans ce manuel supposent que vous avez déjà installé les modules logiciels HP ProtectTools applicables.

# Fonctions HP ProtectTools

Le tableau ci-dessous détaille les principales fonctions des modules HP ProtectTools :

| Module | Principales fonctions |
|---|---|
| Credential Manager for HP ProtectTools | • Credential Manager fournit un choix de fonctions de sécurité et d'identification.<br>• La fonction d'authentification unique mémorise plusieurs mots de passe nécessaires pour accéder à des sites Web, à des applications et à des ressources réseau protégés.<br>• L'authentification unique permet une protection supplémentaire en imposant diverses combinaisons de technologies de sécurité et d'identification des utilisateurs, parmi lesquelles les technologies Java™ Card et de lecture biométrique.<br>• Le stockage du mot de passe est protégé par cryptage et peut bénéficier d'une protection accrue à l'aide d'une puce de sécurité intégrée TPM et/ou d'une authentification via un périphérique de sécurité (Java™ Card ou lecteur biométrique). |
| Embedded Security for HP ProtectTools | • Embedded Security utilise une puce de sécurité intégrée Trusted Platform Module (TPM) empêchant tout accès non autorisé aux données utilisateur confidentielles ou aux informations d'authentification stockées sur un PC.<br>• Embedded Security permet la création d'un lecteur sécurisé personnel (PSD) pour la protection des données utilisateur.<br>• Embedded Security prend en charge des applications d'autres sociétés (telles que Microsoft® Outlook et Internet Explorer) pour les opérations protégées impliquant l'utilisation de certificats numériques. |
| Java Card Security for HP ProtectTools | • Le module Java Card Security configure la Java Card HP ProtectTools pour l'authentification de l'utilisateur avant le chargement du système d'exploitation.<br>• Java Card Security configure des Java Cards distinctes pour l'administrateur et l'utilisateur. |
| BIOS Configuration for HP ProtectTools | • BIOS Configuration fournit un accès à la gestion des mots de passe administrateur et des mots de passe de mise sous tension utilisateur.<br>• Le module BIOS Configuration est une alternative à l'utilitaire de configuration du BIOS avant le démarrage connu sous le nom de F10 Setup.<br>• DriveLock permet de protéger un disque dur des accès non autorisés, même s'il est retiré d'un système, sans que l'utilisateur ait besoin de retenir des mots de passe supplémentaires. |
| Drive Encryption for HP ProtectTools | • Drive Encryption permet un cryptage de disque dur complet au niveau du volume.<br>• Drive Encryption impose une authentification au préamorçage afin de décrypter les données et d'y accéder. |

# Accès à HP ProtectTools Security

Pour accéder à HP ProtectTools Security via le Panneau de configuration Windows® :

- Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.

**REMARQUE :** Une fois que vous avez configuré le module Credential Manager, vous pouvez également ouvrir HP ProtectTools en vous connectant à Credential Manager directement à partir de l'écran de connexion Windows. Pour plus d'informations, reportez-vous à la section «Connexion à Windows via Credential Manager page 17».

# Objectifs de sécurité fondamentaux

La combinaison des modules HP ProtectTools fournit des solutions à de nombreux problèmes de sécurité et répond aux objectifs de sécurité fondamentaux suivants :

- Protection contre le vol ciblé
- Restriction de l'accès à des données confidentielles
- Protection contre des accès non autorisés depuis des sites internes ou externes
- Création de stratégies de mot de passe fort

## Protection contre le vol ciblé

Ce type d'incident pourrait par exemple être illustré par le vol ciblé d'un ordinateur contenant des données confidentielles et des informations clients dans un espace de travail ouvert. Les fonctionnalités suivantes permettent de mieux vous protéger contre ce type de vol :

- L'authentification au préamorçage, lorsqu'elle est activée, empêche tout accès au système d'exploitation. Voir les procédures suivantes :
  - «Activation et désactivation de la prise en charge de l'authentification de la Smart Card à la mise sous tension page 46»
  - «Activation et désactivation de la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée page 47»
  - «Attribution d'un nom à une Java Card page 39»
  - «Drive Encryption for HP ProtectTools page 52»
- DriveLock permet de s'assurer que les données ne sont pas accessibles même si le disque dur est enlevé pour être installé sur un système non sécurisé. Reportez-vous à la section «Activation et désactivation de la protection de disque dur DriveLock page 48».
- Le lecteur sécurisé personnel (PSD, Personal Secure Drive) fourni avec le module Embedded Security for HP ProtectTools assure le cryptage des données confidentielles pour empêcher tout accès sans authentification. Voir les procédures suivantes :
  - Embedded Security «Procédures de configuration page 28»
  - «Utilisation du lecteur sécurisé personnel page 31»

## Restriction de l'accès à des données confidentielles

Imaginons qu'un responsable d'audit externe travaillant sur site puisse accéder aux ordinateurs afin d'examiner des données financières importantes. Vous ne souhaitez pas que ce responsable d'audit puisse imprimer des fichiers ou les enregistrer sur un support tel qu'un CD. Les fonctionnalités suivantes permettent de limiter l'accès aux données :

- DriveLock permet de s'assurer que les données ne sont pas accessibles même si le disque dur est enlevé pour être installé sur un système non sécurisé. Reportez-vous à la section «Activation et désactivation de la protection de disque dur DriveLock page 48».

## Protection contre des accès non autorisés depuis des sites internes ou externes

Si des utilisateurs non autorisés accèdent depuis un site interne ou externe à un PC contenant des données confidentielles et des informations client, ils peuvent avoir accès aux ressources réseau de l'entreprise, au travail d'un dirigeant ou de l'équipe de Recherche et Développement, ou encore à des

données privées telles que des enregistrements concernant des malades ou des informations financières. Les fonctionnalités suivantes empêchent un accès non autorisé :

- L'authentification au préamorçage, lorsqu'elle est activée, empêche tout accès au système d'exploitation. Voir les procédures suivantes :
  - «Activation et désactivation de la prise en charge de l'authentification de la Smart Card à la mise sous tension page 46»
  - «Activation et désactivation de la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée page 47»
  - «Attribution d'un nom à une Java Card page 39»
  - «Drive Encryption for HP ProtectTools page 52»
- Embedded Security for HP ProtectTools utilise les procédures suivantes pour protéger les données utilisateur confidentielles ou les informations d'authentification stockées sur un PC :
  - Embedded Security «Procédures de configuration page 28»
  - «Utilisation du lecteur sécurisé personnel page 31»
- À l'aide des procédures suivantes, Credential Manager for HP ProtectTools empêche les utilisateurs non autorisés de se procurer des mots de passe ou d'accéder à des applications protégées par mot de passe :
  - Credential Manager «Procédures de configuration page 12»
  - «Utilisation de la fonction d'authentification unique page 18»
- Le lecteur sécurisé personnel (PSD, Personal Secure Drive) crypte les données confidentielles pour qu'elles ne soient pas accessibles sans authentification ; dans ce but, les procédures suivantes sont mises en œuvre :
  - Embedded Security «Procédures de configuration page 28»
  - «Utilisation du lecteur sécurisé personnel page 31»

## Création de stratégies de mot de passe fort

Si, dans un contexte spécifique, l'emploi d'une stratégie de mot de passe fort pour des dizaines d'applications et de base de données Web est rendu obligatoire, Credential Manager for HP ProtectTools fournit un référentiel protégé pour les mots de passe et un outil d'authentification unique grâce à l'application des procédures suivantes :

- Credential Manager «Procédures de configuration page 12»
- «Utilisation de la fonction d'authentification unique page 18»

De plus, pour une meilleure sécurité, Embedded Security for HP ProtectTools protège ce référentiel dans lequel sont regroupés des noms d'utilisateur et des mots de passe. Les utilisateurs peuvent ainsi avoir plusieurs mots de passe forts sans avoir à les écrire pour les mémoriser. Voir Embedded Security «Procédures de configuration page 28»

# Éléments de sécurité supplémentaires

## Attribution des rôles de sécurité

Dans la gestion de la sécurité informatique (particulièrement dans le cas d'organisations de grande taille), une pratique importante consiste à répartir les responsabilités et les droits parmi divers types d'administrateurs et d'utilisateurs.

**REMARQUE :** Dans une petite organisation ou pour une utilisation individuelle, ces rôles peuvent être tenus par la même personne.

Dans le cas de HP ProtectTools, les responsabilités et les privilèges de sécurité peuvent être répartis suivant les rôles ci-dessous :

- Responsable de la sécurité : Définit le niveau de sécurité de l'entreprise ou du réseau et détermine les fonctions de sécurité à déployer, telles que les Java™ Cards, les lecteurs biométriques ou les jetons USB.

  **REMARQUE :** Un grand nombre des fonctions HP ProtectTools peuvent être personnalisées par le responsable de la sécurité en coopération avec HP. Consultez le site Web HP (http://www.hp.com) pour plus d'informations.

- Administrateur informatique : Applique et gère les fonctions de sécurité définies par le responsable de la sécurité. Il peut également activer et désactiver certaines fonctions. Par exemple, si le responsable de la sécurité a décidé de déployer des Java Cards, l'administrateur informatique peut activer le mode de sécurité BIOS de la Java Card.

- Utilisateur : Utilise les fonctions de sécurité. Par exemple, si le responsable de la sécurité et l'administrateur informatique ont activé des Java Cards pour le système, l'utilisateur peut définir le code PIN de la Java Card et utiliser la carte à des fins d'authentification.

## Gestion de mots de passe HP ProtectTools

La plupart des fonctions du logiciel HP ProtectTools Security Manager sont protégées par des mots de passe. Le tableau suivant répertorie les mots de passe couramment utilisés, le module logiciel dans lequel le mot de passe est défini, ainsi que la fonction du mot de passe.

Les mots de passe qui sont uniquement définis et utilisés par les administrateurs informatiques sont également indiqués dans ce tableau. Tous les autres mots de passe peuvent être définis par des utilisateurs ou administrateurs ordinaires.

| Mot de passe HP ProtectTools | Défini dans ce module HP ProtectTools | Fonction |
|---|---|---|
| Mot de passe de connexion à Credential Manager | Credential Manager | Ce mot de passe propose 2 options :<br>• Il peut être utilisé en tant que connexion distincte pour accéder à Credential Manager après une connexion à Windows.<br>• Il peut être utilisé à la place du processus de connexion à Windows, en offrant un accès simultané à Windows et Credential Manager. |
| Mot de passe du fichier de restauration Credential Manager | Credential Manager, par l'administrateur informatique | Protège l'accès au fichier de restauration Credential Manager. |
| Mot de passe de clé utilisateur de base | Sécurité intégrée | Utilisé pour accéder aux fonctions Sécurité intégrée, telles que le cryptage du courrier électronique, des fichiers et des dossiers. Lorsqu'il est utilisé pour l'authentification à |

| Mot de passe HP ProtectTools | Défini dans ce module HP ProtectTools | Fonction |
|---|---|---|
| **REMARQUE :** Également appelé mot de passe de sécurité intégrée | | la mise sous tension, protège également l'accès au contenu de l'ordinateur à la mise sous tension, au redémarrage ou lorsque vous quittez le mode Veille prolongée. |
| Mot de passe de jeton de restauration d'urgence<br><br>**REMARQUE :** Également appelé mot de passe de clé de jeton de restauration d'urgence | Sécurité intégrée, par l'administrateur informatique | Protège l'accès au jeton de restauration d'urgence, qui est un fichier de sauvegarde pour la puce de sécurité intégrée. |
| Mot de passe propriétaire | Sécurité intégrée, par l'administrateur informatique | Protège le système et la puce TPM contre l'accès non autorisé à toutes les fonctions propriétaire de la sécurité intégrée. |
| Code PIN de Java™ Card | Java Card Security | Protège l'accès au contenu de la Java Card et authentifie les utilisateurs de celle-ci. Lorsqu'il est utilisé pour l'authentification à la mise sous tension, le code PIN de Java Card protège également l'accès à l'utilitaire Computer Setup et au contenu de l'ordinateur.<br><br>Authentifie les utilisateurs de Drive Encryption en cas de sélection du jeton Java Card. |
| Mot de passe Computer Setup<br><br>**REMARQUE :** Également connu en tant que mot de passe administrateur BIOS, Configuration F10 ou configuration de sécurité | BIOS Configuration, par l'administrateur informatique | Protège l'accès à l'utilitaire Computer Setup. |
| Mot de passe de mise sous tension | BIOS Configuration | Sécurise l'accès au contenu de l'ordinateur à la mise sous tension, au redémarrage ou lorsque vous quittez le mode Veille ou Veille prolongée. |
| Mot de passe de connexion Windows | Panneau de configuration Windows | Peut être utilisé dans une connexion manuelle ou enregistré sur la Java Card. |

### Création d’un mot de passe sécurisé

Lorsque vous créez des mots de passe, vous devez d’abord suivre toutes les instructions définies par le programme. Toutefois, vous devez généralement prendre en compte les points suivants afin de pouvoir créer des mots de passe forts et réduire les risques de corruption de votre mot de passe :

- Utilisez des mots de passe contenant plus de 6 caractères et préférablement plus de 8.
- Utilisez des majuscules et des minuscules dans l’ensemble du mot de passe.
- Chaque fois que cela est possible, mélangez les caractères alphanumériques et incluez des caractères spéciaux et des signes de ponctuation.
- Remplacez les lettres d’un mot clé par des nombres ou caractères spéciaux. Par exemple, vous pouvez utiliser le chiffre 1 pour la lettre I ou L.
- Associez des mots de 2 langues ou plus.
- Divisez un mot ou une phrase par des nombres ou des caractères spéciaux au milieu. Par exemple, "Mary2-2Cat45".
- N’utilisez pas un mot de passe figurant dans un dictionnaire.
- N’utilisez pas votre nom comme mot de passe, ou toute autre information personnelle, telle qu’une date de naissance, le nom de votre chien ou le nom de jeune fille de votre mère, même en l’épelant à l’envers.
- Modifiez les mots de passe régulièrement. Vous pouvez souhaiter ne modifier que quelques caractères par incrément.
- Si vous notez votre mot de passe, ne le placez pas en un lieu visible, à proximité de l’ordinateur.
- N’enregistrez pas le mot de passe dans un fichier, tel qu’un message électronique, sur l’ordinateur.
- Ne partagez pas de comptes et ne communiquez votre mot de passe à personne.

## HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore constitue un moyen rapide et facile pour sauvegarder et restaurer des informations d’authentification de sécurité provenant de tous les modules HP ProtectTools pris en charge.

### Sauvegarde des informations d’authentification et des paramètres

Vous pouvez sauvegarder les informations d’authentification de l’une des manières suivantes :

- Utilisation de l’assistant de sauvegarde HP ProtectTools pour sélectionner et sauvegarder les modules HP ProtectTools
- Sauvegarde des modules HP ProtectTools présélectionnés

**REMARQUE :** Si vous choisissez cette méthode, vous devez au préalable définir des options de sauvegarde.

- Planification de sauvegardes

**REMARQUE :** Si vous choisissez cette méthode, vous devez au préalable définir des options de sauvegarde.

**Utilisation de l'assistant de sauvegarde HP ProtectTools pour sélectionner et sauvegarder les modules HP ProtectTools**

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Sauvegarder et restaurer**.
3. Dans le volet droit, cliquez sur **Backup Options** (Options de sauvegarde). La fenêtre de l'assistant de sauvegarde HP ProtectTools s'affiche. Suivez les instructions à l'écran pour sauvegarder les informations d'authentification.

**Définition des options de sauvegarde**

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Sauvegarder et restaurer**.
3. Dans le volet droit, cliquez sur **Backup Options** (Options de sauvegarde). La fenêtre de l'assistant de sauvegarde HP ProtectTools s'affiche.
4. Suivez les instructions à l'écran.
5. Après avoir défini et confirmé le **Storage File Password** (Mot de passe du fichier de stockage), sélectionnez **Remember all passwords and authentication values for future automated backups** (Mémoriser tous les mots de passe et valeurs d'authentification pour les futures sauvegardes automatiques).
6. Cliquez sur **Enregistrer les paramètres**, puis sur **Terminer**.

**Sauvegarde des modules HP ProtectTools présélectionnés**

**REMARQUE :** Si vous choisissez cette méthode, vous devez au préalable définir des options de sauvegarde.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Sauvegarder et restaurer**.
3. Dans le volet droit, cliquez sur **Sauvegarde**.

**Planification de sauvegardes**

**REMARQUE :** Si vous choisissez cette méthode, vous devez au préalable définir des options de sauvegarde.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Sauvegarder et restaurer**.
3. Dans le volet droit, cliquez sur l'onglet **Planifier vos sauvegardes**.
4. Dans l'onglet **Tâche**, cochez la case **Activé** pour activer les sauvegardes planifiées.
5. Cliquez sur **Set Password** (Définir le mot de passe), puis tapez et confirmez votre mot de passe dans la boîte de dialogue **Set Password** (Définir le mot de passe). Cliquez sur **OK**.
6. Cliquez sur **Appliquer**. Cliquez sur l'onglet **Planifier**. Cliquez sur la flèche **Tâche planifiée** et sélectionnez la fréquence de sauvegarde automatique.
7. Sous **Heure de début**, utilisez les flèches **Heure de début** pour sélectionner l'heure de début de la sauvegarde.
8. Cliquez sur **Avancé** pour sélectionner une date de début, une date de fin et des paramètres de tâches récurrentes. Cliquez sur **Appliquer**.

9. Cliquez sur **Paramètres** et sélectionnez les paramètres pour **Fin de l'exécution de la tâche planifiée**, **Durée d'inactivité** et **Gestion de l'alimentation**.

10. Cliquez sur **Appliquer**, puis sur **OK** pour fermer la boíte de dialogue.

## Restauration d'informations d'authentification

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.

2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Sauvegarder et restaurer**.

3. Dans le volet droit, cliquez sur **Restaurer**. La fenêtre de l'assistant de restauration HP ProtectTools s'affiche. Suivez les instructions à l'écran.

## Configuration des paramètres

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.

2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Paramètres**.

3. Dans le volet droit, sélectionnez les paramètres, puis cliquez sur **OK**.

# 2 Credential Manager for HP ProtectTools

Le module Credential Manager for HP ProtectTools propose les fonctions de sécurité suivantes pour protéger votre ordinateur contre tout accès non autorisé :

- Solutions similaires à la saisie de mots de passe pour ouvrir une session Windows, telle que l'utilisation d'une Java Card ou d'un lecteur biométrique. Pour plus d'informations, reportez-vous à la section «Enregistrement d'informations d'authentification page 13».
- Fonction d'authentification unique qui mémorise automatiquement les informations d'authentification des sites Web, des applications et des ressources réseau protégées.
- Prise en charge de dispositifs de sécurité en option, tels que les Java Cards et les lecteurs biométriques.
- Prise en charge de paramètres de sécurité supplémentaires, tels que la demande d'authentification avec un périphérique de sécurité en option pour déverrouiller l'ordinateur.

# Procédures de configuration

## Connexion au module Credential Manager

En fonction de la configuration, vous pouvez vous connecter à Credential Manager de l'une des manières suivantes :

- Assistant de connexion de Credential Manager (recommandé)
- Icône HP ProtectTools Security Manager dans la zone de notification
- HP ProtectTools Security Manager

**REMARQUE :** Si vous utilisez l'invite de connexion à Credential Manager dans l'écran de connexion Windows pour vous connecter à Credential Manager, vous vous connectez à Windows au même moment.

La première fois que vous ouvrez Credential Manager, connectez-vous à l'aide de votre mot de passe de connexion Windows habituel. Un compte Credential Manager est ensuite automatiquement créé avec vos informations d'authentification de connexion Windows.

Une fois connecté à Credential Manager, vous pouvez enregistrer des informations d'authentification supplémentaires, telles qu'une empreinte digitale ou une Java Card. Pour plus d'informations, reportez-vous à la section «Enregistrement d'informations d'authentification page 13».

À la prochaine connexion, vous pouvez sélectionner la stratégie de connexion et utiliser toute combinaison des informations d'authentification enregistrées.

### Utilisation de l'Assistant de connexion de Credential Manager

Pour vous connecter à Credential Manager à l'aide de l'Assistant de connexion de Credential Manager, procédez comme suit :

1. Ouvrez l'Assistant de connexion de Credential Manager de l'une des manières suivantes :
   - À partir de l'écran de connexion Windows
   - À partir de la zone de notification, en double-cliquant sur l'icône **HP ProtectTools Security Manager**
   - À partir de la page Credential Manager de ProtectTools Security Manager, en cliquant sur le lien **Connexion** dans l'angle supérieur droit de la fenêtre
2. Suivez les instructions à l'écran pour vous connecter à Credential Manager.

### Connexion pour la première fois

Avant de commencer, vous devez être connecté à Windows avec un compte administrateur, sans vous connecter à Credential Manager.

1. Ouvrez HP ProtectTools Security Manager en double-cliquant sur l'icône HP ProtectTools Security Manager dans la zone de notification. La fenêtre HP ProtectTools Security Manager s'affiche.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Connexion** dans l'angle supérieur droit du volet droit. L'Assistant de connexion de Credential Manager s'affiche.
3. Entrez votre mot de passe Windows dans le champ **Mot de passe**, puis cliquez sur **Suivant**.

## Enregistrement d'informations d'authentification

Vous pouvez utiliser la page "Mon identité" pour enregistrer vos diverses méthodes ou informations d'authentification. Une fois ces méthodes enregistrées, vous pouvez les utiliser pour vous connecter à Credential Manager.

### Enregistrement d'empreintes digitales

Un lecteur d'empreintes digitales vous permet de vous connecter à Windows en utilisant votre empreinte pour authentification au lieu d'employer un mot de passe Windows.

### Configuration du lecteur d'empreintes digitales

1. Une fois connecté à Credential Manager, passez votre doigt sur le lecteur d'empreintes. L'Assistant d'enregistrement de Credential Manager s'affiche.
2. Suivez les instructions à l'écran pour enregistrer vos empreintes digitales et configurer le lecteur d'empreintes.
3. Pour configurer le lecteur d'empreintes digitales pour un autre utilisateur Windows, ouvrez une session Windows sous cet utilisateur, puis répétez les étapes 1 et 2.

### Utilisation de votre empreinte digitale enregistrée pour ouvrir une session Windows

1. Dès que vous avez fini d'enregistrer vos empreintes digitales, redémarrez Windows.
2. Dans l'écran de bienvenue de Windows, passez un de vos doigts enregistrés pour vous connecter à Windows.

## Enregistrement d'une Java Card, d'un e-jeton USB ou d'un jeton virtuel

**REMARQUE :** Vous devez avoir configuré un lecteur de carte multimédia ou un clavier Smart Card pour cette procédure. Si vous choisissez de ne pas utiliser de carte à puce, vous pouvez enregistrer un jeton virtuel comme décrit à la section « Création d'un jeton virtuel page 15 ».

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Register Smart Card or Token** (Enregistrer une Smart Card ou un jeton). L'Assistant d'enregistrement de Credential Manager s'affiche.
4. Suivez les instructions à l'écran.

## Enregistrement d'un e-jeton USB

1. Assurez-vous que les pilotes de l'e-jeton USB sont installés.

   **REMARQUE :** Pour plus d'informations, reportez-vous au manuel de l'utilisateur de l'e-jeton USB.

2. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
3. Dans le volet gauche, cliquez sur **Credential Manager**.
4. Dans le volet droit, cliquez sur **Register Smart Card or Token** (Enregistrer une Smart Card ou un jeton). L'Assistant d'enregistrement de Credential Manager s'affiche.
5. Suivez les instructions à l'écran.

## Enregistrement d'autres informations d'authentification

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Enregistrer les informations d'authentification**. L'Assistant d'enregistrement de Credential Manager s'affiche.
4. Suivez les instructions à l'écran.

# Tâches générales

Tous les utilisateurs ont accès à la page "Mon identité" dans Credential Manager. La page "Mon identité" permet de réaliser les tâches suivantes :

- Création d'un jeton virtuel
- Modification du mot de passe de connexion Windows
- Gestion d'un PIN de jeton
- Gestion d'identité
- Verrouillage de l'ordinateur

**REMARQUE :** Cette option est uniquement disponible si l'invite de connexion classique de Credential Manager est activée. Reportez-vous à la section «Exemple 1 : Utilisation de la page Paramètres avancés pour autoriser une connexion à Windows à partir de Credential Manager page 25».

## Création d'un jeton virtuel

Le fonctionnement d'un jeton virtuel est très similaire à celui d'une Java Card ou d'un e-jeton USB. Le jeton est enregistré sur le disque dur de l'ordinateur ou dans le Registre Windows. Lorsque vous vous connectez à l'aide d'un jeton virtuel, vous êtes invité à fournir un code PIN d'utilisateur pour effectuer l'authentification.

Pour créer un jeton virtuel :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Virtual Token** (Jeton virtuel). L'Assistant d'enregistrement de Credential Manager s'affiche.

**REMARQUE :** Si **Virtual Token** (Jeton virtuel) n'est pas une option, utilisez la procédure de la section «Enregistrement d'autres informations d'authentification page 14».

4. Suivez les instructions à l'écran.

## Modification du mot de passe de connexion Windows

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Changement du mot de passe Windows**.
4. Entrez votre ancien mot de passe dans le champ **Ancien mot de passe**.
5. Entrez et confirmez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.
6. Cliquez sur **Terminer**.

## Modification du code PIN d'un jeton

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Change Token PIN** (Modifier le PIN de jeton).

4. Sélectionnez le jeton dont vous souhaitez modifier le code PIN, puis cliquez sur **Suivant**.
5. Suivez les instructions à l'écran pour compléter la modification du code PIN.

# Gestion d'identité

## Effacement d'une identité du système

**REMARQUE :** Cette action n'affecte pas votre compte utilisateur Windows.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Clear Identity for this Account** (Effacer l'identité pour ce compte).
4. Cliquez sur **Oui** dans la boîte de dialogue de confirmation. Votre identité est déconnectée et supprimée du système.

## Verrouillage de l’ordinateur

Cette fonction est disponible si vous vous connectez à Windows via Credential Manager. Pour protéger votre ordinateur lorsque vous quittez votre bureau, utilisez la fonction Verrouiller la station de travail. Ainsi, les utilisateurs non autorisés ne pourront pas accéder à votre ordinateur. Seuls vous et les membres du groupe d’administrateurs sur votre ordinateur peuvent le déverrouiller.

**REMARQUE :** Cette option est uniquement disponible si l’invite de connexion classique de Credential Manager est activée. Reportez-vous à la section «Exemple 1 : Utilisation de la page Paramètres avancés pour autoriser une connexion à Windows à partir de Credential Manager page 25».

Pour renforcer la sécurité, vous pouvez configurer la fonction Verrouiller la station de travail afin de demander une Java Card, un lecteur biométrique ou un jeton pour déverrouiller l’ordinateur. Pour plus d’informations, reportez-vous à la section «Configuration des paramètres de Credential Manager page 25».

Pour verrouiller l’ordinateur :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**.
3. Dans le volet droit, cliquez sur **Lock Workstation** (Verrouiller la station de travail). L’écran de connexion Windows s’affiche. Vous devez utiliser un mot de passe Windows ou l’Assistant de connexion de Credential Manager pour déverrouiller l’ordinateur.

## Utilisation de la connexion à Windows

Vous pouvez utiliser Credential Manager pour vous connecter à Windows, sur un ordinateur local ou sur un domaine de réseau. Lorsque vous vous connectez à Credential Manager pour la première fois, le système ajoute automatiquement votre compte utilisateur Windows local en tant que compte pour le service de connexion Windows.

### Connexion à Windows via Credential Manager

Vous pouvez utiliser Credential Manager pour vous connecter à un compte local ou réseau Windows.

1. Si vous avez enregistré votre empreinte pour vous connecter à Windows, passez votre doigt pour vous connecter.
2. Si vous n’avez pas enregistré d’empreinte pour vous connecter à Windows, cliquez sur l’icône de clavier dans l’angle supérieur gauche de l’écran en regard de l’icône d’empreinte. L’Assistant de connexion de Credential Manager s’affiche.
3. Cliquez sur la flèche **Nom d’utilisateur** et cliquez sur votre nom.
4. Entrez votre mot de passe dans le champ **Mot de passe**, puis cliquez sur **Suivant**.
5. Sélectionnez **More > Wizard Options** (Plus d'options d'assistant).
   a. Si vous souhaitez que ce nom soit le nom d’utilisateur par défaut la prochaine fois que vous vous connectez à l’ordinateur, cochez la case **Use last user name on next logon** (Utiliser le dernier nom d’utilisateur à la prochaine connexion).
   b. Si vous souhaitez que cette stratégie de connexion soit la méthode par défaut, cochez la case **Use last policy on next logon** (Utiliser la dernière stratégie à la prochaine connexion).
6. Suivez les instructions à l’écran. Si vos informations d’authentification sont correctes, vous êtes connecté à votre compte Windows et à Credential Manager.

### Ajout d’un compte

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, cliquez sur **Windows Logon** (Connexion Windows), puis sur **Add a Network Account** (Ajouter un compte réseau). L’assistant d’ajout de compte réseau s’affiche.
4. Suivez les instructions à l’écran.

### Suppression d’un compte

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, cliquez sur **Windows Logon** (Connexion Windows), puis sur **Manage Network Accounts** (Gestion des comptes réseau). La boîte de dialogue **Manage Network Accounts** (Gestion des comptes réseau) s’affiche.
4. Cliquez sur le compte à supprimer, puis sur **Supprimer**.
5. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
6. Cliquez sur **OK**.

## Utilisation de la fonction d’authentification unique

Credential Manager comporte une fonction d’authentification unique qui stocke des noms d’utilisateur et mots de passe pour plusieurs applications Internet et Windows et qui saisit automatiquement des informations de connexion lorsque vous accédez à une application enregistrée.

**REMARQUE :** La sécurité et la confidentialité sont des caractéristiques importantes de la fonction d’authentification unique. Toutes les informations d’authentification sont cryptées et sont uniquement disponibles après une connexion réussie à Credential Manager.

**REMARQUE :** Vous pouvez également configurer la fonction Authentification unique pour valider vos informations d’authentification à l’aide d’une Java Card, d’un lecteur biométrique ou d’un jeton, avant de vous connecter à une application ou à un site sécurisé. Cette fonctionnalité est particulièrement utile lors de la connexion à des applications ou à des sites Web qui contiennent des informations personnelles, telles que des numéros de compte bancaire. Pour plus d’informations, reportez-vous à la section «Configuration des paramètres de Credential Manager page 25».

### Enregistrement d’une nouvelle application

Credential Manager vous invite à enregistrer toutes les applications que vous démarrez lorsque vous êtes connecté à ce dernier. Vous pouvez également enregistrer une application manuellement.

#### Utilisation de l’enregistrement automatique

1. Ouvrez une application qui requiert une connexion.
2. Cliquez sur l’icône d’authentification unique de Credential Manager dans la boîte de dialogue du mot de passe de l’application ou du site Web.
3. Tapez votre mot de passe pour l’application ou le site, puis cliquez sur **OK**. La boîte de dialogue **Credential Manager Single Sign On** (Authentification unique de Credential Manager) s’affiche.

4. Cliquez sur **More** (Autres) et effectuez une sélection parmi les options suivantes :

   - Do not use SSO for this site or application (Ne pas utiliser l'authentification unique pour ce site ou cette application)
   - Prompt to select account for this application (Inviter à sélectionner un compte pour cette application)
   - Fill in credentials but do not submit (Renseigner les informations d'authentification mais ne pas soumettre)
   - Authenticate user before submitting credentials (Authentifier l'utilisateur avant de soumettre les informations d'authentification)
   - Show SSO shortcut for this application (Afficher le raccourci d'authentification unique pour cette application)

5. Cliquez sur **Oui** pour terminer l'enregistrement.

### Utilisation de l'enregistrement manuel (glisser-déposer)

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, cliquez sur **Authentification unique**, puis sur **Enregistrer une nouvelle application**. L'assistant d'application à authentification unique s'affiche.
4. Suivez les instructions à l'écran.

## Gestion d'applications et d'informations d'authentification

### Modification de propriétés d'application

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Authentification unique**, cliquez sur **Gérer les applications et les informations d'authentification**.
4. Cliquez sur l'entrée de l'application à modifier, puis sur **Propriétés**.
5. Cliquez sur l'onglet **Général** pour modifier le nom de l'application et sa description. Modifiez les paramètres en activant ou en décochant les cases en regard des paramètres appropriés.
6. Cliquez sur l'onglet **Script** pour afficher et modifier le script d'application SSO.
7. Cliquez sur **OK**.

### Suppression d'une application de la fonction d'authentification unique

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Authentification unique**, cliquez sur **Gérer les applications et les informations d'authentification**.
4. Cliquez sur l'entrée de l'application à supprimer, puis sur **Supprimer**.
5. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
6. Cliquez sur **OK**.

### Exportation d’une application

Vous pouvez exporter des applications afin de créer une copie de sauvegarde du script d’application SSO. Ce fichier peut ensuite être utilisé pour restaurer les données SSO. Ce fichier agit comme supplément au fichier de sauvegarde d’identité, qui contient uniquement les informations d’authentification.

Pour exporter une application :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Authentification unique**, cliquez sur **Gérer les applications et les informations d’authentification**.
4. Cliquez sur l'entrée d'application que vous souhaitez exporter. Cliquez ensuite sur **More > Applications > Export Script** (Script d'exportation d'autres applications).
5. Suivez les instructions à l’écran pour compléter l’exportation.
6. Cliquez sur **OK**.

### Importation d’une application

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Authentification unique**, cliquez sur **Gérer les applications et les informations d’authentification**.
4. Cliquez sur l'entrée d'application que vous souhaitez importer. Sélectionnez ensuite **More > Applications > Import Script** (Script d'importation d'autres applications).
5. Suivez les instructions à l’écran pour compléter l’importation.
6. Cliquez sur **OK**.

### Modification d’informations d’authentification

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Authentification unique**, cliquez sur **Gérer les applications et les informations d’authentification**.
4. Cliquez sur l’entrée de l’application à modifier, puis sur **Autres**.
5. Sélectionnez les options suivantes souhaitées :
   - Applications
     - Add New (Ajouter nouvelle)
     - Supprimer
     - Propriétés

- Import Script (Script d'importation)
- Export Script (Script d'exportation)

- Informations d'identification
  - Create New (Créer)
- View Password (Afficher le mot de passe)

**REMARQUE :** Vous devez authentifier votre identité avant de pouvoir modifier le mot de passe.

6. Suivez les instructions à l'écran.
7. Cliquez sur **OK**.

## Utilisation de la protection d'application

Cette fonction permet de configurer l'accès à des applications. Vous pouvez restreindre l'accès sur la base des critères suivants :

- Catégorie d'utilisateur
- Heure d'utilisation
- Inactivité d'utilisateur

### Restriction de l'accès à une application

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Protection d'application**, cliquez sur **Manage Protected Applications** (Gérer les applications protégées). La boîte de dialogue **Application Protection Service** (Service de protection d'application) s'affiche.
4. Sélectionnez une catégorie d'utilisateur à gérer.

**REMARQUE :** Si la catégorie n'est pas Everyone (Tout le monde), vous pouvez avoir à sélectionner **Override default settings** (Écraser les paramètres par défaut) pour écraser les paramètres de la catégorie Everyone.

5. Cliquez sur **Ajouter**. L'assistant d'ajout d'une application s'affiche.
6. Suivez les instructions à l'écran.

### Suppression de la protection d'une application

Pour supprimer des restrictions d'une application :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Protection d'application**, cliquez sur **Manage Protected Applications** (Gérer les applications protégées). La boîte de dialogue **Application Protection Service** (Service de protection d'application) s'affiche.
4. Sélectionnez une catégorie d'utilisateur à gérer.

**REMARQUE :** Si la catégorie n'est pas Everyone (Tout le monde), vous pouvez avoir à sélectionner **Override default settings** (Écraser les paramètres par défaut) pour écraser les paramètres de la catégorie Everyone.

5. Cliquez sur l'entrée de l'application à supprimer, puis sur **Supprimer**.
6. Cliquez sur **OK**.

## Modification des paramètres de restriction d'une application protégée

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Credential Manager**, puis sur **Services et applications**.
3. Dans le volet droit, sous **Protection d'application**, cliquez sur **Manage Protected Applications** (Gérer les applications protégées). La boîte de dialogue **Application Protection Service** (Service de protection d'application) s'affiche.
4. Sélectionnez une catégorie d'utilisateur à gérer.

**REMARQUE :** Si la catégorie n'est pas Everyone (Tout le monde), vous pouvez avoir à sélectionner **Override default settings** (Écraser les paramètres par défaut) pour écraser les paramètres de la catégorie Everyone.

5. Cliquez sur l'application à modifier, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** de cette application s'affiche.
6. Cliquez sur l'onglet **Général**. Sélectionnez un des paramètres suivants :
   - Disabled (Cannot be used) (Désactivée [Utilisation impossible])
   - Enabled (Can be used without restrictions) (Activée [Utilisable sans restrictions])
   - Restricted (Usage depends on settings) (Restreinte [Utilisation en fonction des paramètres])
7. Si vous sélectionnez une utilisation restreinte, les paramètres suivants sont disponibles :
   a. Si vous souhaitez restreindre l'utilisation sur la base de l'heure, du jour ou de la date, cliquez sur l'onglet **Planifier** et configurez les paramètres.
   b. Si vous souhaitez restreindre l'utilisation sur la base de l'inactivité, cliquez sur l'onglet **Advanced** (Avancé) et sélectionnez la période d'inactivité.
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de l'application.
9. Cliquez sur **OK**.

# Tâches avancées (administrateur uniquement)

Les pages "Authentification et informations d’identification" et "Paramètres avancés" de Credential Manager sont uniquement disponibles pour les utilisateurs dotés de droits d’administrateur. À partir de ces pages, vous pouvez réaliser les tâches suivantes :

- Spécification de méthodes de connexion d’utilisateurs et d’administrateurs
- Configuration des conditions d’authentification personnalisées
- Configuration des propriétés des informations d’authentification
- Configuration des paramètres de Credential Manager

## Spécification de méthodes de connexion d’utilisateurs et d’administrateurs

La page "Authentification et informations d’identification" permet de spécifier le type ou la combinaison des informations d’authentification requises pour les utilisateurs ou les administrateurs.

Pour spécifier comment les utilisateurs ou administrateurs se connectent :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Authentification et informations d’identification**.
3. Dans le volet droit, cliquez sur l’onglet **Authentification**.
4. Cliquez sur la catégorie (**Utilisateurs** ou **Administrateurs**) dans la liste de catégories.
5. Cliquez sur le type ou la combinaison de méthodes d’authentification dans la liste.
6. Cliquez sur **Appliquer**, puis sur **OK**.

## Configuration des conditions d’authentification personnalisées

Si le jeu d’informations d’authentification souhaité ne figure pas dans l’onglet Authentification de la page "Authentification et informations d’identification", vous pouvez créer des exigences personnalisées.

Pour configurer des exigences personnalisées :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Authentification et informations d’identification**.
3. Dans le volet droit, cliquez sur l’onglet **Authentification**.
4. Cliquez sur la catégorie (**Utilisateurs** ou **Administrateurs**) dans la liste de catégories.
5. Cliquez sur **Personnaliser** dans la liste des modes d’authentification.
6. Cliquez sur **Configure** (Configurer).
7. Sélectionnez les modes d’authentification à utiliser.
8. Choisissez la combinaison de méthodes en cliquant sur une des options suivantes :
   - Utiliser ET pour associer les modes d’authentification.

     Les utilisateurs devront s’authentifier avec tous les modes sélectionnés à chaque connexion.
   - Utiliser OU pour exiger un ou plusieurs modes d’authentification

     Les utilisateurs pourront choisir un des modes sélectionnées à chaque connexion.
9. Cliquez sur **OK**.
10. Cliquez sur **Appliquer**, puis sur **OK**.

## Configuration des propriétés des informations d’authentification

À partir de l’onglet Informations d’authentification de la page "Authentification et informations d’identification", vous pouvez visualiser la liste des modes d’authentification disponibles et modifier les paramètres.

Pour configurer les informations d’authentification :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Authentification et informations d’identification**.
3. Dans le volet droit, cliquez sur l’onglet **Informations d’authentification**.
4. Cliquez sur le type d’informations d’authentification à modifier. Vous pouvez modifier les informations d’authentification en cliquant sur l’une des options suivantes :
   - Pour enregistrer les informations d’authentification, cliquez sur **Enregistrer**, puis suivez les instructions à l’écran.
   - Pour supprimer les informations d’authentification, cliquez sur **Effacer**, puis sur **Oui** dans la boíte de dialogue de confirmation.
   - Pour modifier les informations d’authentification, cliquez sur **Propriétés**, puis suivez les instructions à l’écran.
5. Cliquez sur **Appliquer**, puis sur **OK**.

## Configuration des paramètres de Credential Manager

La page Paramètres permet d'accéder à divers paramètres et de les modifier via les onglets suivants :

- Général : Permet de modifier les paramètres de configuration de base.
- Authentification unique : Permet de modifier les paramètres de fonctionnement de la fonction Authentification unique pour l'utilisateur actuel, par exemple la manière dont elle traite la détection d'écrans de connexion, la connexion automatique sur des boîtes de dialogue enregistrées, ainsi que l'affichage des mots de passe.
- Services et applications : Permet de visualiser les services disponibles et de modifier leurs paramètres.
- Paramètres biométriques : Permet de sélectionner le logiciel du lecteur d'empreintes digitales et de régler le niveau de sécurité du lecteur.
- Smart Cards et jetons : Permet de visualiser et de modifier les propriétés de l'ensemble des Java Cards et jetons disponibles.

Pour modifier les paramètres de Credential Manager :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Paramètres**.
3. Dans le volet droit, cliquez sur l'onglet approprié aux paramètres à modifier.
4. Suivez les instructions à l'écran pour modifier les paramètres.
5. Cliquez sur **Appliquer**, puis sur **OK**.

### Exemple 1 : Utilisation de la page Paramètres avancés pour autoriser une connexion à Windows à partir de Credential Manager

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Paramètres**.
3. Dans le volet droit, cliquez sur l'onglet **Général**.
4. Sous **Select the way users log on to Windows (requires restart)** (Sélection de la méthode de connexion des utilisateurs à Windows [requiert un redémarrage]), cochez la case **Use Credential Manager with classic logon prompt** (Utiliser Credential Manager avec l'invite de connexion classique).
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Redémarrez l'ordinateur.

**REMARQUE :** La sélection de la case **Use Credential Manager with classic logon prompt** (Utiliser Credential Manager avec l'invite de connexion classique) vous permet de verrouiller votre ordinateur. Reportez-vous à la section "Verrouillage de l'ordinateur page 17".

### Exemple 2 : Utilisation de la page Paramètres avancés pour procéder à la vérification de l'utilisateur avant de procéder à l'authentification unique

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, sélectionnez **Credential Manager**, puis cliquez sur **Paramètres**.
3. Dans le volet droit, cliquez sur l'onglet **Authentification unique**.
4. Sous **Lorsqu'une page Web ou une boíte de dialogue de connexion enregistrée est visitée**, cochez la case **Valider l'utilisateur avant d'envoyer les informations d'identification**.
5. Cliquez sur **Appliquer**, puis sur **OK**.
6. Redémarrez l'ordinateur.

# 3 Embedded Security for HP ProtectTools

**REMARQUE :** Pour pouvoir utiliser la fonction Embedded Security for HP ProtectTools, la puce de sécurité intégrée TPM (Trusted Platform Module) doit être installée sur l'ordinateur.

Le module Embedded Security for HP ProtectTools protège les données utilisateur et les informations d'authentification contre tout accès non autorisé. Ce module logiciel propose les fonctions de sécurité suivantes :

- Cryptage de fichiers et de dossiers EFS (Encryption File System) Microsoft®
- Création d'un lecteur sécurisé personnel (PSD) pour la protection de données utilisateur
- Fonctions de gestion de données, telles que la sauvegarde et la restauration de la hiérarchie de clés
- Prise en charge d'applications d'autres sociétés (telles que Microsoft Outlook et Internet Explorer) pour les opérations protégées impliquant l'utilisation de certificats numériques avec la sécurité intégrée

La puce de sécurité intégrée TPM améliore et active d'autres fonctions de sécurité du logiciel HP ProtectTools Security Manager. Par exemple, le module Credential Manager for HP ProtectTools peut utiliser la puce intégrée comme facteur d'authentification lorsque l'utilisateur se connecte à Windows. Sur certains modèles, la puce de sécurité intégrée TPM active également des fonctions évoluées de sécurité du BIOS via le module BIOS Configuration for HP ProtectTools.

# Procédures de configuration

△ **ATTENTION :** Pour réduire les risques de sécurité, il est vivement recommandé que l'administrateur informatique initialise immédiatement la puce de sécurité intégrée. La non-initialisation de la puce de sécurité intégrée pourrait résulter en ce qu'un utilisateur non autorisé, un ver informatique ou un virus devienne propriétaire de l'ordinateur et prenne le contrôle des tâches du propriétaire, telles que le traitement de l'archive de restauration d'urgence et la configuration des paramètres d'accès utilisateur.

Suivez les étapes des deux sections suivantes pour initialiser la puce de sécurité intégrée.

## Activation de la puce de sécurité intégrée

La puce de sécurité intégrée doit être activée dans l'utilitaire Computer Setup. Cette procédure ne peut pas être réalisée dans le module BIOS Configuration for HP ProtectTools.

Pour activer la puce de sécurité intégrée :

1. Ouvrez Computer Setup en démarrant ou redémarrant l'ordinateur, puis en appuyant sur la touche F10 lorsque le message « F10 = ROM Based Setup » s'affiche dans l'angle inférieur gauche de l'écran.
2. Si vous n'avez pas défini de mot de passe administrateur, sélectionnez **Securité > Mot de passe de configuration** à l'aide des touches de direction, puis appuyez sur Entrée.
3. Entrez votre mot de passe dans les zones **New password** (Nouveau mot de passe) et **Verify new Password** (Vérifier le nouveau mot de passe), puis appuyez sur F10.
4. Dans le menu **Sécurité**, utilisez les touches de direction pour sélectionner **Sécurité intégrée TPM**, puis appuyez sur Entrée.
5. Sous **Sécurité intégrée**, si le périphérique est masqué, sélectionnez **Disponible**.
6. Sélectionnez **Etat du périphérique de sécurité intégrée** et modifiez l'état sur **Activé**.
7. Appuyez sur F10 pour accepter les modifications apportées à la configuration d'Embedded Security.
8. Pour enregistrer vos préférences et quitter Computer Setup, sélectionnez **Fichier > Enregistrer les modifications et quitter** à l'aide des touches de direction. Suivez ensuite les instructions affichées à l'écran.

## Initialisation de la puce de sécurité intégrée

Dans le processus d'initialisation de la sécurité intégrée, vous effectuerez les opérations suivantes :

- Définition d'un mot de passe propriétaire pour la puce de sécurité intégrée, afin de protéger l'accès à toutes les fonctions propriétaire sur cette dernière.
- Définition de l'archive de restauration d'urgence, qui est une zone de stockage protégée permettant le recryptage des clés utilisateur de base pour tous les utilisateurs.

Pour initialiser la puce de sécurité intégrée :

1. Cliquez avec le bouton droit sur l'icône HP ProtectTools Security Manager dans la zone de notification, à l'extrémité droite de la barre des tâches, puis sélectionnez **Initialisation de la sécurité intégrée**.

   L'Assistant Initialisation de la sécurité intégrée HP ProtectTools s'affiche.

2. Suivez les instructions à l'écran.

## Configuration du compte utilisateur de base

La définition d'un compte utilisateur de base dans Embedded Security :

- Produit une clé utilisateur de base qui protège les informations cryptées, et définit un mot de passe de la clé utilisateur de base qui protège cette dernière.
- Définit un lecteur sécurisé personnel (PSD) pour le stockage de fichiers et de dossiers cryptés.

△ **ATTENTION :** Protégez le mot de passe de la clé utilisateur de base. Les informations cryptées ne sont pas accessibles ou ne peuvent pas être restaurées sans ce mot de passe.

Pour configurer un compte utilisateur de base et activer les fonctions de sécurité intégrée :

1. Si l'assistant d'initialisation d'Embedded Security n'est pas ouvert, sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Paramètres utilisateur**.
3. Dans le volet droit, sous **Fonctions de sécurité intégrée**, cliquez sur **Configurer**.

   L'Assistant Initialisation de l'utilisateur de la sécurité intégrée s'affiche.
4. Suivez les instructions à l'écran.

**REMARQUE :** Pour utiliser une messagerie électronique sécurisée, vous devez d'abord configurer le client de messagerie pour utiliser un certificat numérique créé dans la sécurité intégrée. Si aucun certificat numérique n'est disponible, vous devez en obtenir un auprès d'une autorité de certification. Pour obtenir des instructions sur la configuration de votre messagerie électronique et obtenir un certificat numérique, reportez-vous à l'aide en ligne du client de messagerie.

# Tâches générales

Une fois le compte utilisateur de base défini, vous pouvez effectuer les tâches suivantes :

- Cryptage de fichiers et dossiers
- Envoi et réception de courrier électronique crypté

## Utilisation du lecteur sécurisé personnel

Une fois le lecteur PSD configuré, vous êtes invité à saisir le mot de passe de la clé utilisateur de base à la connexion suivante. Si ce mot de passe est correctement saisi, vous pouvez accéder au lecteur PSD directement à partir de l'Explorateur Windows.

## Cryptage de fichiers et dossiers

Lors de l'utilisation de fichiers cryptés, respectez les règles suivantes :

- Seuls les fichiers et dossiers situés sur des partitions NTFS peuvent être cryptés. Les fichiers et dossiers situés sur des partitions FAT ne peuvent pas être cryptés.
- Les fichiers système et les fichiers compressés ne peuvent pas être cryptés, et les fichiers cryptés ne peuvent pas être compressés.
- Il est recommandé de crypter les dossiers temporaires car les pirates s'y intéressent particulièrement.
- Une stratégie de restauration est automatiquement définie lorsque vous cryptez un fichier ou un dossier pour la première fois. Grâce à cette stratégie, si vous perdez vos certificats de cryptage et clés privées, vous pourrez utiliser un agent de restauration pour décrypter vos informations.

Pour crypter des fichiers et dossiers :

1. Cliquez avec le bouton droit sur le fichier ou dossier à crypter.
2. Cliquez sur **Crypter**.
3. Cliquez sur une des options suivantes :
   - **Appliquer les modifications à ce dossier uniquement**
   - **Appliquer les modifications à ce dossier, aux sous-dossiers et aux fichiers**
4. Cliquez sur **OK**.

## Envoi et réception de courrier électronique crypté

La sécurité intégrée permet d'envoyer et de recevoir du courrier électronique crypté, mais les procédures varient en fonction du programme que vous utilisez pour accéder à votre courrier. Pour plus d'informations, reportez-vous à l'aide en ligne de la sécurité intégrée et à l'aide en ligne de votre messagerie électronique.

## Modification du mot de passe de la clé utilisateur de base

Pour modifier le mot de passe de la clé utilisateur de base :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Paramètres utilisateur**.
3. Dans le volet droit, sous **Mot de passe de la clé utilisateur de base**, cliquez sur **Modifier**.
4. Entrez l'ancien mot de passe, puis définissez et confirmez le nouveau mot de passe.
5. Cliquez sur **OK**.

# Tâches avancées

## Sauvegarde et restauration

La fonction de sauvegarde de la sécurité intégrée crée une archive qui contient des informations de certification à restaurer en cas d'urgence.

### Création d'un fichier de sauvegarde

Pour créer un fichier de sauvegarde :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Sauvegarde**.
3. Dans le volet droit, cliquez sur **Backup** (Sauvegarde). L'assistant de sauvegarde Embedded Security s'affiche.
4. Suivez les instructions à l'écran.

### Restauration des données de certification à partir du fichier de sauvegarde

Pour restaurer des données à partir du fichier de sauvegarde :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Sauvegarde**.
3. Dans le volet droit, cliquez sur **Restore** (Restaurer). L'assistant de sauvegarde Embedded Security s'affiche.
4. Suivez les instructions à l'écran.

## Modification du mot de passe propriétaire

Pour modifier le mot de passe propriétaire

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Avancé**.
3. Dans le volet droit, sous **Mot de passe propriétaire**, cliquez sur **Modifier**.
4. Entrez l'ancien mot de passe propriétaire, puis définissez et confirmez le nouveau mot de passe propriétaire.
5. Cliquez sur **OK**.

## Réinitialisation d'un mot de passe utilisateur

Un administrateur peut aider un utilisateur à réinitialiser un mot de passe oublié. Pour plus d'informations, reportez-vous à l'aide en ligne.

## Activation et désactivation de la sécurité intégrée

Il est possible de désactiver les fonctions de sécurité intégrée si vous souhaitez travailler sans fonction de sécurité.

Les fonctions de sécurité intégrée peuvent être activées ou désactivées à deux niveaux différents :

- Désactivation temporaire : la sécurité intégrée est automatiquement réactivée au redémarrage de Windows. Cette option est disponible par défaut à tous les utilisateurs.
- Désactivation permanente : le mot de passe propriétaire est requis pour réactiver la sécurité intégrée. Cette option est disponible uniquement pour les administrateurs.

### Désactivation permanente de la sécurité intégrée

Pour désactiver en permanence la sécurité intégrée :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Avancé**.
3. Dans le volet droit, sous **Sécurité intégrée**, cliquez sur **Désactivé**.
4. À l'invite, entrez votre mot de passe propriétaire, puis cliquez sur **OK**.

### Activation de la sécurité intégrée après une désactivation permanente

Pour activer la sécurité intégrée après une désactivation permanente :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Sécurité intégrée**, puis sur **Avancé**.
3. Dans le volet droit, sous **Sécurité intégrée**, cliquez sur **Activé**.
4. À l'invite, entrez votre mot de passe propriétaire, puis cliquez sur **OK**.

## Migration de clés avec l’Assistant de migration

La migration est une tâche avancée d’administrateur qui permet la gestion, la restauration et le transfert de clés et de certificats.

Pour plus d’informations sur la migration, reportez-vous à l’aide en ligne de la sécurité intégrée.

# 4 Java Card Security for HP ProtectTools

Le module Java Card Security for HP ProtectTools permet de gérer l'installation et la configuration d'une Java Card pour les ordinateurs équipés d'un lecteur de Java Card en option.

Le module Java Card Security for HP ProtectTools vous permet d'exécuter les tâches suivantes :

- Accès aux fonctions de sécurité de Java Card
- Exécution de l'utilitaire Computer Setup pour activer l'authentification Java Card à la mise sous tension
- Configuration de Java Cards distinctes pour l'administrateur et l'utilisateur. Un utilisateur peut insérer la Java Card et saisir un code PIN avant le chargement du système d'exploitation.
- Définition et modification du code PIN utilisé pour authentifier les utilisateurs de la Java Card

# Tâches générales

La page Général permet de réaliser les tâches suivantes :

- Modification du code PIN d'une Java Card
- Sélectionnez le lecteur de carte ou le clavier Smart Card

**REMARQUE :** Le lecteur de cartes prend en charge les Smart Cards et les Java Cards. Cette fonction est disponible si vous disposez de plusieurs lecteurs de cartes sur l'ordinateur.

## Modification du code PIN d'une Java Card

Pour modifier le code PIN d'une Java Card :

**REMARQUE :** Le code PIN d'une Java Card doit comprendre entre 4 et 8 caractères numériques.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Général**.
3. Insérez une Java Card (dotée d'un code PIN existant) dans le lecteur de cartes.
4. Dans le volet droit, cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Changer le code PIN**, saisissez le code PIN actuel dans le champ **Code PIN actuel**.
6. Saisissez un nouveau code PIN dans le champ **Nouveau code PIN**, puis saisissez-le à nouveau dans le champ **Confirmer le nouveau code PIN**.
7. Cliquez sur **OK**.

## Sélection du lecteur de cartes

Assurez-vous que le lecteur de cartes approprié est sélectionné dans Java Card Security avant d'utiliser la Java Card. À défaut, certaines des fonctions peuvent ne pas être disponibles ou risquent de s'afficher de manière incorrecte. En outre, les pilotes des lecteurs de cartes doivent être correctement installés, comme indiqué dans le Gestionnaire de périphériques Windows.

Pour sélectionner le lecteur de cartes :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Général**.
3. Insérez la Java Card dans le lecteur de cartes.
4. Dans le volet droit, sous **Lecteur de cartes sélectionné**, cliquez sur le lecteur approprié.

# Tâches avancées (administrateur uniquement)

La page Avancé permet de réaliser les tâches suivantes :

- Attribution d'un code PIN de Java Card
- Attribution d'un nom à une Java Card
- Définition de l'authentification à la mise sous tension
- Sauvegarde et restauration de Java Cards

**REMARQUE :** Pour accéder à la page "Avancé", vous devez disposer de privilèges administrateur Windows.

## Attribution d'un code PIN à la Java Card

Vous devez attribuer un nom et un code PIN à une Java Card avant de pouvoir l'utiliser dans Java Card Security.

Pour attribuer un code PIN à une Java Card :

**REMARQUE :** Le code PIN d'une Java Card doit comprendre entre 4 et 8 caractères numériques.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Avancé**.
3. Insérez une nouvelle Java Card dans le lecteur de cartes.
4. Lorsque la boíte de dialogue **Nouvelle carte** s'affiche, saisissez un nouveau nom dans le champ **Nouveau nom d'affichage**, saisissez un nouveau code PIN dans le champ **Nouveau code PIN**, puis saisissez-le à nouveau dans le champ **Confirmer le nouveau code PIN**.
5. Cliquez sur **OK**.

## Attribution d’un nom à une Java Card

Vous devez attribuer un nom à une Java Card avant de pouvoir l’utiliser pour une authentification à la mise sous tension.

Pour attribuer un nom à une Java Card :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Avancé**.
3. Insérez la Java Card dans le lecteur de cartes.

**REMARQUE :** Si vous n’avez pas attribué de code PIN à cette carte, la boîte de dialogue **Nouvelle carte** s’affiche et permet de saisir un nouveau nom ainsi qu’un nouveau code PIN.

4. Dans le volet droit, sous **Nom d’affichage**, cliquez sur **Modifier**.
5. Saisissez un nom pour la Java Card dans la zone de texte **Nom**.
6. Saisissez le code PIN actuel de la Java Card dans la zone de texte **Code PIN**.
7. Cliquez sur **OK**.

## Définition de l’authentification à la mise sous tension

Lorsqu’elle est activée, l’authentification à la mise sous tension requiert que vous utilisiez une Java Card pour démarrer l’ordinateur.

Le processus d’activation de l’authentification à la mise sous tension de la Java Card implique les étapes suivantes :

1. Activation de la prise en charge de l’authentification par Java Card au démarrage dans BIOS Configuration ou Computer Setup. Pour plus d’informations, reportez-vous à la section "Activation et désactivation de la prise en charge de l’authentification de la Smart Card à la mise sous tension page 46".
2. Activation de l’authentification par Java Card au démarrage dans Java Card Security.
3. Création et activation de la Java Card administrateur.

## Activation de la prise en charge de l'authentification par Java Card au démarrage et création d'une Java Card administrateur

Pour activer l'authentification de la Java Card au démarrage :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Avancé**.
3. Insérez la Java Card dans le lecteur de cartes.

**REMARQUE :** Si vous n'avez pas attribué de nom et de code PIN à cette carte, la boíte de dialogue **Nouvelle carte** s'affiche et permet d'entrer un nouveau nom ainsi qu'un nouveau code PIN.

4. Dans le volet droit, sous **Authentification à la mise sous tension**, cochez la case **Activer**.
5. Dans la boíte de dialogue **Mot de passe Computer Setup**, saisissez le mot de passe Computer Setup, puis cliquez sur **OK**.
6. Si la fonction DriveLock n'est pas activée, saisissez le code PIN de la Java Card, puis cliquez sur **OK**.

   – ou –

   Si la fonction DriveLock est activée :

   a. Cliquez sur **Rendre l'identité de la Java Card unique**.

      – ou –

      Cliquez sur **Rendre l'identité de la Java Card identique au mot de passe DriveLock**.

      **REMARQUE :** Si la fonction DriveLock est activée sur l'ordinateur, vous pouvez définir l'identité de la Java Card sur le mot de passe utilisateur DriveLock, ce qui permet de valider la fonction DriveLock et la Java Card en utilisant uniquement cette dernière au démarrage de l'ordinateur.

   b. S'il y a lieu, saisissez votre mot de passe utilisateur DriveLock dans le champ **Mot de passe DriveLock**, puis saisissez-le à nouveau dans le champ **Confirmer le mot de passe**.

   c. Saisissez le code PIN de la Java Card.

   d. Cliquez sur **OK**.

7. Lorsque vous êtes invité à créer un fichier de restauration, cliquez sur **Annuler** pour créer ultérieurement un fichier de restauration, ou cliquez sur **OK** et suivez les instructions à l'écran de l'assistant de sauvegarde HP ProtectTools pour créer immédiatement un fichier de restauration.

**REMARQUE :** Pour plus d'informations, reportez-vous à la section "HP ProtectTools Backup and Restore page 8".

## Création d’une Java Card utilisateur

**REMARQUE :** L’authentification à la mise sous tension et une carte administrateur doivent être configurées pour créer une Java Card utilisateur.

Pour créer une Java Card utilisateur :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Avancé**.
3. Insérez une Java Card qui sera employée comme carte utilisateur.
4. Dans le volet droit, sous **Authentification à la mise sous tension**, cliquez sur **Créer** en regard de **Identité de la carte utilisateur**.
5. Saisissez un code PIN pour la Java Card utilisateur, puis cliquez sur **OK**.

## Désactivation de l’authentification de la Java Card à la mise sous tension

Lorsque vous désactivez l’authentification de mise sous tension de la Java Card, l’utilisation de la Java Card n’est plus requise pour démarrer l’ordinateur.

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Java Card Security**, puis sur **Avancé**.
3. Insérez la Java Card d’administrateur.
4. Dans le volet droit, sous **Authentification à la mise sous tension**, désactivez la case à cocher **Activer**.
5. Saisissez un code PIN pour la Java Card, puis cliquez sur **OK**.

# 5 BIOS Configuration for HP ProtectTools

Le module BIOS Configuration for HP ProtectTools fournit un accès aux paramètres de configuration et de sécurité de l'utilitaire Computer Setup. Ainsi, les utilisateurs accèdent aux fonctions de sécurité du système gérées par Computer Setup.

Le module BIOS Configuration vous permet d'exécuter les tâches suivantes :

- Gestion des mots de passe de mise sous tension et des mots de passe administrateur
- Configuration d'autres fonctions d'authentification à la mise sous tension, telles que l'activation de la prise en charge de l'authentification de la sécurité intégrée
- Activation et désactivation de fonctions matérielles, telles que l'amorçage par CD-ROM ou différents ports matériels
- Configuration d'options d'amorçage, notamment l'activation MultiBoot et la modification de l'ordre d'amorçage

**REMARQUE :** La plupart des fonctions du module BIOS Configuration for HP ProtectTools sont également disponibles dans Computer Setup.

# Tâches générales

BIOS Configuration permet de gérer divers paramètres de l'ordinateur qui, sinon, seraient uniquement accessibles par une pression sur la touche F10 au démarrage et au lancement de Computer Setup.

## Gestion des options d’amorçage

Vous pouvez utiliser le module BIOS Configuration pour gérer divers paramètres pour des tâches qui s’exécutent à la mise sous tension ou au redémarrage de l’ordinateur.

Pour gérer les options d’amorçage :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**.
3. À l’invite de saisie du mot de passe administrateur du BIOS, saisissez le mot de passe administrateur de Computer Setup, puis cliquez sur **OK**.

**REMARQUE :** L’invite de saisie du mot de passe administrateur du BIOS s’affiche uniquement si vous avez déjà défini le mot de passe de Computer Setup. Pour plus d’informations sur la définition du mot de passe Computer Setup, reportez-vous à la section "Définition du mot de passe de configuration page 50".

4. Dans le volet gauche, cliquez sur **Configuration système**.
5. Dans le volet droit, sélectionnez les délais (en secondes) pour F9, F10 et F12, ainsi que pour **Express Boot Popup Delay (Sec)**.(Délai de la fenêtre de démarrage express (Sec)).
6. Activez ou désactivez **MultiBoot**.
7. Si vous avez activé MultiBoot, sélectionnez l’ordre d’amorçage en sélectionnant un périphérique d’amorçage, puis en cliquant sur la flèche vers le haut ou vers le bas pour le positionner dans la liste.
8. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Activation et désactivation des options de configuration système

**REMARQUE :** Certains des éléments répertoriés ci-dessous peuvent ne pas être pris en charge par votre ordinateur.

Pour activer ou désactiver des options de sécurité ou de périphérique :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**.
3. À l'invite de saisie du mot de passe administrateur du BIOS, entrez le mot de passe administrateur de Computer Setup, puis cliquez sur **OK**.
4. Dans le volet gauche, cliquez sur **Configuration système**, puis activez ou désactivez une option de configuration système, ou configurez une des options suivantes de configuration système dans le volet droit :
   - Options de port
     - Port série
     - Port infrarouge
     - Port parallèle
     - Connecteur SD
     - Port USB
     - Port 1394
     - Connecteur Cardbus
     - Connecteur ExpressCard
   - Options d'amorçage
     - Délais de F9, F10 et F12 (sec.)
     - MultiBoot
     - Retard d'amorçage express (secondes)
     - Amorçage par CD-ROM
     - Amorçage par disquette
     - Amorçage par carte réseau interne
     - Mode d'amorçage par carte réseau interne (PXE ou RPL)
     - Ordre d'amorçage
   - Configurations de périphérique
     - Verrouillage numérique à l'amorçage
     - Échange de touches fn/Ctrl
     - Périphériques de pointage multiples
     - Support USB Legacy
     - Mode de port parallèle (standard, bidirectionnel, EPP ou ECP)

- Prévention d’exécution de données
- Mode natif SATA
- Double unité centrale
- Prise en charge de fonctionnalité Intel® SpeedStep automatique
- Ventilateur toujours actif sous alimentation secteur
- Transferts de données DMA BIOS
- Désactivation d’exécution Intel ou AMD PSAE

- Options de périphérique intégré
  - Périphérique radio WLAN intégré
  - Périphérique radio WWAN intégré
  - Périphérique radio Bluetooth® intégré
  - Basculement LAN/WLAN
  - Remise sous tension de Wake On LAN

5. Cliquez sur **Appliquer**, puis cliquez sur **OK** dans la fenêtre HP ProtectTools pour enregistrer vos modifications et quitter.

# Tâches avancées

## Gestion des paramètres de modules complémentaires HP ProtectTools

Certaines des fonctions du logiciel HP ProtectTools Security Manager peuvent être gérées dans le module BIOS Configuration.

### Activation et désactivation de la prise en charge de l'authentification de la Smart Card à la mise sous tension

L'activation de cette option permet d'utiliser une Smart Card pour l'authentification d'utilisateur à la mise sous tension de l'ordinateur.

**REMARQUE :** Pour activer intégralement la fonction d'authentification à la mise sous tension, vous devez également configurer une Smart Card à l'aide du module Java Card Security for HP ProtectTools.

Pour activer la prise en charge de l'authentification de la Smart Card au démarrage :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**.
3. À l'invite de saisie du mot de passe administrateur du BIOS, entrez le mot de passe administrateur de Computer Setup, puis cliquez sur **OK**.
4. Dans le volet gauche, cliquez sur **Sécurité**.
5. Sous **Sécurité Smart Card**, cliquez sur **Activer**.

   **REMARQUE :** Pour désactiver la prise en charge de l'authentification de la Smart Card à la mise sous tension, cliquez sur **Désactiver**.

6. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Activation et désactivation de la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée

L'activation de cette option permet au système d'utiliser la puce de sécurité intégrée TPM (si disponible) pour l'authentification de l'utilisateur à la mise sous tension de l'ordinateur.

**REMARQUE :** Pour activer intégralement la fonction d'authentification à la mise sous tension, vous devez également configurer la puce de sécurité intégrée TPM à l'aide du module Embedded Security for HP ProtectTools.

Pour activer la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**.
3. À l'invite de saisie du mot de passe administrateur du BIOS, entrez le mot de passe administrateur de Computer Setup, puis cliquez sur **OK**.
4. Dans le volet gauche, cliquez sur **Sécurité**.
5. Sous **Sécurité intégrée**, cliquez sur **Activer la prise en charge de l'authentification à la mise sous tension**.

   **REMARQUE :** Pour désactiver la prise en charge de l'authentification pour la sécurité intégrée au démarrage, cliquez sur **Désactiver**.

6. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Activation et désactivation de la protection de disque dur DriveLock

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

### Utilisation de DriveLock

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

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

### Applications de DriveLock

La fonction de sécurité DriveLock est surtout utilisée dans les entreprises. L'administrateur système est responsable de la configuration du disque dur, qui comprend notamment la définition du mot de passe DriveLock principal et d'un mot de passe d'utilisateur temporaire. Si l'utilisateur oublie son mot de passe ou si un autre employé récupère l'équipement, le mot de passe principal permet de redéfinir le mot de passe d'utilisateur et d'accéder à nouveau au disque dur.

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

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

## Gestion de mots de passe Computer Setup

Vous pouvez utiliser le module BIOS Configuration pour définir et modifier les mots de passe de mise sous tension et de configuration dans Computer Setup, ainsi que pour gérer divers paramètres de mot de passe.

△ **ATTENTION :** Les mots de passe que vous définissez via la page "Mots de passe" du module BIOS Configuration sont immédiatement enregistrés lorsque vous cliquez sur le bouton **Appliquer** ou **OK** dans la fenêtre HP ProtectTools. Assurez-vous de mémoriser le mot de passe que vous avez défini car vous ne pourrez pas annuler une définition de mot de passe sans fournir le mot de passe antérieur.

Le mot de passe de mise sous tension peut protéger votre ordinateur d'une utilisation non autorisée.

**REMARQUE :** Une fois un mot de passe de mise sous tension défini, le bouton Définir de la page "Mots de passe" est remplacé par un bouton Modifier.

Le mot de passe Computer Setup protège les paramètres de configuration et les informations d'identification du système dans Computer Setup. Une fois ce mot de passe défini, vous devez le saisir pour accéder à Computer Setup. Si vous avez défini un mot de passe de configuration, vous serez invité à le fournir avant l'ouverture du module BIOS Configuration de HP ProtectTools.

**REMARQUE :** Une fois un mot de passe de configuration défini, le bouton Définir de la page "Mots de passe" est remplacé par un bouton Modifier.

### Définition du mot de passe de mise sous tension

Pour définir le mot de passe de mise sous tension :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, en regard de **Mot de passe de mise sous tension**, cliquez sur **Définir**.
4. Entrez et confirmez le mot de passe dans les champs **Entrer le mot de passe** et **Vérifier le mot de passe**.
5. Cliquez sur **OK** dans la boîte de dialogue **Mots de passe**.
6. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

### Modification du mot de passe de mise sous tension

Pour modifier le mot de passe de mise sous tension :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, en regard de **Mot de passe de mise sous tension**, cliquez sur **Modifier**.
4. Entrez le mot de passe actuel dans le champ **Ancien mot de passe**.
5. Définissez et confirmez le nouveau mot de passe dans le champ **Nouveau mot de passe**.

6. Cliquez sur **OK** dans la boíte de dialogue **Mots de passe**.
7. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Définition du mot de passe de configuration

Pour définir le mot de passe Computer Setup :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, en regard de **Mot de passe de configuration**, cliquez sur **Définir**.
4. Entrez et confirmez le mot de passe dans les champs **Entrer le mot de passe** et **Confirmer le mot de passe**.
5. Cliquez sur **OK** dans la boíte de dialogue **Mots de passe**.
6. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Modification du mot de passe de configuration

Pour modifier le mot de passe Computer Setup :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, en regard de **Mot de passe de configuration**, cliquez sur **Modifier**.
4. Entrez le mot de passe actuel dans le champ **Ancien mot de passe**.
5. Entrez et confirmez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Vérifier le nouveau mot de passe**.
6. Cliquez sur **OK** dans la boíte de dialogue **Mots de passe**.
7. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

## Définition d’options de mot de passe

Vous pouvez utiliser le module BIOS Configuration for HP ProtectTools pour définir des options de mot de passe afin d’améliorer la sécurité de votre système.

### Activation et désactivation de la sécurité stricte

△ **ATTENTION :** Pour empêcher que l’ordinateur ne devienne définitivement inutilisable, enregistrez le mot de passe de configuration, le mot de passe de mise sous tension ou le code PIN de la Smart Card en lieu sûr, loin de l’ordinateur. Sans ces mots de passe ou le code PIN, l’ordinateur ne peut pas être déverrouillé.

L’activation de la sécurité stricte fournit une protection améliorée pour les mots de passe d’administrateur et de mise sous tension, ainsi que d’autres formes d’authentification à la mise sous tension.

Pour activer ou désactiver la sécurité stricte :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, sous **Options de mot de passe**, activez ou désactivez l’option **Sécurité stricte**.

**REMARQUE :** Si vous souhaitez désactiver la sécurité stricte, décochez la case **Activer la sécurité stricte**.

4. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

### Activation et désactivation de l'authentification à la mise sous tension au redémarrage de Windows

Cette option permet d'améliorer la sécurité stricte en demandant aux utilisateurs de saisir un mot de passe de mise sous tension, TPM ou de la Smart Card au redémarrage de Windows.

Pour activer ou désactiver l'authentification à la mise sous tension au redémarrage de Windows :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **BIOS Configuration**, puis sur **Sécurité**.
3. Dans le volet droit, sous **Options de mot de passe**, activez ou désactivez l'option **Exiger un mot de passe au redémarrage**.
4. Cliquez sur **Appliquer**, puis sur **OK** dans la fenêtre HP ProtectTools.

# 6 Drive Encryption for HP ProtectTools

△ **ATTENTION :** Si vous souhaitez désinstaller le module Drive Encryption, vous devez au préalable décrypter tous les lecteurs cryptés. À défaut, vous ne pourrez pas accéder aux données enregistrées sur les lecteurs cryptés tant que vous ne vous serez pas inscrit auprès du service de récupération Drive Encryption (reportez-vous à la section "Récupération page 56"). La réinstallation du module Drive Encryption ne vous permettra pas d'accéder aux lecteurs cryptés.

# Gestion du cryptage

### Cryptage de lecteur

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Encryption Management** (Gestion du cryptage).
3. Dans le volet droit, cliquez sur **Activer**. L'Assistant Drive Encryption for HP ProtectTools s'affiche.
4. Suivez les instructions à l'écran pour activer le cryptage.

**REMARQUE :** Vous devrez spécifier une disquette, un périphérique de stockage flash ou un autre support de stockage USB sur lequel enregistrer les informations de récupération.

### Modification du cryptage

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Encryption Management** (Gestion du cryptage).
3. Dans le volet droit, cliquez sur **Change encryption** (Modifier le cryptage). Dans la boíte de dialogue **Change Encryption** (Modifier le cryptage), sélectionnez les disques à crypter, puis cliquez sur **OK**.
4. Cliquez à nouveau sur **OK** pour commencer le cryptage.

### Décryptage de lecteur

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Encryption Management** (Gestion du cryptage).
3. Dans le volet droit, cliquez sur **Désactiver**.

# Gestion des utilisateurs

### Ajout d'un utilisateur

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **User Management** (Gestion des utilisateurs).
3. Dans le volet droit, cliquez sur **Ajouter**. Cliquez sur le nom d'un utilisateur dans la liste **Nom d'utilisateur** ou saisissez un nom d'utilisateur dans la zone **Nom d'utilisateur**. Cliquez sur **Suivant**.
4. Saisissez le mot de passe Windows pour l'utilisateur sélectionné, puis cliquez sur **Suivant**.
5. Sélectionnez une méthode d'authentification pour le nouvel utilisateur, puis cliquez sur **Terminer**.

### Suppression d'un utilisateur

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **User Management** (Gestion des utilisateurs).
3. Dans le volet droit, cliquez sur le nom d'un utilisateur pour le supprimer de la liste **Nom d'utilisateur**. Cliquez sur **Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression.

### Modification de jeton

Pour modifier la méthode d'authentification d'un utilisateur, procédez comme suit :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **User Management** (Gestion des utilisateurs).
3. Dans le volet droit, sélectionnez le nom d'un utilisateur dans la liste **Nom d'utilisateur**, puis cliquez sur **Change Token** (Modifier le jeton).
4. Saisissez le mot de passe Windows de l'utilisateur, puis cliquez sur **Suivant**.
5. Sélectionnez une nouvelle méthode d'authentification, puis cliquez sur **Terminer**.
6. Si vous avez sélectionné une Java Card comme méthode d'authentification, saisissez le mot de passe Java Card lorsque vous y êtes invité, puis cliquez sur **OK**.

### Définition d'un mot de passe

Pour définir un mot de passe ou modifier la méthode d'authentification d'un utilisateur, procédez comme suit :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **User Management** (Gestion des utilisateurs).
3. Dans le volet droit, sélectionnez l'utilisateur dans la liste **Nom d'utilisateur**, puis cliquez sur **Définir le mot de passe**.
4. Entrez le mot de passe Windows de l'utilisateur, puis cliquez sur **Suivant**.

5. Sélectionnez la nouvelle méthode d’authentification, puis cliquez sur **Terminer**.

6. Si vous avez sélectionné une Java Card comme méthode d’authentification, tapez le mot de passe Java Card lorsque vous y êtes invité, puis cliquez sur **OK**.

# Récupération

Les deux mesures de sécurité suivantes sont disponibles :

- Si vous oubliez votre mot de passe, vous ne pouvez pas accéder aux lecteurs cryptés. Cependant, vous pouvez vous inscrire au service de récupération Drive Encryption pour pouvoir accéder à votre ordinateur en cas d'oubli de votre mot de passe.
- Vous pouvez sauvegarder vos clés de cryptage Drive Encryption sur une disquette, un périphérique de stockage flash ou un autre support de stockage USB.

**Inscription auprès du service de récupération Drive Encryption**

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Récupération**.
3. Dans le volet droit, cliquez sur **Click here to register** (Cliquez ici pour vous inscrire). Saisissez les informations demandées pour exécuter la procédure de sauvegarde de sécurité.

**Sauvegarde de vos clés Drive Encryption**

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Drive Encryption**, puis sur **Récupération**.
3. Dans le volet droit, cliquez sur **Click here to backup your keys** (Cliquez ici pour sauvegarder vos clés).
4. Sélectionnez une disquette, un périphérique de stockage flash ou un autre support de stockage USB sur lequel sauvegarder les informations de récupération, puis cliquez sur **Suivant**. L'Assistant Drive Encryption for HP ProtectTools s'affiche.
5. Suivez les instructions à l'écran pour sauvegarder les clés Drive Encryption.

**REMARQUE :** Vous devrez spécifier une disquette, un périphérique de stockage flash ou un autre support de stockage USB sur lequel enregistrer les informations de récupération.

# 7 Résolution des problèmes

## Credential Manager for ProtectTools

| Brève description | Détails | Solution |
|---|---|---|
| En utilisant l'option de comptes réseau Credential Manager, un utilisateur peut sélectionner un compte de domaine pour ouvrir une session. Lorsque l'authentification TPM est utilisée, cette option n'est pas disponible. Toutes les autres méthodes d'authentification fonctionnent correctement. | Avec une authentification TPM, l'utilisateur ne peut ouvrir une session que sur l'ordinateur local. | À l'aide des outils de signature unique Credential Manager, l'utilisateur peut authentifier d'autres comptes. |
| L'identification par jeton USB n'est pas disponible lors d'une ouverture de session Windows XP Service Pack 1. | Après avoir installé le logiciel du jeton USB, enregistré sa légitimation et configuré Credential Manager comme gestionnaire principal d'ouverture de session, le jeton USB n'apparaît pas dans la liste et n'est pas disponible dans la boíte de dialogue d'ouverture de session Credential Manager ou d'authentification et d'identification graphique.<br><br>En revenant à Windows pour fermer puis rouvrir la session Credential Manager et sélectionner de nouveau le jeton USB comme légitimation principale, l'ouverture de session par jeton USB fonctionne normalement. | Cela se produit uniquement avec Windows Service Pack 1 ; l'installation du Service Pack 2 via Windows Update résout le problème.<br><br>Comme solution de rechange en gardant le Service Pack 1, ouvrez une nouvelle session Windows avec une autre légitimation (mot de passe Windows) afin de fermer et rouvrir la session Credential Manager. |
| Des pages Web de certaines applications génèrent des erreurs qui empêchent l'utilisateur d'accomplir ou de terminer des tâches. | Certaines applications Web cessent de fonctionner et signalent des erreurs en raison du caractère d'invalidation de la signature unique. Par exemple, un **!** dans un triangle jaune indiquant qu'une erreur s'est produite, peut être observé dans Internet Explorer. | La signature unique du Credential Manager ne prend pas en charge toutes les interfaces Web. Désactivez la prise en charge de la signature unique pour les pages Web en question. Pour obtenir une documentation plus complète sur la fonction de signature unique, reportez-vous aux fichiers d'aide de Credential Manager.<br><br>Si une signature unique ne peut pas être désactivée pour une application donnée, appelez l'assistance HP et demandez un support de 3ème niveau via votre contact de service HP. |
| Aucune option **Browse for Virtual Token** (Parcourir les jetons virtuels) lors de l'ouverture de session. | L'utilisateur ne peut pas déplacer l'emplacement des jetons virtuels enregistrés dans Credential Manager, car l'option Parcourir à été supprimée pour des raisons de sécurité. | Cette option Parcourir a été supprimée des versions actuelles du logiciel parce qu'elle permettait à des utilisateurs non enregistrés de supprimer et de renommer des fichiers et de prendre le contrôle de Windows. |

| Brève description | Détails | Solution |
|---|---|---|
| L'ouverture de session avec authentification TPM ne présente pas l'option **Network Accounts** (Comptes réseau). | Avec l'option **Network Accounts** (Comptes réseau), un utilisateur peut sélectionner un compte de domaine pour ouvrir une session. Lorsque l'authentification TPM est utilisée, cette option n'est pas disponible. | HP recherche actuellement un palliatif pour les prochaines versions du logiciel. |
| Les administrateurs de domaines ne peuvent pas changer le mot de passe Windows, même avec autorisation. | Cela se produit lorsqu'un administrateur de domaines se connecte à un domaine et enregistre l'identité de ce domaine dans Credential manager sous un compte avec droits d'administrateur sur le domaine et sur l'ordinateur local. Lorsque l'administrateur de domaines tente de modifier le mot de passe Windows dans Credential Manager, il obtient un message d'échec d'ouverture de session : **User account restriction** (Restriction du compte utilisateur). | Credential Manager ne peut pas modifier le mot de passe d'un compte utilisateur de domaine par le biais de l'option **Change Windows password** (Changer le mot de passe Windows). Credential Manager ne peut changer que les mots de passe des comptes de l'ordinateur local. L'utilisateur d'un domaine peut modifier son mot de passe à l'aide de l'option **Windows security** > **Change password** (Sécurité Windows > Modifier le mot de passe) mais, comme l'utilisateur du domaine ne possède pas de compte physique sur l'ordinateur local, Credential Manager peut uniquement changer le mot de passe utilisé pour l'ouverture de session. |
| Le paramétrage par défaut de la signature unique dans Credential Manager devrait afficher une invite afin d'éviter une boucle. | Par défaut, la signature unique est définie de manière à ouvrir automatique la session de l'utilisateur. Cependant, lors de la création d'un second document protégé par un mot de passe différent, Credential Manager utilise le dernier mot de passe enregistré (celui du premier document). | HP recherche actuellement un palliatif pour les prochaines versions du logiciel. |
| Problèmes d'incompatibilité avec l'authentification et l'identification graphique du mot de passe Corel WordPerfect 12. | Si l'utilisateur ouvre une session Credential Manager, crée un document dans WordPerfect et l'enregistre avec une protection par mot de passe, Credential Manager ne peut pas détecter ou reconnaître le mot de passe d'authentification et d'identification graphique, que ce soit manuellement ou automatiquement. | HP recherche actuellement un palliatif pour les prochaines versions du logiciel. |
| Credential Manager ne reconnaît pas le bouton **Connect** (Connecter) à l'écran. | Si les légitimations de signature unique pour la connexion RDP (Remote Desktop Connection) sont définies sur **Connect**, la signature unique, au redémarrage, entre toujours **Save As** (Enregistrer sous) au lieu de **Connect** (Connecter). | HP recherche actuellement un palliatif pour les prochaines versions du logiciel. |
| L'assistant de configuration ATI Catalyst ne peut pas être utilisé avec Credential Manager. | La signature unique de Credential Manager entre en conflit avec l'assistant de configuration ATI Catalyst. | Désactivez la signature unique de Credential Manager. |
| Lors d'une ouverture de session avec authentification TPM, le bouton **Back** (Précédent) saute l'option et passe à une autre méthode d'authentification. | Si l'utilisateur se servant de l'authentification TPM pour Credential Manager saisit son mot de passe, le bouton **Back** (Précédent) ne fonctionne pas correctement et affiche immédiatement l'écran d'ouverture de session Windows. | HP recherche actuellement un palliatif pour les prochaines versions du logiciel. |
| Credential Manager apparaît à la sortie de l'état de veille, alors qu'il est configuré pour ne pas le faire. | Lorsque l'option **use Credential Manager log on to Windows** (Utiliser Credential Manager pour ouvrir une session Windows) n'est pas sélectionnée, le fait de permettre au système de passer dans l'état S3, puis de le réactiver provoque l'apparition du | Sans mot de passe administrateur, l'utilisateur ne peut pas ouvrir une session Windows via Credential Manager en raison des restrictions de compte invoquées par Credential Manager.<br>• Sans carte Java/jeton, l'utilisateur peut annuler la boîte de dialogue Credential Manager, ce qui fait apparaître la fenêtre d'ouverture de session |

| Brève description | Détails | Solution |
|---|---|---|
| | dialogue d'ouverture de session Credential Manager. | Windows. L'utilisateur peut alors ouvrir une session.<br>• Sans carte Java/jeton, le palliatif suivant permet à l'utilisateur d'activer/désactiver l'ouverture de Credential Manager à l'insertion de la carte Java.<br>1. Cliquez sur **Advanced Settings** (Paramètres avancés).<br>2. Cliquez sur **Service & Applications**.<br>3. Cliquez **Java Cards and Tokens** (Cartes Java et jetons).<br>4. Cliquez lorsque la carte Java ou le jeton est inséré.<br>5. Cochez la case **Advise to log-on** (Conseiller l'ouverture de session). |
| Si le module TPM est retiré ou endommagé, les utilisateurs perdent toutes les légitimations de Credential Manager protégées par le module TPM. | Les utilisateurs perdent toutes les légitimations protégées par le module TPM si celui-ci est retiré ou endommagé. | Le système est ainsi conçu.<br>Le module TPM est conçu pour protéger les légitimations de Credential Manager. Il est donc conseillé à l'utilisateur de sauvegarder les identités gérées par Credential Manager avant de retirer le module TPM. |
| Credential Manager n'est pas configuré pour l'ouverture de session principale sous Windows 2000. | Lors de l'installation de Windows 2000, la règle d'ouverture de session est réglée sur « ouverture manuelle » ou « ouverture admin. automatique ». Si le mode automatique est sélectionné, la valeur 1 est enregistrée dans le registre Windows comme valeur par défaut et Credential Manager ne la remplace pas. | Le système est ainsi conçu.<br>Si l'utilisateur souhaite modifier le paramétrage du système d'exploitation pour l'ouverture admin. automatique, la clé du registre est `HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon`.<br>**ATTENTION :** Vous utilisez l'éditeur de registre à vos propres risques ! Une utilisation incorrecte de l'éditeur de registre (regedit) peut causer de sérieux problèmes qui peuvent vous obliger à réinstaller le système d'exploitation. Il n'existe aucune garantie de pouvoir résoudre les problèmes résultant d'un mauvais usage de l'éditeur de registre. |
| Le message d'ouverture de session par empreinte digitale apparaît, qu'un lecteur d'empreinte soit ou non installé ou enregistré. | Si l'utilisateur sélectionne l'écran d'ouverture de session Windows, l'alerte suivante apparaît dans la barre des tâches de Credential Manager : **You can place your finger on the fingerprint reader to log on to Credential Manager** (Vous pouvez placer votre doigt sur le lecteur d'empreinte pour vous connecter à Credential Manager). | Le but de cette alerte est de prévenir l'utilisateur que l'authentification par empreinte digitale est disponible, si elle a été configurée. |
| L'écran d'ouverture de session Credential Manager pour Windows 2000 indique **insert card** (insérer la carte) alors qu'aucun lecteur de carte n'est branché. | L'écran d'accueil de Credential Manager suggère que l'utilisateur peut ouvrir une session par **insertion d'une carte** alors qu'aucun lecteur de carte Java n'est connecté à l'ordinateur. | Le but de cette alerte est de prévenir l'utilisateur que l'authentification par carte Java est disponible, si elle a été configurée. |
| Impossible d'ouvrir une session dans Credential Manager après un passage de l'état de veille à l'état de veille prolongée sous Windows XP Service Pack 1 uniquement. | Après avoir permis au système de passer de l'état de veille à l'état de veille prolongée, l'administrateur ou l'utilisateur est incapable d'ouvrir une session dans Credential Manager et l'écran d'ouverture de session Windows reste affiché quelle que soit la | Ce problème semble résolu par Microsoft dans le Service Pack 2. Pour plus d'informations sur la cause du problème, consultez la Base de connaissances Microsoft, article 813301, à l'adresse http://www.microsoft.com. |

| Brève description | Détails | Solution |
|---|---|---|
| | légitimation sélectionnée (mot de passe, empreinte digitale ou carte Java). | Pour ouvrir une session, l'utilisateur doit sélectionner Credential Manager et s'y connecter. Une fois la session Credential Manager ouverte, l'utilisateur est invité à ouvrir une session Windows (il se peut qu'il ait à sélectionner l'option d'écran d'accueil Windows) pour achever l'ouverture de session.<br><br>Si l'utilisateur commence par ouvrir une session Windows, il doit ensuite se connecter manuellement à Credential Manager. |
| La restauration de la sécurité intégrée provoque l'échec de Credential Manager. | Une fois le module ROM de sécurité intégrée restauré sur les paramètres usine, Credential Manager ne réussit pas à enregistrer des identités. | Le logiciel HP Credential Manager for ProtectTools ne réussit pas à accéder au module TPM si la ROM a été réinitialisée sur les paramètres usine après l'installation de Credential Manager.<br><br>La puce de sécurité TPM peut être activée dans l'utilitaire BIOS Computer Setup, le module BIOS Configuration for ProtectTools ou l'application HP Client Manager. Pour activer la puce de sécurité intégrée TPM :<br><br>1. Ouvrez Computer Setup en démarrant ou redémarrant l'ordinateur, puis en appuyant sur la touche F10 lorsque le message **F10 = ROM Based Setup** s'affiche dans l'angle inférieur gauche de l'écran.<br><br>2. Utilisez les touches de direction pour sélectionner **Security** > **Setup Password** (Sécurité > Mot de passe de configuration). Définissez un mot de passe.<br><br>3. Sélectionnez **Embedded Security Device** (Périphérique de sécurité intégrée).<br><br>4. Utilisez les touches de direction pour sélectionner **Embedded Security Device — Disable** (Périphérique de sécurité intégrée — Désactiver). Utilisez les touches de direction pour modifier l'entrée en **Embedded Security Device — Enable** (Périphérique de sécurité intégrée — Activer).<br><br>5. Sélectionnez **Enable** > **Save changes and exit** (Activer > Enregistrer les modifications et quitter).<br><br>HP recherche d'autres solutions pour les prochaines versions du logiciel. |
| Le processus de sécurité **Restore Identity** (Restaurer l'identité) perd l'association avec le jeton virtuel. | Lorsque l'utilisateur restaure son identité, Credential Manager peut perdre l'association avec l'emplacement du jeton virtuel dans l'écran d'ouverture de session. Bien que Credential Manager ait enregistré le jeton virtuel, l'utilisateur doit le réenregistrer pour rétablir l'association. | Le système est ainsi conçu.<br><br>Lorsque Credential Manager est désinstallé sans garder les identités, la partie système (serveur) du jeton est détruite, de sorte que le jeton ne peut plus être utilisé pour l'ouverture de session, même si la partie client du jeton est rétablie par une restauration d'identité.<br><br>HP recherche des solutions à long terme. |

# Embedded Security for ProtectTools

| Brève description | Détails | Solution |
|---|---|---|
| Le chiffrement de dossiers, sous-dossiers et fichiers sur PSD cause un message d'erreur. | Si l'utilisateur copie des fichiers et des dossiers sur l'unité PSD et tente de chiffrer des dossiers/fichiers ou des dossiers/sous-dossiers, le message **Error Applying Attributes** (Erreur d'application des attributs) s'affiche. L'utilisateur peut chiffrer les mêmes fichiers du disque C:\ sur un disque dur supplémentaire. | Le système est ainsi conçu.<br><br>Le fait de déplacer des fichiers/dossiers vers l'unité PSD entraîne leur chiffrement. Il n'est pas nécessaire de chiffrer deux fois les fichiers ou dossiers. Toute tentative de chiffrer des fichier ou dossiers déjà chiffrés provoquera l'affichage de ce message d'erreur. |
| Prise de possession impossible avec un autre système d'exploitation sur une plate-forme à plusieurs amorçages. | Si un disque dur est configuré pour le démarrage de plusieurs systèmes d'exploitation, la prise de possession ne peut être faite que par l'assistant d'initialisation d'un seul système d'exploitation. | Le système est ainsi conçu pour des raisons de sécurité. |
| Un administrateur non autorisé peut consulter, supprimer, renommer ou déplacer le contenu de dossiers EFS chiffrés. | Le chiffrement d'un dossier n'empêche pas un intrus possédant des droits d'administrateur de consulter, supprimer ou déplacer le contenu d'un dossier. | Le système est ainsi conçu.<br><br>Il s'agit d'une caractéristique du système EFS, pas du module TPM de sécurité intégrée. La sécurité intégrée utilise le logiciel EFS de Microsoft dans lequel tous les administrateurs conservent leurs droits d'accès aux fichiers et dossiers. |
| Les dossiers chiffrés par le système EFS dans Windows 2000 ne sont pas mis en surbrillance en vert. | Les dossiers chiffrés par le système EFS apparaissent en vert dans Windows XP, mais pas dans Windows 2000. | Le système est ainsi conçu.<br><br>Il s'agit d'une caractéristique propre au système EFS, que le module TPM de sécurité intégrée soit installé ou non. |
| Le système EFS ne requiert pas de mot de passe pour consulter des fichiers chiffrés dans Windows 2000. | Si un utilisateur initialise la sécurité intégrée, ouvre une session d'administrateur, puis la referme et la rouvre en tant qu'administrateur, il peut ensuite voir les fichiers et dossiers dans Windows 2000 sans mot de passe. Ceci se produit uniquement dans le premier compte administrateur sous Windows 2000. Si une session est établie via un compte administrateur secondaire, ceci ne se produit pas. | Le système est ainsi conçu.<br><br>Il s'agit d'une caractéristique propre au système EFS sous Windows 2000. Sous Windows XP, le système EFS ne permet pas à l'utilisateur d'ouvrir des dossiers ou des fichiers sans mot de passe. |
| Le logiciel ne devrait pas être installé sur une partition restaurée en FAT32. | Si l'utilisateur tente de restaurer le disque dur au format FAT32, il n'y aura aucune option de chiffrement pour tous les fichiers ou dossiers utilisant le système EFS. | Le système est ainsi conçu.<br><br>Le système EFS de Microsoft est uniquement pris en charge par le système de fichiers NTFS et ne fonctionne pas en FAT32. Il s'agit d'une particularité du système EFS de Microsoft qui n'a aucun lien avec le logiciel HP ProtectTools. |
| Un utilisateur Windows 2000 peut partager une quelconque unité PSD sur le réseau en partage masqué ($). | Un utilisateur Windows 2000 peut partager une quelconque unité PSD sur le réseau en partage masqué ($). Le partage masqué est accessible sur le réseau à l'aide du partage masqué ($). | En principe, l'unité PSD n'est pas partagée sur le réseau, mais elle peut l'être via le partage masqué ($) sous Windows 2000 uniquement. Il est vivement recommandé de protéger le compte Administrateur par un mot de passe. |
| Il est possible pour l'utilisateur de chiffrer ou de supprimer le fichier d'archive de restauration XML. | Par conception, la liste des autorisations d'accès à ce dossier n'est pas définie ; un utilisateur peut donc accidentellement ou volontairement supprimer le fichier et le rendre ainsi inaccessible. Une fois ce fichier chiffré ou supprimé, plus personne ne peut utiliser le logiciel TPM. | Le système est ainsi conçu.<br><br>Les utilisateurs ont accès à un fichier d'archives de secours afin d'enregistrer ou de mettre à jour la copie de sauvegarde de leur clé utilisateur de base. Il convient donc d'adopter des règles de bonne pratique en matière de sécurité et d'instruire les utilisateurs afin qu'ils ne procèdent pas au chiffrement ou à la suppression des fichiers d'archives. |

| Brève description | Détails | Solution |
|---|---|---|
| L'interaction entre le système EFS de la sécurité intégrée HP ProtectTools et Symantec Antivirus ou Norton Antivirus produit des temps d'analyse et de chiffrement/déchiffrement plus longs. | Les fichiers chiffrés interfèrent avec l'analyse Symantec Antivirus ou Norton Antivirus 2005 à la recherche de virus. Pendant l'analyse, l'invite de mot de passe de la clé utilisateur de base demande d'entrer un mot de passe tous les 10 fichiers environ. Si l'utilisateur n'entre pas de mot de passe, le dépassement de temps de l'invite de mot de passe permet à NAV2005 de poursuivre l'analyse. Le chiffrement des fichiers à l'aide du système EFS de la sécurité intégrée HP ProtectTools demande plus de temps lorsque Symantec Antivirus ou Norton Antivirus est activé. | Pour réduire le temps d'analyse des fichiers EFS HP ProtectTools, l'utilisateur peut soit entrer le mot de passe de chiffrement avant l'analyse, soit déchiffrer les fichiers avant de les analyser.<br><br>Pour minimiser le temps de chiffrement/déchiffrement des données à l'aide du système EFS de la sécurité intégrée HP ProtectTools, l'utilisateur doit désactiver la protection automatique de Symantec Antivirus ou Norton Antivirus. |
| Le stockage de l'archive de récupération d'urgence sur un support amovible n'est pas pris en charge. | Si l'utilisateur insère une carte mémoire MMC ou SD lors de la création du chemin d'accès au fichier d'archives pendant l'initialisation de la sécurité intégrée, un message d'erreur s'affiche. | Le système est ainsi conçu.<br><br>Le stockage de l'archive de récupération sur un support amovible n'est pas pris en charge. L'archive de récupération peut être stockée sur un disque réseau ou sur un disque dur local autre que l'unité C. |
| Impossible de chiffrer des données dans l'environnement Windows 2000 en version française (France). | Le menu contextuel affiché par un clic droit sur l'icône d'un fichier ne présente pas d'option de chiffrement. | Il s'agit d'une limitation du système d'exploitation Microsoft. Si une autre option régionale est sélectionnée (par exemple, français [Canada]), l'option **Chiffrer** apparaît.<br><br>Pour contourner le problème, procédez au chiffrement du fichier comme suit : cliquez avec le bouton droit sur l'icône du fichier et sélectionnez **Propriétés > Avancées > Chiffrer le contenu**. |
| Des erreurs se produisent après une coupure de courant survenue pendant la prise de possession lors de l'initialisation de la sécurité intégrée. | Si une coupure de courant se produit pendant l'initialisation de la puce de sécurité intégrée, les problèmes suivants apparaissent :<br><br>• Lorsque vous tentez de lancer l'assistant d'initialisation de la sécurité intégré, vous obtenez le message d'erreur **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner** (La sécurité intégrée ne peut pas être initialisée car le propriétaire de la puce de sécurité intégrée est déjà défini).<br><br>• Lorsque vous tentez de lancer l'assistant d'initialisation de l'utilisateur, vous obtenez le message d'erreur **The Embedded security is not initialized.** (La sécurité intégrée n'est pas initialisée.) **To use the wizard, the Embedded Security must be initialized first.** (Pour pouvoir utiliser l'Assistant, la sécurité intégrée doit être initialisée.) | Pour restaurer l'état normal après une coupure de courant, procédez comme suit :<br><br>**REMARQUE :** Utilisez les touches de direction pour sélectionner différents menus, leurs options, puis changez les valeurs (sauf si indiqué autrement).<br><br>1. Démarrez ou redémarrez l'ordinateur.<br><br>2. Appuyez sur la touche F10 lorsque le message **F10=Setup** apparaît à l'écran (ou dès que le voyant vert du moniteur s'allume).<br><br>3. Sélectionnez l'option de langue appropriée.<br><br>4. Appuyez sur Entrée.<br><br>5. Sélectionnez **Security** > **Embedded Security** (Sécurité > Sécurité intégrée).<br><br>6. Définissez l'option **Embedded Security Device** (Périphérique de sécurité intégrée) sur **Enable** (Activer).<br><br>7. Appuyez sur F10 pour accepter la modification.<br><br>8. Sélectionnez **File** > **Save Changes and Exit** (Fichier > Enregistrer les modifications et quitter).<br><br>9. Appuyez sur Entrée.<br><br>10. Appuyez sur F10 pour enregistrer les modifications et quitter l'utilitaire Setup (F10). |

| Brève description | Détails | Solution |
|---|---|---|
| Le mot de passe de l'utilitaire Computer Setup (F10) peut être supprimé après l'activation du module TPM. | L'activation du module TPM requiert un mot de passe Computer Setup (F10). Une fois le module TPM activé, l'utilisateur peut supprimer le mot de passe. Cela permet à n'importe qui d'accéder directement au système pour réinitialiser le module TPM avec une perte possible de données. | Le système est ainsi conçu.<br><br>Le mot de passe de l'utilitaire Computer Setup (F10) ne peut être supprimé que par un utilisateur connaissant ce mot de passe. Il est toutefois vivement recommandé de protéger en permanence l'utilitaire Computer Setup (F10) par un mot de passe. |
| La boîte de dialogue de mot de passe de l'unité PSD ne s'affiche plus lorsque le système sort d'un mode veille. | Lorsqu'un utilisateur ouvre une session sur le système après avoir créé une unité PSD, le module TPM lui demande le mot de passe utilisateur de base. Si l'utilisateur n'entre pas le mot de passe et que le système passe en mode veille, la boîte de dialogue de mot de passe n'est plus disponible lorsque le système sort du mode veille. | Le système est ainsi conçu.<br><br>L'utilisateur doit fermer sa session et en ouvrir une nouvelle pour accéder de nouveau à la boîte de dialogue de mot de passe. |
| Aucun mot de passe n'est requis pour modifier les règles de la plate-forme de sécurité. | L'accès aux règles de la plate-forme de sécurité (machine et utilisateur) ne requiert pas de mot de passe TPM pour les utilisateurs qui ont des droits d'administrateur sur le système. | Le système est ainsi conçu.<br><br>Tout administrateur peut modifier les règles de la plate-forme de sécurité avec ou sans initialisation TPM. |
| Microsoft EFS ne fonctionne pas intégralement sous Windows 2000. | Un administrateur peut accéder aux informations chiffrées du système sans connaître le mot de passe correct. Si l'administrateur saisit un mot de passe incorrect ou annule la boîte de dialogue de mot de passe, le fichier chiffré s'ouvre comme si l'administrateur avait saisi correctement le mot de passe. Cela se produit quels que soient les paramètres de sécurité utilisés lors du chiffrement des données. Ceci se produit uniquement dans le premier compte administrateur sous Windows 2000. | La règle de restauration des données est automatiquement configurée de manière à désigner un administrateur comme agent de restauration. Lorsqu'une clé d'utilisateur ne peut pas être récupérée (comme dans le cas d'un mot de passe incorrect ou de l'annulation de la boîte de dialogue de saisie du mot de passe), le fichier est automatiquement déchiffré à l'aide de la clé de restauration.<br><br>Il s'agit d'une particularité du système EFS de Microsoft. Pour plus d'informations, reportez-vous à l'article Q257705 de la Base de connaissances de Microsoft à l'adresse http://www.microsoft.com.<br><br>Les documents ne peuvent pas être ouverts par un utilisateur qui ne possède pas de droits d'administrateur. |
| Lors de la consultation d'un certificat, celui-ci n'apparaît pas comme certificat de confiance. | Une fois HP ProtectTools installé et après avoir exécuté l'Assistant d'initialisation, l'utilisateur peut consulter le certificat émis ; ce certificat n'apparaît cependant pas comme certificat de confiance. Bien qu'il puisse être installé en cliquant sur le bouton Installer, l'installation n'en fait pas un certificat de confiance. | Les certificats auto-signés ne sont pas des certificats de confiance. Dans un environnement d'entreprise convenablement configuré, les certificats EFS de confiance sont émis en ligne par des autorités de certification. |
| Erreurs intermittentes de chiffrement et de déchiffrement : **Le processus ne peut pas accéder au fichier parce qu'il est utilisé par un autre processus.** | Une erreur extrêmement rare se produit pendant le chiffrement ou le déchiffrement, indiquant que le fichier est utilisé par un autre processus, alors que ce fichier ou dossier n'est pas traité par le système d'exploitation ou une application. | Pour résoudre ce problème :<br><br>1. Redémarrez le système.<br><br>2. Déconnectez-vous.<br><br>3. Connectez-vous à nouveau. |
| Une perte de données sur un support amovible se produit si le support est retiré avant un transfert ou une nouvelle génération de données. | Après le retrait d'un support de stockage tel qu'un disque dur MultiBay, le système indique toujours la disponibilité de l'unité PSD et ne génère par d'erreur lors de l'ajout ou de la modification de données sur l'unité PSD. Après redémarrage du système, l'unité PSD ne reflète pas les | Ce problème ne se rencontre que si l'utilisateur accède à l'unité PSD, puis retire le disque dur avant la fin d'un transfert ou de la génération de nouvelles données. Si l'utilisateur tente d'accéder à l'unité PSD alors que le disque dur n'est pas présent, un message d'erreur s'affiche indiquant que **le périphérique n'est pas prêt**. |

| Brève description | Détails | Solution |
|---|---|---|
| | modifications apportées dans les fichiers après son retrait. | |
| Lors de la désinstallation, si l'utilisateur ouvre l'outil Administration sans avoir initialisé la clé utilisateur de base, l'option **Disable** (Désactiver) n'est pas disponible et le programme de désinstallation s'arrête tant que l'outil Administration n'est pas refermé. | L'utilisateur a la possibilité de désactiver ou non le module TPM (à l'aide de l'outil Administration) avant de procéder à la désinstallation. L'accès à l'outil Administration requiert l'initialisation de la clé utilisateur de base. Si l'initialisation de base n'est pas faite, l'utilisateur ne peut accéder à aucune option.<br><br>Comme l'utilisateur a explicitement choisi d'ouvrir l'outil Admin (en cliquant sur **Yes** (Oui) à l'invite **Click Yes to open Embedded Security Administration tool**) (Cliquez sur Oui pour ouvrir l'outil d'administration de la sécurité intégrée), le programme de désinstallation attend que l'outil Admin soit refermé. Si l'utilisateur clique sur **No** (Non), l'outil Admin ne s'ouvre pas du tout et la désinstallation se poursuit. | L'outil Admin permet de désactiver la puce TPM, mais cette option n'est pas disponible tant que la clé utilisateur de base n'est pas initialisée. Si c'est le cas, sélectionnez **OK** ou **Cancel** (Annuler) pour poursuivre la désinstallation. |
| Blocage intermittent du système après avoir créé une unité PSD sur 2 comptes utilisateur et utilisé le changement rapide d'utilisateur dans des systèmes à 128 Mo. | Lors du changement rapide d'utilisateur avec un minimum de mémoire, le système peut se bloquer sur un écran noir et ne répond plus au clavier ni à la souris, au lieu d'afficher l'écran d'accueil (ouverture de session). | La cause première soupçonnée est un problème de top horloge dans les configurations à minimum de mémoire.<br><br>L'adaptateur graphique intégré utilise une architecture UMA qui se réserve 8 Mo de mémoire en ne laissant que 120 Mo à l'utilisateur. Ces 120 Mo sont partagés par deux utilisateurs qui ont ouvert une session et qui sont en cours de changement rapide au moment où l'erreur s'est produite.<br><br>La solution de rechange consiste à redémarrer le système ; il est ensuite vivement conseillé d'augmenter la taille de la mémoire (HP ne livre pas de configurations à 128 Mo avec des modules de sécurité). |
| L'authentification de l'utilisateur par le système EFS (demande de mot de passe) dépasse la limite de temps avec le message **access denied** (accès refusé). | La boîte de dialogue EFS d'authentification de l'utilisateur s'ouvre de nouveau après avoir cliqué sur **OK** ou lorsque l'état normal est restauré après une mise en veille. | Le système est ainsi conçu. Pour éviter tout problème avec le système EFS de Microsoft, une minuterie de surveillance de 30 secondes est activée pour générer le message d'erreur. |
| La description fonctionnelle est légèrement tronquée pendant l'installation japonaise. | Les descriptions fonctionnelles sont tronquées lors de l'installation personnalisée à l'aide de l'Assistant d'installation. | Ce problème sera résolu par HP dans une prochaine version. |
| Le chiffrement EFS fonctionne sans entrer de mot de passe à l'invite. | Par un dépassement de temps de l'invite du mot de passe utilisateur, le chiffrement d'un fichier ou d'un dossier est toujours possible. | Cette possibilité de chiffrement ne requiert pas de mot de passe d'authentification, car il s'agit d'une particularité du système EFS de Microsoft. Pour le déchiffrement, il sera toutefois nécessaire de fournir le mot de passe utilisateur. |
| La messagerie sécurisée est prise en charge, même si cette option n'est pas cochée dans l'Assistant d'initialisation ou si la configuration de la messagerie sécurisée est | Le logiciel de sécurité intégrée et l'Assistant ne vérifient pas le paramétrage d'un client de messagerie (Outlook, Outlook Express ou Netscape). | Ce comportement découle de la conception. La configuration des paramètres de messagerie TPM n'interdit pas l'édition de paramètres de chffrement dans le client de messagerie. L'utilisation d'une messagerie sécurisée est définie et contrôlée par des applications de partie tierce. L'assistant HP autorise la liaison aux trois applications de référence pour une personnalisation immédiate. |

| Brève description | Détails | Solution |
|---|---|---|
| désactivée dans les règles de l'utilisateur. | | |
| L'exécution d'un déploiement à grande échelle pour une seconde fois sur le même ordinateur, ou sur un ordinateur précédemment initialisé, remplace les fichiers de secours et de restauration d'urgence des clés. Les nouveaux fichiers sont inutilisables pour une restauration. | L'exécution d'un déploiement à grande échelle sur tout système initialisé avec un module de sécurité intégrée HP ProtectTools rend inutilisables les fichiers de restauration xml en les remplaçant par d'autres. | HP s'efforce de résoudre ce problème de remplacement des fichiers xml et fournira une solution dans un prochain SoftPaq. |
| Les scripts d'ouverture de session automatique ne fonctionnent pas pendant la restauration de l'utilisateur dans la sécurité intégrée. | L'erreur se produit après avoir<br>• initialisé le propriétaire et l'utilisateur dans la sécurité intégrée (à l'aide des emplacements par défaut **Mes documents**),<br>• restauré les paramètres par défaut du BIOS du module TPM,<br>• redémarré l'ordinateur,<br>• commencé à restaurer la sécurité intégrée. Pendant le processus de restauration, l'utilitaire Credential Manager demande à l'utilisateur si le système peut automatiser l'ouverture de session sur « Infineon TPM User Authentication ». Si l'utilisateur choisit **Yes** (Oui), l'emplacement SPEmRecToken apparaît automatiquement dans la zone de texte.<br>Bien que cet emplacement soit correct, le message d'erreur suivant s'affiche : **No Emergency Recovery Token is provided.** (Aucun jeton de récupération d'urgence fourni.) **Select the token location the Emergency Recovery Token should be retrieved from.** (Sélectionnez l'emplacement à partir duquel il doit être récupéré.) | Cliquez sur le bouton **Parcourir** pour sélectionner l'emplacement. Le processus de restauration continue. |
| Les unités PSD de plusieurs utilisateurs ne fonctionnent pas dans un environnement à changement rapide d'utilisateur. | Cette erreur se produit lorsque plusieurs utilisateurs ont été définis et ont reçu une unité PSD identifiée par la même lettre. Lorsqu'un changement rapide d'utilisateur a lieu, une unité PSD étant chargée, l'unité PSD du second utilisateur n'est plus accessible. | L'unité PSD du second utilisateur ne sera de nouveau disponible que si elle est reconfigurée avec une autre lettre d'unité ou si le premier utilisateur ferme sa session. |
| L'unité PSD est désactivée et ne peut pas être supprimée après formatage du disque dur sur lequel elle a été créée. | L'unité PSD est désactivée et ne peut pas être supprimée après formatage du disque dur secondaire sur lequel elle a été créée. L'icône PSD est toujours visible, mais le message **unité de disque inaccessible** s'affiche lorsque l'utilisateur tente d'accéder à l'unité PSD. | Le système est ainsi conçu : si un utilisateur force la suppression ou se déconnecte de l'emplacement de stockage des données PSD, l'émulation d'unité PSD de la sécurité intégrée continue de fonctionner et génère des erreurs par perte de liaison aux données manquantes. |

| Brève description | Détails | Solution |
|---|---|---|
| | L'utilisateur ne parvient pas à supprimer l'unité PSD et obtient le message : **your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process** (votre unité PSD est en cours d'utilisation, veuillez vous assurer qu'elle ne contient pas de fichiers ouverts et qu'elle n'est pas utilisée par un autre processus). L'utilisateur doit redémarrer le système afin que l'unité PSD soit supprimée et ne soit plus rechargée après le redémarrage. | Solution : après le redémarrage suivant, l'émulation PSD échoue et l'utilisateur peut supprimer l'ancienne émulation PSD et en créer une nouvelle. |
| Une erreur interne a été détectée lors d'une restauration à partir du fichier de sauvegarde automatique. | Si l'utilisateur<br>• Clique sur l'option **Restore under Backup** (Restaurer sous sauvegarde) du logiciel Embedded Security dans HPPTSM, pour effectuer une restauration à partir de la sauvegarde automatique.<br>• Sélectionne **SPSystemBackup .xml**.<br>L'Assistant de restauration échoue et le message d'erreur suivant s'affiche : **The selected Backup Archive does not match the restore reason.** (Le fichier de sauvegarde ne correspond pas au motif de restauration). **Please select another archive and continue.** (Sélectionnez un autre fichier de sauvegarde et poursuivez.) | Si l'utilisateur sélectionne le fichier **SpSystemBackup.xml** est requis, l'Assistant Embedded Security échoue et affiche le message : **An internal Embedded Security error has been detected.** (Une erreur interne a été détectée dans la sécurité intégrée.)<br>L'utilisateur doit alors sélectionner le fichier .xml correct qui correspond au motif de restauration.<br>Les processus fonctionnent convenablement tels qu'ils ont été conçus ; le message d'erreur interne de la sécurité intégrée n'est toutefois pas clair et devrait être précisé. HP s'occupe de cette amélioration pour les futures versions. |
| Erreur de restauration du système de sécurité avec plusieurs utilisateurs. | Pendant le processus de restauration, si l'administrateur sélectionne les utilisateurs à restaurer, ceux qui ne sont pas sélectionnés ne peuvent plus ultérieurement restaurer les clés. Un message d'erreur s'affiche indiquant l'**échec du processus de déchiffrement**. | Les utilisateurs non sélectionnés peuvent être restaurés en réinitialisant le module TPM, puis en exécutant la restauration et en sélectionnant tous les utilisateurs avant que la prochaine sauvegarde automatique journalière ne s'exécute. Si cette sauvegarde automatique a lieu, elle remplace les utilisateurs non restaurés et leurs données sont perdues. Si une nouvelle sauvegarde du système est stockée, les utilisateurs précédemment non sélectionnés ne peuvent plus être restaurés.<br>De plus, l'utilisateur doit restaurer la sauvegarde système dans son ensemble. Une sauvegarde d'archives peut être individuellement restaurée. |
| La restauration de la ROM système sur les paramètres par défaut masque le module TPM. | Lorsque les valeurs par défaut de la ROM système sont restaurées, le module TPM n'est plus visible dans Windows. Il en résulte que le logiciel de sécurité intégrée ne fonctionne plus convenablement et que les données chiffrées par le module TPM ne sont plus accessibles. | Réactivez le module TPM dans le BIOS :<br>Ouvrez l'utilitaire Computer Setup (F10), naviguez vers **Security** > **Device security** (Sécurité > Sécurité des périphériques), changez l'option **Hidden** (Masqué) en **Available** (Disponible). |
| La sauvegarde automatique ne fonctionne pas avec une unité mappée. | Lorsqu'un administrateur configure la sauvegarde automatique dans la sécurité intégrée, il crée une entrée dans **Windows** > **Tâches** > **Tâches planifiées**. La tâche planifiée dans Windows est définie de manière à utiliser les droits de NT AUTHORITY\ SYSTEM pour l'exécution de la sauvegarde. Cela | La solution de rechange consiste à changer NT AUTHORITY\SYSTEM en (nom_ordinateur \ (nom_administrateur). Il s'agit de la configuration par défaut lorsque la tâche planifiée est créée manuellement.<br>Dans les prochaines versions du logiciel, HP prévoira d'inclure [nom_ordinateur/nom_administrateur] comme paramétrage par défaut. |

| Brève description | Détails | Solution |
| --- | --- | --- |
| | fonctionne convenablement sur n'importe quelle unité locale.<br><br>En revanche, si l'administrateur configure la sauvegarde automatique sur une unité mappée, le processus échoue parce que NT AUTHORITY\SYSTEM ne dispose pas des droits permettant l'utilisation d'une unité mappée.<br><br>Si l'exécution de la sauvegarde automatique est planifiée à l'ouverture de session, l'icône TNA de la sécurité intégrée affiche le message suivant : **The Backup Archive location is currently not accessible.** (L'emplacement de l'archive de sauvegarde n'est pas accessible actuellement.) **Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** (Cliquez ici si vous désirez créer un fichier de sauvegarde temporaire jusqu'à ce que l'archive de sauvegarde soit de nouveau accessible.) Si la sauvegarde automatique est planifiée à une heure spécifique, elle échoue sans que cet échec soit annoncé. | |
| Impossible de désactiver temporairement l'état de la sécurité intégrée dans l'interface graphique du logiciel. | La version actuelle 4.0 du logicielle a été conçue pour les portables HP Notebook 1.1B, ainsi que pour les ordinateurs de bureau HP Desktop 1.2.<br><br>Cette option de désactivation est toujours prise en charge dans l'interface du logiciel pour les plates-formes TPM 1.1. | Ce problème sera résolu par HP dans les prochaines versions. |

# Divers

| Logiciel affecté — Brève description | Détails | Solution |
|---|---|---|
| HP ProtectTools Security Manager — message d'avertissement : **The security application can not be installed until the HP Protect Tools Security Manager is installed** (L'application de sécurité ne peut pas être installée tant que le logiciel HP Protect Tools Security Manager n'est pas installé) | Toutes les applications de sécurité comme la sécurité intégrée et les périphériques à carte Java ou biométriques sont des applications additionnelles de l'interface HP Security Manager. Le logiciel HP Security Manager doit donc être installé avant de pouvoir charger une application additionnelle approuvée par HP. | Le logiciel HP ProtectTools Security Manager doit être installé avant d'installer une quelconque application d'extension. |
| Utilitaire de mise à jour du microprogramme HP ProtectTools TPM pour modèles dc7600 et modèles contenant un module TPM Broadcom. — L'outil mis à disposition sur le site Web HP signale **ownership required** (possession requise). | Il s'agit d'un comportement attendu de l'utilitaire du microprogramme TPM pour les modèles dc7600 et ceux contenant un module TPM Broadcom.<br><br>L'outil de mise à jour permet à l'utilisateur de mettre à jour le microprogramme avec ou sans clé d'autorisation (EK). Lorsqu'il n'y a pas de clé, aucune autorisation n'est requise pour accomplir la mise à jour du microprogramme.<br><br>Lorsqu'il y a une clé d'autorisation, le propriétaire du module TPM doit exister, étant donné que la mise à jour requiert son autorisation. Une fois la mise à jour réussie, la plate-forme doit être redémarrée pour que le nouveau microprogramme prenne effet.<br><br>Si les paramètres par défaut du BIOS du module TPM sont restaurés, la possession est supprimée et il n'est plus possible de mettre à jour le microprogramme tant que la plate-forme et l'utilisateur n'ont pas été configurés dans l'Assistant d'initialisation.<br><br>*Un redémarrage est toujours recommandé après une mise à jour du microprogramme. La version du microprogramme n'est correctement détectée qu'après redémarrage. | 1. Réinstallez le logiciel HP ProtectTools Embedded Security.<br><br>2. Exécutez l'assistant de configuration de la plate-forme et de l'utilisateur.<br><br>3. Vérifiez que Microsoft .NET Framework 1.1 est installé sur le système :<br><br>**a.** Cliquez sur **Démarrer**.<br><br>**b.** Cliquez sur **Panneau de configuration**.<br><br>**c.** Cliquez sur **Ajout ou suppression de programmes**.<br><br>**d.** Vérifiez que **Microsoft .NET Framework 1.1** figure dans la liste des programmes.<br><br>4. Vérifiez la configuration matérielle et logicielle :<br><br>**a.** Cliquez sur **Démarrer**.<br><br>**b.** Cliquez sur **Tous les programmes**.<br><br>**c.** Cliquez sur **HP ProtectTools Security Manager**.<br><br>**d.** Sélectionnez **Embedded Security** (Sécurité intégrée) dans le menu d'arborescence.<br><br>**e.** Cliquez sur **More Details** (Détails). Le système devrait présenter la configuration suivante :<br><br>• Product version (Version de produit) = V4.0.1<br><br>• Embedded Security State (État de la sécurité intégrée) : Chip State (Puce) = Enabled (Activée), Owner State (Propriétaire) = Initialized (Initialisé), User State (Utilisateur) = Initialized (Initialisé)<br><br>• Component Info (Info composants) : TCG Spec. Version = 1.2<br><br>• Vendor (Fabricant) = Broadcom Corporation |

| Logiciel affecté — Brève description | Détails | Solution |
|---|---|---|
| | | • FW Version (Version microprog.) = 2.18 (ou ultérieure)<br>• TPM Device driver library version (Version de la bibliothèque de drivers de périphériques TPM) = 2.0.0.9 (ou ultérieure)<br>5. Si la version du microprogramme ne correspond pas à 2.18, téléchargez et mettez à jour le microprogramme du module TPM. Le SoftPaq de mise à jour du microprogramme TPM est disponible sur le site http://www.hp.com. |
| Une erreur se produit parfois lors de la fermeture de l'interface du Security Manager. | Occasionnellement (1 fois sur 12) une erreur se produit en cliquant sur l'icône de fermeture dans l'angle supérieur droit de la fenêtre du Security Manager avant que le chargement des applications additionnelles soit terminé. | Ce problème est en relation avec le temps de chargement des applications additionnelles lors de la fermeture et du redémarrage du Security Manager. Étant donné que PTHOST.exe est le programme principal couvrant les autres applications additionnelles, il dépend du temps de chargement des autres applications (services). Le fait de fermer le programme principal avant qu'un service soit complètement chargé est la cause première de l'erreur.<br><br>Pour résoudre le problème, attendez que le message (en haut de la fenêtre) indique que les services sont chargés et que ceux-ci soient affichés dans la colonne de gauche. Pour éviter toute défaillance, patientez un temps raisonnable pour permettre le chargement des services. |
| HP ProtectTools * En général— Un accès illimité ou des privilèges d'administration non contrôlés posent un risque pour la sécurité. | Divers risques sont possibles lorsque l'accès au PC client est illimité :<br>• suppression de l'unité PSD<br>• modification malveillante des paramètres utilisateur<br>• désactivation des règles et des fonctions de sécurité | Il est conseillé aux administrateurs d'appliquer des règles de bonne pratique pour limiter les privilèges et l'accès des utilisateurs finaux.<br><br>Des privilèges d'administration ne devraient pas être accordés à des utilisateurs non autorisés. |
| Les mots de passe de sécurité intégrée et du BIOS ne sont pas synchronisés. | Si l'utilisateur ne valide pas un nouveau mot de passe en tant que mot de passe de sécurité intégrée du BIOS, le mot de passe de sécurité intégrée du BIOS est restauré sur le mot de passe de sécurité intégrée d'origine via F10 BIOS. | Ceci fonctionne comme conçu ; ces mots de passe peuvent être resynchronisés en modifiant le mot de passe utilisateur de base et en l'authentifiant à l'invite du mot de passe de sécurité intégrée du BIOS. |
| Un seul utilisateur peut se connecter au système une fois que l'authentification de préamorçage TPM est activée dans le BIOS. | Le numéro PIN du BIOS du module TPM est associé au premier utilisateur qui initialise le paramètre d'utilisateur. Si un ordinateur a plusieurs utilisateurs, le premier utilisateur est, par principe, l'administrateur. Le premier utilisateur devra donner son numéro PIN d'utilisateur TPM aux autres utilisateurs afin de se connecter. | Ceci fonctionne comme conçu ; HP recommande que le service informatique du client suive de bonnes stratégies de sécurité pour le déploiement de sa solution de sécurité et s'assure que le mot de passe administrateur du BIOS est configuré par des administrateurs informatiques pour une protection au niveau du système. |
| L'utilisateur doit modifier son numéro PIN pour que le préamorçage TPM fonctionne après une réinitialisation usine du module TPM. | L'utilisateur doit modifier son numéro PIN ou créer un autre utilisateur pour initialiser ce paramètre utilisateur pour que l'authentification BIOS TPM fonctionne après une réinitialisation. Il n'existe aucune option qui permette de rendre l'authentification BIOS TPM fonctionnelle. | Le système est ainsi conçu et la réinitialisation usine efface la clé utilisateur de base. L'utilisateur doit modifier son numéro PIN ou créer un nouvel utilisateur pour réinitialiser la clé utilisateur de base. |

| Logiciel affecté — Brève description | Détails | Solution |
|---|---|---|
| La **prise en charge d'authentification à la mise sous tension** n'est pas définie pour utiliser par défaut l'option **Reset to Factory Settings** (Restaurer les paramètres usine) de la sécurité intégrée. | Dans Computer Setup, la **prise en charge d'authentification à la mise sous tension** n'est pas réinitialisée sur les paramètres usine lors de l'utilisation de l'option de périphérique de sécurité intégrée **Reset to Factory Settings** (Restaurer les paramètres usine). Par défaut, la **prise en charge d'authentification à la mise sous tension** est définie sur **Disable** (Désactiver). | L'option **Reset to Factory Settings** (Restaurer les paramètres usine) désactive le périphérique de sécurité intégrée, qui masque les autres options de sécurité intégrée (y compris la **prise en charge d'authentification à la mise sous tension**). Toutefois, suite à la réactivation du périphérique de sécurité intégrée, la **prise en charge d'authentification à la mise sous tension** restait activée.<br><br>HP s'efforce de trouver une solution, qui sera fournie dans un prochain SoftPaq de ROM de type Web. |
| L'authentification à la mise sous tension de la sécurité chevauche le mot de passe BIOS durant la séquence d'amorçage. | L'authentification à la mise sous tension invite l'utilisateur à se connecter au système à l'aide du mot de passe TPM mais, si l'utilisateur appuie sur la touche F10 pour accéder au BIOS, seul un accès en lecture est octroyé. | Pour pouvoir écrire vers le BIOS, l'utilisateur doit entrer le mot de passe BIOS au lieu du mot de passe TPM dans la fenêtre de prise en charge d'authentification à la mise sous tension. |
| Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après la modification du mot de passe propriétaire dans le logiciel Windows de sécurité intégrée. | Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après la modification du mot de passe propriétaire dans le logiciel Windows de sécurité intégrée. | Le système est ainsi conçu. Ceci est dû à l'incapacité du BIOS à communiquer avec le module TPM, une fois le système d'exploitation démarré et exécuté, et à vérifier la phrase de passe TPM par rapport au blob de clé TPM. |

# Glossaire

**Archive de restauration d'urgence** Zone de stockage protégée qui permet le recryptage de clés utilisateur de base d'une clé de propriétaire de plateforme à une autre.

**Authentification** Processus permettant de vérifier si un utilisateur est autorisé à effectuer une tâche, telle que l'accès à un ordinateur, la modification de paramètres d'un programme spécifique ou l'affichage de données sécurisées.

**Authentification de mise sous tension** Fonction de sécurité qui requiert une certaine forme d'authentification, telle qu'une Java Card, une puce de sécurité ou un mot de passe, lors la mise sous tension de l'ordinateur.

**Authentification unique** Fonction qui stocke des informations d'authentification et qui permet d'utiliser le module Credential Manager pour accéder à des applications Internet et Windows qui requièrent une authentification par mot de passe.

**Autorité de certification** Service qui émet les certificats requis pour exécuter une infrastructure de clés publiques.

**Biométrie** Catégorie d'informations d'authentification qui utilisent une caractéristique physique, telle qu'une empreinte digitale, pour identifier un utilisateur.

**Certificat numérique** Informations d'authentification électroniques qui confirment l'identité d'un individu ou d'une société en reliant l'identité du propriétaire du certificat numérique à une paire de clés électroniques utilisées pour signer des informations numériques.

**Compte réseau** Compte d'utilisateur ou d'administrateur Windows, sur un ordinateur local, dans un groupe de travail ou sur un domaine.

**Compte utilisateur Windows** Profil d'un individu autorisé à se connecter à un réseau ou à un ordinateur individuel.

**Cryptage** Procédure, telle que l'utilisation d'un algorithme, employée en cryptographie pour convertir un texte normal en un texte chiffré afin d'empêcher la lecture des données par des destinataires non autorisés. Il existe plusieurs types de cryptage de données, qui forment la base de la sécurité du réseau. Les types courants incluent DES (Data Encryption Standard) et le cryptage de clés publiques.

**Cryptographie** Pratique de cryptage et décryptage de données afin qu'elles ne puissent être décodées que par des individus spécifiques.

**Décryptage** Procédure utilisée en cryptographie pour convertir des données cryptées en un texte normal.

**Domaine** Groupe d'ordinateurs qui font partie d'un réseau et qui partagent une base de données de répertoires communs. Chaque domaine possède un nom unique et dispose d'un ensemble de règles et procédures communes.

**DriveLock** Fonction de sécurité qui relie le disque dur à un utilisateur et qui requiert que ce dernier saisisse correctement le mot de passe DriveLock au démarrage de l'ordinateur.

**EFS (Encryption File System)** Système qui crypte tous les fichiers et sous-dossiers au sein du dossier sélectionné.

**Fournisseur de service cryptographique** Fournisseur ou bibliothèque d'algorithmes cryptographiques qui peut être utilisé(e) dans une interface proprement définie pour exécuter des fonctions cryptographiques spécifiques.

**Identité** Dans l'utilitaire HP ProtectTools Credential Manager, groupe d'informations d'authentification et de paramètres qui est traité comme un compte ou un profil pour un utilisateur donné.

**Informations d'identification** Méthode par laquelle un utilisateur prouve son éligibilité pour une tâche donnée dans le processus d'authentification.

**Infrastructure de clés publiques (PKI)** Norme qui définit les interfaces pour la création, l'utilisation et l'administration de certificats et de clés cryptographiques.

**Java Card** Petite pièce de matériel, de mêmes taille et forme qu'une carte bancaire, qui stocke des informations d'identification concernant le propriétaire. Utilisée pour authentifier le propriétaire sur un ordinateur.

**Jeton USB** Périphérique de sécurité qui stocke des informations d'identification concernant un utilisateur. Comme une Java Card ou un lecteur biométrique, il peut être utilisé pour authentifier le propriétaire sur un ordinateur.

**Jeton virtuel** Fonction de sécurité dont le fonctionnement est très similaire à celui d'une Java Card et d'un lecteur de carte. Le jeton est enregistré sur le disque dur de l'ordinateur ou dans le registre Windows. Lorsque vous vous connectez à l'aide d'un jeton virtuel, vous êtes invité à fournir un code PIN d'utilisateur pour effectuer l'authentification.

**Lecteur sécurisé personnel** Fournit une zone de stockage protégée pour des informations confidentielles.

**Migration** Tâche qui permet la gestion, la restauration et le transfert de clés et de certificats.

**Mode de sécurité du BIOS** Paramètre de sécurité de Java Card qui, lorsqu'il est activé, requiert l'utilisation d'une Java Card et d'un code PIN valide pour l'authentification de l'utilisateur.

**Partition FAT** File Allocation Table (tableau d'allocation de fichier), méthode d'indexation de supports de stockage.

**Partition NTFS** NT File System (Système de fichiers NT), méthode d'indexation de supports de stockage. Il s'agit de la méthode standard sous Windows Vista et Windows XP.

**Profil BIOS** Groupe de paramètres de configuration du BIOS qui peut être enregistré et appliqué à d'autres comptes.

**Puce de sécurité intégrée TPM (Trusted Platform Module) (certains modèles)** Puce de sécurité intégrée qui peut protéger des informations utilisateur hautement confidentielles contre des attaques malveillantes. Il s'agit de la racine de confiance dans une plateforme donnée. Le module TPM fournit des opérations et algorithmes cryptographiques qui suivent les spécifications de l'organisme TCG (Trusted Computing Group).

**Réamorçage** Processus de redémarrage de l'ordinateur.

**Sécurité stricte** Fonction de sécurité dans la configuration du BIOS qui fournit une protection améliorée pour les mots de passe d'administrateur et de mise sous tension, ainsi que d'autres formes d'authentification à la mise sous tension.

**Signature numérique** Données transmises avec un fichier qui vérifient l'expéditeur du matériel et la non modification du fichier après sa signature.

**Smart Card** Petite pièce de matériel, de mêmes taille et forme qu'une carte bancaire, qui stocke des informations d'identification concernant le propriétaire. Utilisée pour authentifier le propriétaire sur un ordinateur.

# Index