ProtectTools

Manuel de l'utilisateur

© 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 contenues dans ce document peuvent être modifiées sans préavis. Les garanties relatives aux produits et aux services HP sont décrites dans les textes de garantie limitée expresse qui les accompagnent. Aucun élément du présent document ne peut être interprété comme constituant une garantie supplémentaire. HP ne saurait être tenu pour responsable des erreurs ou omissions de nature technique ou rédactionnelle qui pourraient subsister dans le présent document.

Première édition : Janvier 2007

Référence du document : 438371-051

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
- Device Access Manager 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 à partir du site Web HP. Visitez le site http://www.hp.com pour plus d'informations.

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. • 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. • 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. • 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. • Embedded Security permet la création d'un lecteur sécurisé personnel (PSD) pour la protection des données utilisateur. • 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. • 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. • BIOS Configuration permet d'effectuer les mêmes opérations que l'utilitaire de configuration BIOS au préamorçage (accessible via la touche de configuration f10). • DriveLock, dotée de la puce de sécurité intégrée, empêche tout accès non autorisé à un disque dur, même si ce dernier est enlevé pour être installé sur un autre système. L'utilisateur ne doit mémoriser que le mot de passe utilisateur de la puce de sécurité intégrée.

Module	Principales fonctions
Device Access Manager for HP ProtectTools	• Device Access Manager permet aux responsables des départements informatiques de contrôler l'accès aux périphériques en fonction de profils utilisateur. • Device Access Manager empêche les utilisateurs non autorisés de retirer des données à l'aide de supports de stockage externes et d'introduire des virus dans le système via des supports externes. • L'administrateur peut interdire l'accès aux périphériques inscriptibles à des utilisateurs ou à des groupes d'utilisateurs sélectionnés.
Drive Encryption for HP ProtectTools	• Drive Encryption permet un cryptage de disque dur complet au niveau du volume. • 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 20.”

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

Il y a par exemple vol ciblé si des données confidentielles et des informations client sont dérobées sur l'ordinateur d'un point de contrôle de sécurité dans un aéroport. Les fonctionnalités suivantes offrent une protection contre le vol ciblé :

- 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 53”
  - “Activation et désactivation de la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée page 54”
  - “Attribution d'un nom à une Java Card page 46”
  - “Drive Encryption for HP ProtectTools page 65”
- 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 automatique page 55”.
- 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 34”
  - “Utilisation du lecteur sécurisé personnel page 37”

Restriction de l'accès à des données confidentielles

Supposons qu'un auditeur, dans le cadre d'un travail de sous-traitance effectué sur site, se voit accorder l'accès à un ordinateur afin d'examiner des données financières stratégiques ; en pareil cas, vous

pouvez l'empêcher d'imprimer les fichiers ou de les enregistrer sur un support inscriptible tel qu'un CD. Les fonctionnalités suivantes permettent de restreindre l'accès aux données :

- Device Access Manager for HP ProtectTools permet aux responsables des départements informatiques de restreindre l'accès aux périphériques inscriptibles de façon à éviter que des informations confidentielles ne soient imprimées ou copiées du disque dur sur un support amovible. Reportez-vous à la section “Configuration de classes de périphériques (tâches avancées) page 62”.
- 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 automatique page 55”.

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 53”
  - “Activation et désactivation de la prise en charge de l'authentification à la mise sous tension pour la sécurité intégrée page 54”
  - “Attribution d'un nom à une Java Card page 46”
  - “Drive Encryption for HP ProtectTools page 65”
- 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 34”
  - “Utilisation du lecteur sécurisé personnel page 37”
- 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 14”
  - “Utilisation de la fonction d'authentification unique page 21”
- Device Access Manager for HP ProtectTools permet aux responsables des départements informatiques de restreindre l'accès aux périphériques inscriptibles de façon à éviter que des

informations confidentielles ne soient copiées depuis le disque dur. Reportez-vous à la section “Configuration simple page 61”.

- 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 34”
  - “Utilisation du lecteur sécurisé personnel page 37”

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 14”
- “Utilisation de la fonction d'authentification unique page 21”

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 34”

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: De nombreuses fonctions HP ProtectTools peuvent être personnalisées par le responsable de la sécurité en collaboration avec HP. Pour plus d'informations, consultez le site Web HP http://www.hp.com.

- 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 : • Il peut être utilisé en tant que connexion distincte pour accéder à Credential Manager après une connexion à Windows. • 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 HP ProtectTools	Défini dans ce module HP ProtectTools	Fonction
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 **REMARQUE:** Également appelé mot de passe de sécurité intégrée	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 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 **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. Authentifie les utilisateurs de Drive Encryption en cas de sélection du jeton Java Card.
Mot de passe Computer Setup **REMARQUE:** Également appelé mot de passe administrateur du BIOS, configuration f10 ou configuration de la 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 boîte 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 15.”
- 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 15.”

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: Cette procédure requiert un lecteur de carte configuré. Si vous ne disposez pas d'un lecteur installé, vous pouvez enregistrer un jeton virtuel, tel que décrit dans la section Création d'un jeton virtuel page 18.

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 29”.

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 16”.

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 29".

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 29."

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** (Autres > Options de l'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 29.”

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 de l'application à exporter. Cliquez ensuite sur **More > Applications > Export Script** (Autres > Applications > Script d'exportation).
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 de l'application à importer. Cliquez ensuite sur **More > Applications > Import Script** (Autres > Applications > Script d'importation).
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 boîte 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 20".

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 boîte 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/redémarrant l'ordinateur, puis appuyez sur f10 lorsque le message "F10 = ROM Based Setup" (F10 = Configuration ROM) s'affiche dans l'angle inférieur gauche de l'écran.
2. Si vous n'avez pas défini de mot de passe administrateur, utilisez les touches de direction pour sélectionner **Sécurité > Mot de passe de configuration**, puis appuyez sur entrée.
3. Entrez votre mot de passe dans les champs **Nouveau mot de passe** et **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 de sécurité intégrée.
8. Pour enregistrer vos préférences et quitter Computer Setup, utilisez les touches de direction pour sélectionner **Fichier > Enregistrer les modifications et quitter**. Suivez ensuite les instructions 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 Initialisation de l'utilisateur de la sécurité intégrée 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 **Sauvegarde**. L'Assistant de sauvegarde de Embedded Security for ProtectTools 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 **Restaurer**. L'Assistant de sauvegarde de Embedded Security for ProtectTools 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
- Sélection du lecteur de cartes

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 boîte 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 53".
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 boîte 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 boîte 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 10".

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

Le module BIOS Configuration permet de gérer divers paramètres d'ordinateur qui, sinon, seraient uniquement accessibles par pression sur la touche f10 au démarrage et à l'ouverture 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 56".

4. Dans le volet gauche, cliquez sur **Configuration système**.
5. Dans le volet droit, sélectionnez le délai (en secondes) des touches f9, f10 et f12, ainsi que la valeur du paramètre **Retard d'amorçage 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
     - Délai des touches f9, f10 et f12 (en secondes)
     - 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 automatique

Lorsque cette option est activée, les mots de passe DriveLock seront automatiquement générés et définis dans l'unité, et protégés par la puce de sécurité intégrée TPM.

REMARQUE: Les mots de passe automatiquement générés ne seront pas définis dans l'unité tant que l'ordinateur n'est pas redémarré et que vous n'avez pas entré le mot de passe de la sécurité intégrée TPM à l'invite de saisie du mot de passe.

L'option permettant d'activer la fonction Drivelock automatique n'est disponible que si une puce de sécurité TPM a été installée et initialisée sur l'ordinateur et si aucun mot de passe DriveLock n'est activé. Pour obtenir des instructions sur l'activation et l'initialisation de la puce de sécurité TPM, reportez-vous aux sections "Activation de la puce de sécurité intégrée page 34" et "Initialisation de la puce de sécurité intégrée page 35".

REMARQUE: Si vous avez déjà défini manuellement des mots de passe DriveLock sur l'ordinateur, vous devez d'abord les désactiver avant de pouvoir définir la protection DriveLock automatique.

Pour activer ou désactiver la protection DriveLock automatique :

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** en regard de **Prise en charge DriveLock automatique**.

   REMARQUE: Pour désactiver la prise en charge de la protection DriveLock automatique pour la sécurité intégrée, cliquez sur **Désactiver**.

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

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 boîte 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 boîte 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 boîte 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 Device Access Manager for HP ProtectTools

Cet outil de sécurité est disponible uniquement pour les administrateurs. Le module Device Access Manager for HP ProtectTools dispose des fonctions de sécurité suivantes qui fournissent une protection contre un accès non autorisé aux périphériques reliés à votre système informatique :

- Des profils de périphérique créés pour chaque utilisateur afin de définir l'accès aux périphériques
- Accès aux périphériques qui peut être octroyé ou refusé sur la base de l'appartenance à un groupe

Démarrage du service en arrière-plan

Pour pouvoir appliquer des profils de périphérique, le service en arrière-plan de verrouillage/audit de périphérique de HP ProtectTools doit être exécuté. Lorsque vous essayez pour la première fois d'appliquer des profils de périphérique, HP ProtectTools Security Manager affiche une boîte de dialogue qui vous invite à démarrer le service en arrière-plan. Cliquez sur **Oui** pour démarrer le service en arrière-plan et le configurer pour le démarrer automatiquement à l'amorçage du système.

Configuration simple

Cette fonction permet de refuser l'accès aux classes de périphériques suivantes :

- Périphériques USB pour tous les non administrateurs
- Tous les supports amovibles (disquettes, clé de mémoire USB, etc.) pour tous les non administrateurs
- Toutes les unités de DVD/CD-ROM pour tous les non administrateurs
- Tous les ports série et parallèle pour tous les non administrateurs

Pour refuser l'accès à une classe de périphérique pour tous les non administrateurs :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Configuration simple**.
3. Dans le volet droit, cochez la case d'un périphérique auquel refuser l'accès.
4. Cliquez sur **Appliquer**.

REMARQUE: Si le service en arrière-plan n'est pas en cours d'exécution, il essaie de démarrer maintenant. Cliquez sur **Oui** pour autoriser son exécution.

5. Cliquez sur **OK**.

Configuration de classes de périphériques (tâches avancées)

Des sélections supplémentaires sont disponibles pour permettre à des utilisateurs ou groupes d'utilisateurs spécifiques de se voir accorder ou refuser l'accès à des types de périphériques.

Ajout d'un utilisateur ou groupe

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Device Class Configuration** (Configuration de classes de périphériques).
3. Dans la liste de périphériques, cliquez sur la classe de périphériques à configurer.
4. Cliquez sur **Ajouter**. La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.
5. Sélectionnez **Advanced > Find Now** (Avancé > Rechercher maintenant) pour rechercher des utilisateurs ou groupes à ajouter.
6. Cliquez sur un utilisateur ou un groupe pour l'ajouter dans la liste des utilisateurs et groupes disponibles, puis cliquez sur **OK**.
7. Cliquez sur **OK**.

Suppression d'un utilisateur ou groupe

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Device Class Configuration** (Configuration de classes de périphériques).
3. Dans la liste de périphériques, cliquez sur la classe de périphériques à configurer.
4. Cliquez sur l'utilisateur ou groupe à supprimer, puis cliquez sur **Supprimer**.
5. Cliquez sur **Appliquer**, puis sur **OK**.

Refus d'accès à un utilisateur ou groupe

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Device Class Configuration** (Configuration de classes de périphériques).
3. Dans la liste de périphériques, cliquez sur la classe de périphériques à configurer.
4. Sous **User/Groups** (Utilisateur/Groupe), cliquez sur l'utilisateur ou groupe auquel refuser l'accès.
5. Cliquez sur **Deny** (Refuser) en regard de l'utilisateur ou groupe auquel refuser l'accès.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Octroi d'accès à une classe de périphérique pour un utilisateur d'un groupe

Vous pouvez autoriser un utilisateur à accéder à une classe de périphérique tout en refusant l'accès à tous les autres membres du groupe de cet utilisateur.

Pour autoriser l'accès à un utilisateur mais pas au groupe :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Device Class Configuration** (Configuration de classes de périphériques).
3. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer.
4. Sous **User/Groups** (Utilisateur/Groupe), ajoutez le groupe auquel refuser l'accès.
5. Cliquez sur **Deny** (Refuser) en regard du groupe auquel refuser l'accès.
6. Naviguez vers le dossier au-dessous de la classe requise et ajoutez l'utilisateur spécifique. Cliquez sur **Allow** (Autoriser) pour octroyer l'accès à cet utilisateur.
7. Cliquez sur **Appliquer**, puis sur **OK**.

Octroi d'accès à un périphérique spécifique pour un utilisateur d'un groupe

Vous pouvez autoriser un utilisateur à accéder à un périphérique spécifique tout en refusant l'accès à tous les autres membres du groupe de cet utilisateur pour tous les périphériques dans la classe.

Pour autoriser l'accès à un périphérique spécifique à un utilisateur mais pas au groupe :

1. Sélectionnez **Démarrer > Tous les programmes > HP ProtectTools Security Manager**.
2. Dans le volet gauche, cliquez sur **Device Access Manager**, puis sur **Device Class Configuration** (Configuration de classes de périphériques).
3. Dans la liste de périphériques, cliquez sur la classe de périphérique à configurer, puis naviguez vers le dossier au-dessous.
4. Sous **User/Groups** (Utilisateur/Groupe), ajoutez le groupe auquel refuser l'accès.
5. Cliquez sur **Deny** (Refuser) en regard du groupe auquel refuser l'accès.
6. Dans la liste de périphériques, naviguez vers le périphérique spécifique à autoriser pour l'utilisateur.
7. Cliquez sur **Ajouter**. La boîte de dialogue **Select Users or Groups** (Sélection d'utilisateurs ou groupes) s'affiche.
8. Sélectionnez **Advanced > Find Now** (Avancé > Rechercher maintenant) pour rechercher des utilisateurs ou groupes à ajouter.
9. Cliquez sur un utilisateur auquel octroyer l'accès, puis cliquez sur **OK**.
10. Cliquez sur **Allow** (Autoriser) pour octroyer l'accès à cet utilisateur.
11. Cliquez sur **Appliquer**, puis sur **OK**.

7 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 69"). 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 boîte 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.

8 Résolution de problèmes

Credential Manager for HP ProtectTools

Brève description	Détails	Solution
À l'aide de l'option Credential Manager Network Accounts (Comptes réseau Credential Manager), un utilisateur peut sélectionner le compte auquel se connecter dans le domaine. Lorsque l'authentification TPM est utilisée, cette option n'est pas disponible. Toutes les autres méthodes d'authentification fonctionnent normalement.	Avec l'authentification TPM, l'utilisateur est uniquement connecté à l'ordinateur local.	Avec les outils Credential Manager Single Sign On, l'utilisateur peut authentifier d'autres comptes.
Les informations d'authentification du jeton USB ne sont pas disponibles lors de la connexion à Windows XP Service Pack 1.	Après l'installation du logiciel du jeton USB, l'enregistrement des informations d'authentification du jeton USB et la définition de Credential Manager comme connexion principale, le jeton USB n'apparaît toujours pas et n'est pas disponible dans la connexion Credential Manager/GINA. Après ouverture d'une nouvelle session Windows, fermeture, puis réouverture de Credential Manager et resélection du jeton comme connexion primaire, la procédure de connexion se déroule normalement.	Effectuez la mise à jour de Windows vers le Service Pack 2 avec Windows Update. En cas de maintien du Service Pack 1, ouvrez une nouvelle session Windows en utilisant d'autres informations d'authentification (mot de passe Windows) afin de fermer, puis d'ouvrir à nouveau Credential Manager.
Certaines pages Web d'application créent des erreurs qui empêchent l'utilisateur d'exécuter ou de terminer des tâches.	Certaines applications Web arrêtent de fonctionner et signalent des erreurs dues à la désactivation du modèle d'authentification unique (SSO). Par exemple, un **!** dans un triangle jaune apparaît dans Internet Explorer, indiquant qu'une erreur est survenue.	La fonction d'authentification unique de Credential Manager ne prend pas en charge toutes les interfaces Web logicielles. Désactivez la prise en charge de l'authentification unique pour la page Web concernée. Reportez-vous à la documentation complète sur l'authentification unique, disponible dans les fichiers d'aide en ligne de Credential Manager. S'il n'est pas possible de désactiver l'authentification unique pour une application donnée, contactez l'assistance technique HP et demandez une assistance de niveau 3 au technicien HP.

Brève description	Détails	Solution
L'option **Browse for Virtual Token** (Rechercher un jeton virtuel) ne s'affiche pas pendant la procédure de connexion.	L'utilisateur ne peut pas accéder à l'emplacement contenant un jeton virtuel enregistré dans Credential Manager car l'option de navigation a été supprimée en vue de réduire les risques de sécurité.	L'option de navigation a été supprimée car elle permettait à des non utilisateurs de supprimer et de renommer des fichiers, puis de prendre le contrôle de Windows.
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 du compte d'un utilisateur du domaine à l'aide de l'option **Changement du mot de passe Windows**. Credential Manager peut uniquement modifier les mots de passe associés à des comptes sur des PC locaux. L'utilisateur de domaine peut modifier son mot de passe à l'aide de l'option **Sécurité Windows > Modifier le mot de passe**, mais l'utilisateur de domaine n'ayant pas de compte physique sur le PC local, Credential Manager peut uniquement modifier le mot de passe qui sert à la connexion.
Credential Manager a des problèmes d'incompatibilité avec le mot de passe GINA de Corel WordPerfect 12.	Si l'utilisateur se connecte à Credential Manager, crée un document dans WordPerfect et l'enregistre avec une protection par mot de passe, Credential Manager ne parvient pas à détecter ou à reconnaître le mot de passe GINA, 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 informations d'authentification unique pour une Connexion Bureau à distance sont définies sur **Connecter**, lorsque la fonction d'authentification unique est relancée, elle indique toujours **Enregistrer sous** au lieu de **Connecter**.	HP recherche actuellement un palliatif pour les prochaines versions du logiciel.
Les utilisateurs peuvent perdre toutes les informations d'authentification 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. Le module TPM est conçu pour protéger les informations d'authentification de Credential Manager. HP recommande aux utilisateurs de sauvegarder leur identité Credential Manager avant de supprimer le module TPM.
L'utilisateur ne peut pas accéder à Credential Manager une fois que le système est passé du mode Veille au mode Veille prolongée (Windows XP Service Pack 1 uniquement).	Après le passage du système en mode Veille ou Veille prolongée, l'administrateur ou l'utilisateur ne parvient pas à accéder à Credential Manager et l'écran de connexion Windows reste affiché, quel que soit le type des informations d'authentification (mot de passe, empreintes digitales ou Java Card) sélectionné.	Effectuez la mise à jour de Windows vers le Service Pack 2 avec Windows Update. Pour plus d'informations sur la cause du problème, reportez-vous à l'article 813301 de la base de connaissances Microsoft sur le site http://www.microsoft.com. L'utilisateur doit sélectionner Credential Manager, puis se connecter. Après avoir obtenu l'accès à Credential Manager, l'utilisateur est invité à ouvrir une session Windows (il est possible de sélectionner l'option de connexion Windows). Si l'utilisateur ouvre Windows en premier, il doit 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.	Credential Manager ne parvient pas à accéder au module TPM si la mémoire RAM est réinitialisée avec les paramètres d'usine après l'installation de Credential Manager.

Brève description	Détails	Solution
		Il est possible d'activer la puce de sécurité intégrée TPM à l'aide de l'utilitaire Computer Setup accessible par la touche f10, BIOS Configuration ou HP Client Manager. Pour activer la puce de sécurité intégrée via Computer Setup, procédez comme suit : 1. Ouvrez Computer Setup en démarrant/redémarrant l'ordinateur, puis appuyez sur f10 lorsque le message **F10 = ROM Based Setup** (F10 = Configuration ROM) s'affiche dans l'angle inférieur gauche de l'écran. 2. Utilisez les touches de direction pour sélectionner **Sécurité > Mot de passe de configuration**. Définissez un mot de passe. 3. Sélectionnez **Embedded Security Device** (Périphérique de sécurité intégrée). 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). 5. Sélectionnez **Activer > Enregistrer les modifications et quitter**. HP recherche d'autres solutions pour les prochaines versions du logiciel.
Le processus de sécurité **Restauration d'identité** perd l'association avec le jeton virtuel.	Lorsque l'utilisateur restaure une identité, Credential Manager peut perdre l'association avec l'emplacement du jeton virtuel indiqué sur l'écran de connexion. Même si le jeton virtuel est enregistré pour Credential Manager, l'utilisateur doit le réenregistrer afin de rétablir l'association.	Le système est ainsi conçu. En cas de désinstallation de Credential Manager sans sauvegarde des identités, la partie système (serveur) du jeton est détruite et le jeton n'est donc plus réutilisable pour la connexion, même si la partie client du jeton est rétablie via la procédure de restauration. HP recherche des solutions à long terme.

Embedded Security for HP ProtectTools

Brève description	Détails	Solution
Le cryptage de dossiers, de sous-dossiers et de fichiers sur le lecteur sécurisé personnel (PSD) entraîne un message d'erreur.	Si l'utilisateur copie des fichiers et des dossiers sur le lecteur sécurisé personnel et tente de crypter des dossiers/fichiers ou des dossiers/sous-dossiers, le message **Erreur lors de l'application des attributs** s'affiche. L'utilisateur peut crypter les mêmes fichiers sur l'unité C:\ ou sur un disque dur supplémentaire installé sur le système.	Le système est ainsi conçu. Le déplacement des fichiers/dossiers sur le lecteur sécurisé personnel entraîne automatiquement leur cryptage. Il n'est pas nécessaire d'exécuter à nouveau le cryptage des fichiers/dossiers. Toute tentative pour effectuer un nouveau cryptage EFS sur le lecteur sécurisé génère 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 afficher, supprimer, renommer ou déplacer le contenu des dossiers cryptés avec EFS.	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. 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.
L'utilisateur ne dispose pas d'options de cryptage lorsqu'il tente de restaurer le disque dur avec une partition 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. Le logiciel ne doit pas être installé dans une procédure de restauration avec une partition FAT32. Le système Microsoft EFS est pris en charge uniquement au format NTFS et ne fonctionne pas avec des partitions FAT32. Il s'agit d'une fonctionnalité de Microsoft EFS sans rapport avec le logiciel HP ProtectTools.
L'utilisateur peut crypter ou supprimer le fichier XML d'archive de restauration.	À dessein, les listes de contrôle d'accès pour ce dossier ne sont pas définies. Par conséquent, un utilisateur peut malencontreusement ou intentionnellement crypter ou supprimer le fichier, le rendant inaccessible. Une fois que le fichier a été crypté ou supprimé, personne ne peut utiliser le logiciel TPM.	Le système est ainsi conçu. Les utilisateurs ont des droits d'accès à une archive d'urgence afin d'enregistrer/de mettre à jour leur copie de sauvegarde des clés utilisateur de base. Les utilisateurs doivent avoir instruction de ne jamais crypter ni supprimer les fichiers d'archive de restauration.
L'interaction du système Embedded Security EFS avec Symantec Antivirus ou Norton Antivirus rallonge la durée des procédures de cryptage/décryptage et d'analyse.	Les fichiers cryptés interfèrent avec la recherche de virus effectuée par Antivirus ou Norton Antivirus 2005. Durant l'analyse, le système demande à l'utilisateur de base de saisir un mot de passe tous les 10 fichiers environ. Si l'utilisateur ne saisit pas de mot de passe, l'invite fait l'objet d'une temporisation et NAV2005 reprend l'analyse. Le cryptage des fichiers avec Embedded Security EFS est plus long lorsque Symantec Antivirus ou Norton Antivirus est en cours d'exécution.	Pour réduire la durée de l'analyse des fichiers Embedded Security EFS, l'utilisateur peut saisir le mot de passe de cryptage avant l'analyse ou effectuer le décryptage avant l'analyse. Pour réduire la durée de cryptage/décryptage des données avec Embedded Security EFS, l'utilisateur doit désactiver la fonction Auto-Protect de Symantec Antivirus ou Norton Antivirus.

Brève description	Détails	Solution
L'archive de restauration d'urgence ne peut pas être sauvegardée sur un support amovible.	Si l'utilisateur insère une carte mémoire MultiMediaCard ou Secure Digital (SD) lorsqu'il crée le chemin d'accès à l'archive de restauration d'urgence pendant l'initialisation de la sécurité intégrée, un message d'erreur s'affiche.	Le système est ainsi conçu. Le stockage de l'archive de restauration sur un support amovible n'est pas pris en charge. Il est possible d'enregistrer l'archive de restauration sur une unité du réseau ou une unité locale autre que l'unité C.
Des erreurs sont générées après une coupure de courant pendant l'initialisation de la sécurité intégrée.	Si une coupure de courant survient pendant l'initialisation de la puce de sécurité intégrée, vous risquez de rencontrer les problèmes suivants : • Si vous essayez de lancer l'assistant Initialisation de la sécurité intégrée, vous obtenez le message d'erreur suivant : **The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.** (Impossible d'initialiser la sécurité intégrée car la puce de sécurité intégrée a déjà un propriétaire.) • Si vous essayez de lancer l'assistant Initialisation utilisateur, vous obtenez le message d'erreur suivant : **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.** (La sécurité intégrée n'est pas initialisée. Pour utiliser l'assistant, vous devez au préalable initialiser la sécurité intégrée.)	Pour restaurer l'état normal après une coupure de courant, procédez comme suit : **REMARQUE:** Utilisez les touches fléchées pour sélectionner les menus et les options et pour modifier les valeurs (sauf instruction contraire). 1. Démarrez ou redémarrez l'ordinateur. 2. Appuyez sur f10 lorsque le message **f10=Setup** (f10=Configuration) apparaît à l'écran. 3. Sélectionnez l'option de langue appropriée. 4. Appuyez sur la touche entrée. 5. Sélectionnez **Sécurité > Sécurité intégrée**. 6. Définissez l'option **Embedded Security Device** (Périphérique de sécurité intégrée) sur **Enable** (Activer). 7. Appuyez sur f10 pour accepter la modification. 8. Sélectionnez **Fichier > Enregistrer les modifications et quitter**. 9. Appuyez sur la touche entrée. 10. Appuyez sur f10 pour enregistrer les modifications et quitter l'utilitaire.
Le mot de passe de l'utilitaire Computer Setup (**f10**) peut être supprimé après activation du module TPM.	L'activation du module TPM exige un mot de passe Computer Setup (**f10**). Lorsque le module est activé, l'utilisateur peut supprimer le mot de passe. Par conséquent, toute personne qui possède un accès direct au système peut réinitialiser le module TPM, générant un risque de perte de données.	Le système est ainsi conçu. Le mot de passe de l'utilitaire Computer Setup (**f10**) ne peut être supprimé que par un utilisateur connaissant le mot de passe. Cependant, HP recommande vivement de protéger en permanence le mot de passe Computer Setup (**f10**).
La zone du mot de passe du lecteur sécurisé personnel ne s'affiche plus lorsque le système redevient actif après le mode Veille.	Lorsqu'un utilisateur se connecte au système après avoir créé un lecteur sécurisé personnel, le module TPM lui demande le mot de passe utilisateur de base. Si l'utilisateur ne fournit pas le mot de passe et si le système passe en mode Veille, la zone de saisie du mot de passe n'est plus disponible lorsque le système sort du mode Veille.	Le système est ainsi conçu. 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 nécessaire 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	Le système est ainsi conçu. Tout administrateur peut modifier les règles de la plate-forme de sécurité avec ou sans initialisation TPM.

Brève description	Détails	Solution
	les utilisateurs qui ont des droits d'administrateur sur le système.	
Lorsqu'un certificat est visualisé, il apparaît comme non approuvé.	Après configuration de HP ProtectTools et exécution de l'assistant Initialisation de l'utilisateur, l'utilisateur peut afficher le certificat émis. Cependant, lors de sa visualisation, le certificat apparaît comme n'étant pas approuvé. Même s'il est possible à ce stade d'installer le certificat en cliquant sur le bouton Installer, celui-ci ne prend pas pour autant le statut approuvé.	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.
Une erreur intermittente de cryptage et décryptage apparaît : **The process cannot access the file because it is being used by another process.** (Le processus ne peut pas accéder au fichier car il est utilisé par un autre processus).	Il s'agit d'une erreur intermittente durant l'opération de cryptage ou de décryptage du fait que le fichier est utilisé par un autre processus, même si le fichier ou le dossier concerné ne fait pas l'objet d'un traitement par le système d'exploitation ou une autre application.	Pour résoudre ce problème : 1. Redémarrez le système. 2. Déconnectez-vous. 3. Reconnectez-vous.
Les données stockées sur un support de stockage amovible sont perdues si vous retirez celui-ci avant la fin du processus de création ou de transfert.	En cas de retrait d'un support de stockage tel qu'un disque dur MultiBay, le lecteur sécurisé personnel continue d'apparaître comme étant disponible et aucune erreur n'est générée pendant l'ajout/la modification de données sur le lecteur. Après le redémarrage du système, le lecteur ne reflète pas les modifications de fichiers qui ont eu lieu pendant que le support amovible était indisponible.	Ne retirez pas le lecteur sécurisé personnel du système avant que la génération des données ou que leur transfert ne soit terminé. Ce problème ne se rencontre que si l'utilisateur accède au lecteur, puis retire le disque dur alors que la génération des nouvelles données ou leur transfert n'est pas terminé. Si l'utilisateur tente d'accéder au lecteur sécurisé personnel pendant que le disque dur est absent, le message d'erreur **Le périphérique n'est pas prêt.** s'affiche.
Durant une désinstallation, si l'utilisateur ouvre l'outil d'administration sans avoir initialisé l'utilisateur de base, l'option **Désactiver** n'est pas disponible et le programme de désinstallation ne se termine pas tant que l'outil d'administration n'est pas fermé.	L'utilisateur peut procéder à une désinstallation sans désactiver le module TPM ou activer d'abord le TPM (via l'outil d'administration), puis effectuer la désinstallation. L'accès à l'outil d'administration exige l'initialisation d'une clé utilisateur de base. Si l'installation de base n'est pas exécutée, les options sont toutes inaccessibles. Du fait que l'utilisateur a choisi explicitement d'ouvrir l'outil d'administration (en cliquant sur **Oui** dans la boîte de dialogue indiquant **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 d'administration soit fermé. Si l'utilisateur clique sur **Non** dans cette boîte de dialogue, l'outil d'administration ne s'ouvre pas du tout et le programme de désinstallation se poursuit.	L'outil d'administration permet de désactiver la puce TPM, mais cette option n'est pas disponible tant que la clé utilisateur de base n'a pas été initialisée. Si elle n'a pas été initialisée, sélectionnez **OK** ou **Annuler** pour revenir au programme de désinstallation.

Brève description	Détails	Solution
Un blocage intermittent du système se produit après la création d'un lecteur sécurisé personnel sur des comptes à deux utilisateurs et l'utilisation de la fonction de changement rapide d'utilisateur dans des configurations système 128 Mo.	Le système peut se bloquer et afficher un écran noir, sans clavier ni souris, au lieu d'afficher un écran de bienvenue (ou de connexion) si la fonction de changement rapide d'utilisateur est sollicitée sur un système doté d'une RAM minimum.	La cause semble due à un problème de synchronisation dans les configurations à faible quantité de mémoire. Les graphiques intégrés utilisent une architecture UMA qui exige 8 Mo, ce qui ne laisse à l'utilisateur que 120 Mo disponibles. L'erreur est générée lorsque ces 120 Mo sont partagés par les deux utilisateurs connectés et qu'ils utilisent le changement rapide. La solution consiste à redémarrer le système et à augmenter la configuration de la mémoire (HP ne fournit pas des 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 zone de saisie du mot de passe de l'authentification de l'utilisateur du système EFS s'ouvre à nouveau lorsque l'utilisateur clique sur **OK** ou que le système sort du mode 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.
Durant l'installation de la version japonaise, des chaînes légèrement tronquées apparaissent dans des descriptions fonctionnelles.	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 cryptage EFS fonctionne sans qu'il soit nécessaire de saisir un mot de passe dans la zone de message.	En raison du délai d'expiration associé à la saisie d'un mot de passe utilisateur, le cryptage est encore disponible pour un fichier ou un dossier.	Le cryptage ne nécessite pas d'authentification par mot de passe puisqu'il s'agit d'une fonctionnalité du système Microsoft EFS. En revanche, le décryptage exige la saisie du mot de passe utilisateur.
La messagerie électronique sécurisée est prise en charge, même si elle n'est pas spécifiée dans l'assistant Initialisation de l'utilisateur ou si la configuration de messagerie électronique est désactivée dans les stratégies d'utilisateur.	Le logiciel de sécurité intégrée et l'assistant ne contrôlent pas les paramètres d'un client de messagerie (Outlook, Outlook Express ou Netscape).	Le système est ainsi conçu. La configuration des paramètres de messagerie TPM n'interdit pas la modification des paramètres de cryptage directement dans un client de messagerie. L'utilisation d'une messagerie électronique sécurisée est définie et contrôlée par des applications tierces. L'assistant HP permet d'établir une liaison avec les trois applications de référence pour une personnalisation immédiate.
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 de scripts de déploiement à grande échelle sur un système HP ProtectTools Embedded Security déjà initialisé rend les archives de restauration et les jetons de restauration inutiles du fait qu'elle entraîne l'écrasement de ces fichiers XML.	HP cherche à résoudre le problème de remplacement des fichiers XML et proposera une solution dans un futur SoftPaq.

Brève description	Détails	Solution
Les scripts de connexion automatisée ne fonctionnent pas pendant la restauration de l'utilisateur dans Embedded Security.	L'erreur se produit après que l'utilisateur effectue les actions suivantes : • initialisé le propriétaire et l'utilisateur dans la sécurité intégrée (à l'aide des emplacements par défaut **Mes documents**), • restauré les paramètres par défaut du BIOS du module TPM, • redémarré l'ordinateur, • commencé à restaurer Embedded Security. Pendant la restauration, Credential Manager demande si le système peut automatiser la connexion avec la technologie d'authentification utilisateur du module TPM Infineon. Si l'utilisateur sélectionne **Oui**, l'emplacement de SPEmRecToken est automatiquement affiché dans la zone de texte. 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 lecteurs sécurisés personnels à utilisateurs multiples ne fonctionnent pas dans un environnement où l'identité de l'utilisateur change rapidement.	Cette erreur se produit lorsque plusieurs utilisateurs possèdent un lecteur sécurisé personnel avec une lettre de lecteur identique. Toute tentative de modification de l'identité de l'utilisateur au chargement du lecteur sécurisé rend le lecteur de l'autre utilisateur indisponible.	Le lecteur de l'autre utilisateur sera disponible seulement s'il est redéfini avec une autre lettre de lecteur ou si le premier utilisateur est déconnecté.
Le lecteur sécurisé personnel est désactivé et ne peut pas être supprimé après le formatage du disque dur sur lequel il a été créé.	L'icône du lecteur sécurisé personnel est toujours visible, mais le message d'erreur **drive is not accessible** (lecteur inaccessible) apparaît lorsque l'utilisateur tente d'accéder au lecteur sécurisé personnel. L'utilisateur ne peut pas supprimer le lecteur sécurisé personnel et le message suivant s'affiche : **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process** (votre lecteur sécurisé personnel est en cours d'utilisation, vérifiez qu'il ne contient aucun fichier ouvert ou n'est pas utilisé par un autre programme). L'utilisateur doit redémarrer le système pour supprimer le lecteur sécurisé personnel	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. Solution : après le redémarrage suivant, l'émulation PSD échoue et l'utilisateur peut supprimer l'ancienne émulation PSD et en créer une nouvelle.

Brève description	Détails	Solution
	et empêcher son chargement au prochain démarrage.	
Une erreur interne est détectée lorsque l'utilisateur effectue une restauration à partir de l'archive de sauvegarde automatique.	Dans Embedded Security, si l'utilisateur sélectionne l'option **Restore under Backup** (Restaurer à partir de la sauvegarde) pour utiliser l'utilitaire d'archive de sauvegarde automatique, puis sélectionne **SPSystemBackup.xml**, l'assistant de restauration échoue et le message d'erreur suivant s'affiche : **The selected Backup Archive does not match the restore reason. Please select another archive and continue.** (L'archive de sauvegarde sélectionnée ne correspond pas à la condition requise. Sélectionnez une autre archive, puis continuez.)	Si l'utilisateur sélectionne **SpSystemBackup.xml** lorsque SpBackupArchive.xml est requis, l'assistant de sécurité intégrée échoue et affiche le message suivant : **An internal Embedded Security error has been detected.** (Une erreur de sécurité interne a été détectée.) L'utilisateur doit sélectionner le fichier XML approprié pour satisfaire la condition requise. 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.
Le système de sécurité détecte une erreur de restauration 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 redéfinissant le module TPM, en exécutant la restauration et en sélectionnant tous les utilisateurs avant l'exécution de la prochaine sauvegarde quotidienne définie par défaut. Si la sauvegarde automatisée est exécutée, les utilisateurs non restaurés et les données correspondantes sont supprimés. Si une nouvelle sauvegarde du système est enregistrée, les utilisateurs non sélectionnés précédemment ne peuvent pas être restaurés. Par ailleurs, l'utilisateur doit restaurer la sauvegarde du système dans son intégralité. Une sauvegarde des archives peut être restaurée individuellement.
Réinitialiser la ROM système sur les paramètres par défaut rend le module TPM invisible.	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 : Ouvrez l'utilitaire Computer Setup (**f10**), accédez à **Sécurité > Sécurité des périphériques**, puis modifiez le champ de **Caché** à **Disponible**.
La sauvegarde automatique ne fonctionne pas avec une unité mappée.	Lorsqu'un administrateur définit la sauvegarde automatique dans Embedded Security, une entrée est créée dans **Windows** > **Tâches** > **Tâche planifiée**. Cette tâche planifiée Windows est définie pour utiliser NT AUTHORITY \SYSTEM lors de l'exécution de la sauvegarde. Ceci fonctionne correctement sur n'importe quelle unité locale. 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. Si la sauvegarde automatique est planifiée pour avoir lieu à la connexion, l'icône TNA de Embedded Security	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. Dans les prochaines versions du logiciel, HP prévoira d'inclure [nom_ordinateur/nom_administrateur] comme paramétrage par défaut.

Brève description	Détails	Solution
	affiche le message suivant : **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** (L'emplacement de l'archive de sauvegarde n'est pas accessible pour le moment. Cliquez ici si vous souhaitez sauvegarder une archive temporaire jusqu'à ce que l'archive de sauvegarde soit de nouveau accessible.) Si la sauvegarde automatique est planifiée à un moment spécifique, la sauvegarde échoue sans aucune notification d'échec.	
La sécurité intégrée ne peut pas être temporairement désactivée dans l'interface utilisateur Embedded Security.	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. 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.

Device Access Manager for HP ProtectTools

Brève description	Détails	Solution
L'accès aux périphériques a été refusé à des utilisateurs dans Device Access Manager. Néanmoins, les périphériques sont toujours accessibles.	Des configurations simples et/ou de classes de périphériques ont été utilisées dans Device Access Manager pour interdire l'accès des utilisateurs aux périphériques. Malgré cette interdiction, les utilisateurs peuvent toujours accéder aux périphériques.	Vérifiez que le service de verrouillage de périphériques HP ProtectTools est activé. En tant qu'administrateur, accédez à **Panneau de configuration > Outils d'administration > Services**. Dans la fenêtre **Services**, recherchez le service **Verrouillage des périphériques/Audition HP ProtectTools**. Vérifiez que le service est activé et que le type de démarrage est **Automatique**.
Un utilisateur peut ou ne peut pas accéder à un périphérique de manière inattendue.	Device Access Manager a été utilisé pour refuser l'accès à certains périphériques et autoriser l'accès à d'autres périphériques. Depuis leur ordinateur, les utilisateurs peuvent accéder aux périphériques pour lesquels Device Access Manager a refusé l'accès et se voient refuser l'accès aux périphériques pour lesquels Device Access Manager devrait autoriser l'accès.	La configuration de classes de périphériques dans Device Access Manager doit être utilisée pour rechercher les paramètres des périphériques utilisateur. Sélectionnez **Security Manager > Device Access Manager > Configuration des classes de périphériques**. Développez les niveaux dans l'arborescence de classes de périphériques et passez en revue les paramètres applicables à l'utilisateur. Vérifiez toute autorisation "refusée" pouvant être définie pour l'utilisateur ou tout groupe Windows auquel l'utilisateur peut appartenir, par exemple, Utilisateurs, Administrateurs, etc.
Autoriser ou Refuser : lequel prévaut ?	Dans la configuration de classes de périphériques, la configuration suivante a été définie : • L'autorisation Autoriser a été accordée à un groupe Windows (par exemple, BUILTIN \Administrators) et l'autorisation Refuser a été attribuée à un autre groupe Windows (par exemple, BUILTIN\Users) au même niveau dans la hiérarchie des classes de périphériques (par exemple, Lecteurs de DVD/CD-ROM). Si un utilisateur est membre de ces deux groupes (par exemple, Administrateur), lequel prévaut ?	L'accès au périphérique est refusé à l'utilisateur. Refuser prévaut sur Autoriser. L'accès est refusé en raison du fonctionnement de Windows en matière de gestion des autorisations d'accès aux périphériques. L'accès est refusé à un groupe et autorisé à un autre groupe, or l'utilisateur appartient aux deux groupes. L'accès est refusé à l'utilisateur car le fait de refuser l'accès prévaut sur toute autorisation d'accès. Une autre solution consisterait à refuser au groupe Utilisateurs l'accès au niveau des lecteurs de DVD/CD-ROM et d'accorder au groupe Administrateurs l'accès au niveau inférieur aux lecteurs de DVD/CD-ROM. Il est également possible de définir des groupes Windows spécifiques : un groupe pour autoriser l'accès aux DVD/CD et un groupe pour refuser l'accès aux DVD/CD. Des utilisateurs spécifiques seraient alors ajoutés dans le groupe approprié.

Divers

Logiciel affecté — Brève description	Détails	Solution
Security Manager - Avertissement reçu : **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 HP Protect Tools Security Manager n'est pas installé.)	Toutes les applications de sécurité telles que Embedded Security, Java Card Security et les lecteurs biométriques sont des modules évolutifs pour l'interface de Security Manager. Security Manager doit être installé avant de pouvoir charger un module de sécurité agréé HP.	Le logiciel Security Manager doit être installé avant toute installation d'un module de sécurité.
L'utilitaire de mise à jour du microprogramme TPM pour les modèles contenant des modules TPM Broadcom : l'outil fourni via le site Web d'assistance HP indique **ownership required** (propriété requise).	Il s'agit du comportement attendu de l'utilitaire du microprogramme TPM pour les modèles contenant des modules TPM Broadcom. 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. 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. 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. **REMARQUE:** Un redémarrage est toujours recommandé après l'exécution de la mise à jour du microprogramme. La version du microprogramme n'est pas identifiée correctement tant que le redémarrage n'est pas effectué.	1. Réinstallez le logiciel Embedded Security. 2. Exécutez l'assistant de configuration d'utilisateur et de plate-forme. 3. Vérifiez que le système contient le programme Microsoft .NET framework 1.1 : a. Cliquez sur **Démarrer**. b. Cliquez sur **Panneau de configuration**. c. Cliquez sur **Ajout ou suppression de programmes**. d. Vérifiez que **Microsoft .NET Framework 1.1** apparaît dans la liste des programmes. 4. Vérifiez la configuration matérielle et logicielle : a. Cliquez sur **Démarrer**. b. Cliquez sur **Tous les programmes**. c. Cliquez sur **HP ProtectTools Security Manager**. d. Sélectionnez **Sécurité intégrée** dans l'arborescence. e. Cliquez sur **More Details** (Détails). Le système devrait présenter la configuration suivante : • Product version (Version de produit) = V4.0.1 • Embedded Security State (État de la sécurité intégrée) : Chip State (Puce) = Enabled (Activée), Owner State (Propriétaire) = Initialized (Initialisé), User State (Utilisateur) = Initialized (Initialisé) • Component Info (Info composants) : TCG Spec. Version = 1.2

Logiciel affecté — Brève description	Détails	Solution
		• Vendor (Fabricant) = Broadcom Corporation • FW Version (Version microprog.) = 2.18 (ou ultérieure) • TPM Device driver library version (Version de la bibliothèque de drivers de périphériques TPM) = 2.0.0.9 (ou ultérieure) 5. Si la version du microprogramme ne correspond pas à 2.18, téléchargez et mettez à jour le microprogramme TPM. Le SoftPaq du microprogramme TPM peut être téléchargé sur le site Web HP à l'adresse 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. Autorisez Security Manager à finaliser le chargement des services (message affiché en haut de la fenêtre Security Manager) et de tous les modules répertoriés dans la colonne de gauche. Pour éviter un échec, prévoyez un temps de chargement raisonnable pour les modules.
HP ProtectTools : les privilèges d'accès non restreint ou d'administrateur non contrôlés entraînent des risques de sécurité.	De nombreux risques existent avec un accès au PC client non restreint, notamment les suivants : • Suppression du lecteur sécurisé personnel • Modification malveillante des paramètres utilisateur • Désactivation des stratégies et 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. Des privilèges d'administration ne devraient pas être accordés à des utilisateurs non autorisés.
Les mots de passe de sécurité intégrée du BIOS et du système d'exploitation sont désynchronisés.	Si un utilisateur ne valide pas un nouveau mot de passe pour la sécurité intégrée du BIOS, le mot de passe d'origine est réutilisé à l'aide de la commande **f10** du 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 code PIN du TPM est associé au premier utilisateur qui initialise le paramètre utilisateur. Si un ordinateur compte plusieurs utilisateurs, l'administrateur est considéré comme le premier utilisateur. Ce dernier devra communiquer son code PIN utilisateur TPM aux autres utilisateurs pour la connexion.	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.

Logiciel affecté — Brève description	Détails	Solution
L'utilisateur doit modifier son code PIN pour que le préamorçage du module TPM soit possible après la réinitialisation des paramètres d'usine.	L'utilisateur doit modifier son code PIN ou créer un autre utilisateur pour initialiser les paramètres utilisateur et exécuter l'authentification du BIOS TPM après la réinitialisation. Il n'existe aucune option spécifique permettant d'exécuter l'authentification du BIOS TPM.	Le système est ainsi conçu. La réinitialisation des paramètres d'usine efface la clé utilisateur de base. L'utilisateur doit modifier son code PIN ou créer un nouvel utilisateur pour réinitialiser la clé utilisateur de base.
La **Prise en charge de l'authentification à la mise sous tension** n'est pas définie par défaut à l'aide de l'option **Restaurer les paramètres d'usine** de Embedded Security.	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 **Restaurer les paramètres d'usine** désactive le périphérique de sécurité intégrée, lequel masque les autres options de sécurité intégrée (notamment la **Prise en charge de l'authentification à la mise sous tension**). Cependant, après la réactivation du périphérique de sécurité intégrée, l'option **Prise en charge de l'authentification à la mise sous tension** reste activée. HP s'efforce de trouver une solution, qui sera fournie dans un prochain SoftPaq de ROM de type Web.
L'authentification de sécurité à la mise sous tension chevauche le mot de passe du BIOS pendant la séquence de démarrage.	L'authentification au démarrage demande à l'utilisateur de se connecter au système à l'aide du mot de passe TPM. Toutefois, si l'utilisateur appuie sur la touche **f10** pour accéder au BIOS, l'utilisateur dispose des droits d'accès en lecture seule.	Pour écrire dans le BIOS, l'utilisateur doit saisir le mot de passe du BIOS au lieu du mot de passe du TPM dans la fenêtre d'authentification au démarrage.
Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après modification du mot de passe propriétaire.	Le BIOS demande l'ancien et le nouveau mots de passe via Computer Setup après 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 TPM, après l'exécution du système d'exploitation, et à vérifier la phrase secrète du 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.

DriveLock automatique Fonction de sécurité qui entraîne la génération et la protection de mots de passe DriveLock par la puce de sécurité intégrée TPM. Lorsque l'utilisateur est authentifié par la puce de sécurité intégrée TPM durant le démarrage en entrant le mot de passe de clé utilisateur de base TPM correct, le BIOS déverrouille le disque dur pour l'utilisateur.

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.

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