HP ProtectTools
Manuel de l'utilisateur

Microsoft et Windows sont des marques déposées de Microsoft Corporation aux États-Unis. Bluetooth est une marque détenue par son propriétaire et utilisée sous licence par Hewlett-Packard Company. Java est une marque de Sun Microsystems, Inc. aux États-Unis. Le logo SD est une marque de 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 : juin 2008

Référence du document : 481201-051

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
- Drive Encryption for HP ProtectTools (sur certains modèles seulement)
- Privacy Manager for HP ProtectTools (sur certains modèles seulement)
- File Sanitizer for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools (sur certains modèles seulement)
- Device Access Manager for HP ProtectTools (sur certains modèles seulement)

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 accessibles par téléchargement sur le site Web HP. Pour plus d'informations, visitez le site http://www.hp.com.

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

Fonctions HP ProtectTools

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

Module	Principales fonctions
Credential Manager for HP ProtectTools	• L'utilisation de Credential Manager s'apparente à celle d'un coffre-fort de mot de passe. Ce logiciel simplifie le processus de connexion grâce à la fonction d'authentification unique, qui mémorise et applique automatiquement les informations d'authentification des utilisateurs. • La fonction d'authentification unique (Single Sign On) offre également une protection supplémentaire en exigeant l'authentification au moyen de différentes technologies de sécurité combinées, telles qu'une carte Java™ Card et des données biométriques. • Le stockage des mots de passe est protégé par chiffrement logiciel et peut être étendu via une puce de sécurité TPM et/ou une authentification de périphérique sécurisée, telle que des cartes Java Card ou des données biométriques.
Drive Encryption for HP ProtectTools (sur certains modèles seulement)	• Drive Encryption permet le chiffrement total d'un disque dur sur l'ensemble du volume. • Drive Encryption force l'authentification au préamorçage afin de décrypter et accéder aux données.
Privacy Manager for HP ProtectTools (sur certains modèles seulement)	• Privacy Manager repose sur des techniques avancées de connexion qui vérifient la source, l'intégrité et la sécurité des communications lors de l'utilisation du courrier électronique, des documents Microsoft® Office ou de la messagerie instantanée.
File Sanitizer for HP ProtectTools	• File Sanitizer for HP ProtectTools vous permet de détruire en toute sécurité des ressources de données (informations confidentielles comprenant des fichiers d'applications, données historiques ou de navigation sur le Web ou autres composants de données) sur votre ordinateur et de "nettoyer" régulièrement votre disque dur.
BIOS Configuration for HP ProtectTools	• BIOS Configuration permet d'accéder à la gestion de l'authentification au démarrage et du mot de passe d'administration. • BIOS Configuration offre une alternative à l'utilitaire de configuration du BIOS au préamorçage (Computer Setup). • L'activation sous BIOS Configuration de la prise en charge Drivelock automatique, renforcée par la puce de sécurité intégrée, permet de protéger un disque dur contre les accès non autorisés, même après son retrait du système, en ne requérant de la part de l'utilisateur la mémorisation d'aucun autre mot de passe que celui de la puce de sécurité intégrée.
Embedded Security for HP ProtectTools (sur certains modèles seulement)	• 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 de créer un lecteur sécurisé personnel (PSD), ce qui est utile pour protéger les informations relatives aux fichiers utilisateur et aux dossiers. • Embedded Security prend en charge des applications d'autres sociétés (telles que Microsoft® Outlook et Internet Explorer) pour

Module	Principales fonctions
	les opérations protégées impliquant l'utilisation de certificats numériques.
Device Access Manager for HP ProtectTools (sur certains modèles seulement)	• 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.

Accès à HP ProtectTools Security

Pour accéder à HP ProtectTools Security Manager à partir du Panneau de configuration Windows®, procédez comme suit :

1. Sous Windows Vista®, cliquez sur **Démarrer**, puis sur **HP ProtectTools Security Manager pour administrateurs**.

   – ou –

   Sous Windows XP, cliquez sur **Démarrer**, cliquez sur **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.

   REMARQUE : Si vous n'êtes pas un administrateur de HP ProtectTools, vous pouvez exécuter HP ProtectTools en mode non-administrateur afin de visualiser les informations, mais vous ne pourrez effectuer aucune modification.

2. Dans le volet gauche, cliquez sur **HP ProtectTools**, puis sur **Getting Started** (Mise en route).

3. Cliquez sur le bouton **Security Manager Setup** (Configuration du gestionnaire de sécurité) situé sous l'icône d'HP ProtectTools représentant un bouclier, afin de lancer l'assistant Security Manager.

   La page suivante s'affiche :

- L'assistant guide les administrateurs du système d'exploitation Windows lors de la configuration des niveaux de sécurité et des méthodes de connexion sécurisée utilisées dans les environnements de préamorçage, Credential Manager et Drive Encryption.
- Les utilisateurs font également appel à l'assistant d'installation pour configurer leurs méthodes de connexion sécurisées.

REMARQUE : Pour accéder à chaque module HP ProtectTools et configurer des fonctionnalités plus puissantes, cliquez sur l'icône du module concerné.

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 à la page 17.”

Objectifs de sécurité fondamentaux

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

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

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 :
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- DriveLock permet de garantir qu'aucune donnée n'est accessible même après le retrait de l'unité de disque dur et son installation sur un système non sécurisé.
- 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 à la page 74”
  - “Utilisation du lecteur sécurisé personnel à la page 77”

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) à la page 84”.
- DriveLock permet de garantir qu'aucune donnée n'est accessible même après le retrait de l'unité de disque dur et son installation sur un système non sécurisé.

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

L'accès non autorisé à un ordinateur professionnel non sécurisé représente un danger potentiel pour des ressources en réseau, telles que les informations d'un service financier, d'un cadre de l'entreprise ou d'un service de Recherche & Développement, de même que pour les informations d'ordre privé telles que les brevets ou relevés de compte personnels. Les fonctionnalités suivantes contribuent à empêcher l'accès non autorisé :

- L'authentification au préamorçage, lorsqu'elle est activée, empêche tout accès au système d'exploitation. Voir les procédures suivantes :
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- 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 à la page 74”
  - “Utilisation du lecteur sécurisé personnel à la page 77”
- 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 à la page 12”
  - “Utilisation de la fonction d'authentification unique à la page 18”
- 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 à la page 83”.
- 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 à la page 74”
  - “Utilisation du lecteur sécurisé personnel à la page 77”

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 à la page 12”
- “Utilisation de la fonction d'authentification unique à la page 18”

De plus, pour une meilleure sécurité, Embedded Security for HP ProtectTools protège ce référentiel dans lequel sont regroupés des noms d'utilisateur et des mots de passe. Les utilisateurs peuvent ainsi

avoir plusieurs mots de passe forts sans avoir à les écrire pour les mémoriser. Voir Embedded Security “Procédures de configuration à la page 74”

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 : La plupart des fonctions de HP ProtectTools peuvent être personnalisées par le responsable de la sécurité, en collaboration avec HP. Pour plus d'informations, visitez le site Web HP à l'adresse 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,

Mot de passe HP ProtectTools	Défini dans ce module HP ProtectTools	Fonction
		en offrant un accès simultané à Windows et Credential Manager.
Mot de passe du fichier de restauration Credential Manager	Credential Manager, par l'administrateur informatique	Protège l'accès au fichier de restauration Credential Manager.
Mot de passe de clé utilisateur de base **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.

Sauvegarde et restauration des informations d'authentification HP ProtectTools

Pour sauvegarder et restaurer des données d'authentification à partir de tous les modules HP ProtectTools pris en charge, reportez-vous aux informations suivantes :

Sauvegarde des informations d'authentification et des paramètres

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

- Sélectionnez et sauvegardez les informations d'authentification HP ProtectTools avec Drive Encryption.

  Vous pouvez également souscrire le service en ligne de restauration de clé Drive Encryption (Online Drive Encryption Key Recovery Service), afin de sauvegarder une copie de votre clé de chiffrement et accéder à votre ordinateur en cas de perte du mot de passe empêchant l'accès à votre sauvegarde locale.

  REMARQUE : Pour récupérer votre mot de passe via ce service, vous devez être connecté à Internet et posséder une adresse électronique valide.

- Utilisez Embedded Security for HP ProtectTools afin de sauvegarder les informations d'authentification HP ProtectTools.

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 à la page 12.”
- 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 à Credential Manager

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

- Icône de HP ProtectTools Security Manager dans la zone de notification
- Sous Windows Vista®, cliquez sur **Démarrer**, puis sur **HP ProtectTools Security Manager pour administrateurs**.
- Sous Windows XP, cliquez sur **Démarrer**, puis sur **HP ProtectTools Security Manager**.

REMARQUE : Sous Windows Vista, vous devez exécuter HP ProtectTools Security Manager pour administrateurs si vous souhaitez effectuer des modifications.

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 à la page 12.”

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**
   - Sur la page “Credential Manager” de HP ProtectTools Security Manager, en cliquant sur le lien **Log On** (Connexion) dans le coin supérieur droit de la fenêtre
2. Suivez les instructions à l'écran pour vous connecter à Credential Manager.

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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Register Fingerprints** (Enregistrement des empreintes digitales).
3. Suivez les instructions à l'écran pour procéder à l'enregistrement de vos empreintes digitales et configurer le lecteur d'empreintes.
4. Si vous souhaitez configurer le lecteur d'empreintes digitales pour un autre utilisateur Windows, connectez-vous à Windows avec l'identité de cet utilisateur et répétez la procédure ci-dessus.

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 Smart Card ou d'un jeton de sécurité

Une Smart Card est une carte en matière plastique de taille à peu près équivalente à celle d'une carte de crédit, et qui contient un microprocesseur dans lequel des informations peuvent être chargées. Les cartes Smart Card permettent de protéger les informations et données d'authentification des individus. La connexion à un réseau au moyen d'une Smart Card permet de bénéficier d'une authentification de haut niveau lorsque la technologie utilisée fait appel à une identification sur la base de données cryptographiques et un justificatif de propriété pour l'authentification d'un utilisateur sur un domaine.

Un jeton USB est simplement une carte Smart Card de format différent. Le processeur intelligent, au lieu d'être déployé sur une carte de crédit en plastique, est inséré dans un jeton en plastique également appelé clé USB. La principale différence entre une Smart Card et un jeton réside dans l'interface d'accès. Une carte nécessite un lecteur, tandis qu'un jeton s'insère directement dans un port USB quelconque. En revanche, il n'existe aucune différence quant aux fonctionnalités principales ni à l'enregistrement et à la spécification des informations d'identification.

Un jeton USB est utilisé dans le cas d'une authentification renforcée. Il permet d'étendre les fonctionnalités de sécurité et garantit un accès sûr aux informations.

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 à la page 15.

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Register Smart Card or Token** (Enregistrer une Smart Card ou un jeton).
3. Dans la boîte de dialogue **Device Type** (Type de périphérique), sélectionnez le type de périphérique souhaité et cliquez sur **Suivant**.
4. Si le périphérique sélectionné est une Smart Card ou un jeton USB, assurez-vous que la Smart Card est insérée ou que le jeton est connecté à un port USB.

REMARQUE : Si la Smart Card n'est pas insérée ou que le jeton USB n'est pas connecté, le bouton Suivant est désactivé dans la boîte de dialogue Select Token (Sélectionner un jeton).

5. Dans la boîte de dialogue Device Type (Type de périphérique), sélectionnez **Suivant**.

   La boîte de dialogue Token Properties (Propriétés du jeton) s'affiche.

6. Entrez le code confidentiel, sélectionnez l'option **Register smart card or token for authentication** (Enregistrer une Smart Card ou un jeton pour l'authentification) et cliquez sur **Finish** (Fin).

Enregistrement d'autres informations d'authentification

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Register Credentials** (Enregistrer les données d'identification).

   L'assistant d'enregistrement de Credential Manager s'ouvre.

3. 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 :

- Modification du mot de passe de connexion à Windows
- Modification du code confidentiel d'un jeton
- Verrouillage d'un poste de travail

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 à la page 25”.

Création d'un jeton virtuel

Le fonctionnement d'un jeton virtuel est sensiblement identique à celui d'une carte Java Card ou d'un jeton USB. La sauvegarde du jeton s'effectue soit sur le disque dur de l'ordinateur, soit dans le registre Windows. Lorsque vous vous connectez à l'aide d'un jeton virtuel, vous êtes invité à vous authentifier au moyen d'un code confidentiel.

Pour créer un jeton virtuel :

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Register Smart Card or Token** (Enregistrer une Smart Card ou un jeton).
3. Dans la boîte de dialogue **Device Type** (Type de périphérique), cliquez sur **Virtual Token** (Jeton virtuel), puis sur **Suivant**.
4. Indiquez le nom et l'emplacement du jeton, puis cliquez sur **Suivant**.

   Un nouveau jeton virtuel peut être stocké dans un fichier ou dans la base de données de registre de Windows.
5. Dans la boîte de dialogue Token Properties (Propriétés du jeton), indiquez le code confidentiel principal (Master PIN) et le code utilisateur (User PIN) du jeton virtuel nouvellement créé, sélectionnez l'option **Register smart card or token for authentication** (Enregistrer une Smart Card ou un jeton pour l'authentification) et cliquez sur **Finish** (Fin).

Modification du mot de passe de connexion Windows

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Change Windows Password** (Changer le mot de passe Windows).
3. Entrez votre ancien mot de passe dans le champ **Ancien mot de passe**.
4. Entrez et confirmez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.
5. Cliquez sur **Terminer**.

Modification du code PIN d'un jeton

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité), puis sur **Change Token PIN** (Changer le code confidentiel du jeton).
3. Dans la boîte de dialogue Device Type (Type de périphérique), sélectionnez le type de périphérique souhaité et cliquez sur **Suivant**.
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.

REMARQUE : Si vous entrez plusieurs fois de suite un code confidentiel erroné, le verrouillage du jeton s'active. L'utilisation du jeton ne sera possible qu'une fois celui-ci déverrouillé.

Verrouillage de l'ordinateur (poste de travail)

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 à la page 25".

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

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **My Identity** (Mon identité).
3. Cliquez sur **Lock Workstation** (Poste de travail local) pour verrouiller immédiatement votre ordinateur.

   Pour déverrouiller l'ordinateur, vous devez utiliser le mot de passe Windows ou l'assistant de connexion de Credential Manager.

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. Sous Windows XP, si vous n'avez pas enregistré vos empreintes digitales pour vous connecter à Windows, cliquez sur l'icône de clavier située dans le coin supérieur gauche de l'écran, à côté de l'icône d'empreinte digitale. L'assistant de connexion de Credential Manager s'ouvre.

   Sous Windows Vista, si vous n'avez pas enregistré vos empreintes digitales pour vous connecter à Windows, cliquez sur l'icône **Credential Manager** dans l'écran de connexion. L'assistant de connexion de Credential Manager s'ouvre.
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 l'option **More** (Plus) et cliquez sur **Wizard Options** (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.

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 à la page 25.”

Enregistrement d'une nouvelle application

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

Utilisation de l'enregistrement automatique

1. Ouvrez une application qui requiert une connexion.
2. Cliquez sur l'icône d'authentification unique de Credential Manager dans la boîte de dialogue du mot de passe de l'application ou du site Web.
3. Tapez votre mot de passe pour l'application ou le site, puis cliquez sur **OK**. La boîte de dialogue **Credential Manager Single Sign On** (Authentification unique de Credential Manager) s'affiche.
4. Cliquez sur **More** (Autres) et effectuez une sélection parmi les options suivantes :

   - Do not use SSO for this site or application (Ne pas utiliser l'authentification unique pour ce site ou cette application)
   - Prompt to select account for this application (Inviter à sélectionner un compte pour cette application)
   - Fill in credentials but do not submit (Renseigner les informations d'authentification mais ne pas soumettre)

- Authenticate user before submitting credentials (Authentifier l'utilisateur avant de soumettre les informations d'authentification)
- Show SSO shortcut for this application (Afficher le raccourci d'authentification unique pour cette application)

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

Utilisation de l'enregistrement manuel (glisser-déposer)

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications) dans le volet de gauche.
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Pour modifier ou supprimer un site Web ou une application précédemment enregistré(e), sélectionnez l'enregistrement souhaité dans la liste.
4. Suivez les instructions à l'écran.

Gestion d'applications et d'informations d'authentification

Modification de propriétés d'application

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications) dans le volet de gauche.
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Cliquez sur l'entrée de l'application à modifier, puis sur **Propriétés**.
4. 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.
5. Cliquez sur l'onglet **Script** pour afficher et modifier le script d'application SSO.
6. Cliquez sur **OK**.

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

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications) dans le volet de gauche.
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Cliquez sur l'entrée correspondant à l'application que vous souhaitez supprimer, puis sur **Remove** (Supprimer).
4. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
5. 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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications) dans le volet de gauche.
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Cliquez sur l'entrée correspondant à l'application que vous souhaitez exporter, puis sur **More** (Plus).
4. Suivez les instructions à l'écran pour compléter l'exportation.
5. Cliquez sur **OK**.

Importation d'une application

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications) dans le volet de gauche.
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Cliquez sur l'entrée correspondant à l'application que vous souhaitez importer, puis sur **More** (Plus).
4. Suivez les instructions à l'écran pour compléter l'importation.
5. Cliquez sur **OK**.

Modification d'informations d'authentification

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Services and Applications** (Services et applications).
2. Cliquez sur **Manage Services and Applications** (Gestion des services et applications).

   La boîte de dialogue Single Sign On (Authentification unique) de Credential Manager s'affiche.
3. Cliquez sur l'entrée de l'application à modifier, puis sur **Autres**.
4. 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.

5. Suivez les instructions à l'écran.
6. 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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** dans le volet de gauche, puis sur **Services and Applications** (Services et applications).
2. Cliquez sur **Application Protection** (Protection des applications).
3. 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.

4. Cliquez sur **Add** (Ajouter).

   L'assistant Add a Program (Ajouter un programme) s'affiche.
5. Suivez les instructions à l'écran.

Suppression de la protection d'une application

Pour supprimer des restrictions d'une application :

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Services and Applications** (Services et applications).
3. Cliquez sur **Application Protection** (Protection des applications).
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. Cliquez sur **Application Protection** (Protection des applications).
2. 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.

3. Cliquez sur l'application à modifier, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** de cette application s'affiche.
4. 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])
5. 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.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de l'application.
7. 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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Multifactor Authentication** (Authentification multi-facteurs)
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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Multifactor Authentication** (Authentification multi-facteurs).
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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Multifactor Authentication** (Authentification multi-facteurs).
3. Sélectionnez l'onglet **Credentials** (Données d'identification).

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 “Advanced Settings” (Paramètres avancés) vous permet d'accéder à différents 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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Settings** (Paramètres).
3. Cliquez sur l'onglet approprié en fonction des 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. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager** (Gestionnaire de données d'identification) dans le volet de gauche.
2. Cliquez sur **Settings** (Paramètres).
3. Sélectionnez l'onglet **General** (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 (poste de travail) à la page 17".

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

1. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, puis sur **Settings** (Paramètres).

2. Sélectionnez l'onglet **Single Sign On** (Authentification unique).

3. 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**.

4. Cliquez sur **Appliquer**, puis sur **OK**.

5. Redémarrez l'ordinateur.

3 Drive Encryption for HP ProtectTools (sur certains modèles seulement)

△ **ATTENTION :** Si vous décidez de désinstaller le module Drive Encryption, vous devez préalablement procéder au déchiffrement de toutes les unités cryptées. Si vous n'effectuez pas cette opération, vous ne pourrez accéder aux données stockées sur les unités chiffrées que si vous avez souscrit au service de récupération correspondant. La réinstallation du module Drive Encryption ne permet pas de restaurer l'accès aux unités cryptées.

Procédures de configuration

Ouverture de Drive Encryption

1. Cliquez sur Démarrer, Tous les programmes, puis sur **HP ProtectTools Security Manager**.
2. Cliquez sur **Drive Encryption**.

Tâches générales

Activation de Drive Encryption.

Pour activer Drive Encryption, utilisez l'assistant de configuration de HP ProtectTools Security Manager.

Désactivation de Drive Encryption.

Pour désactiver Drive Encryption, utilisez l'assistant de configuration de HP ProtectTools Security Manager.

Connexion après activation de Drive Encryption

Lorsque vous mettez votre ordinateur sous tension après l'activation de Drive Encryption et l'inscription de votre compte d'utilisateur, vous devez vous connecter à l'écran d'ouverture de session de Drive Encryption :

REMARQUE : Si l'administrateur Windows a activé l'option Pre-boot Security (Sécurité de pré-amorçage) dans HP ProtectTools Security Manager, vous vous connecterez à l'ordinateur immédiatement après la mise sous tension de celui-ci, et non via l'écran d'ouverture de session de Drive Encryption.

1. Sélectionnez votre nom d'utilisateur et saisissez votre mot de passe Windows ou code confidentiel de carte Java™ Card. Vous pouvez également passer votre doigt si votre empreinte est enregistrée.
2. Cliquez sur **OK**.

REMARQUE : Si vous utilisez une clé de restauration pour vous connecter à partir de l'écran de connexion de Drive Encryption, vous serez également invité à sélectionner votre nom d'utilisateur Windows et à saisir votre mot de passe sur l'écran de connexion Windows.

Tâches avancées

Gestion de Drive Encryption (administrateur uniquement)

La page “Encryption Management” (Gestion du cryptage) permet aux administrateurs Windows d'afficher et de modifier l'état de Drive Encryption (actif ou inactif), ainsi que de voir l'état de cryptage de tous les disques durs de l'ordinateur.

Activation d'un mot de passe protégé par TPM (sur certains modèles uniquement)

Utilisez l'outil Embedded Security de HP ProtectTools pour activer la TPM. Après l'activation, la connexion à partir de l'écran de connexion de Drive Encryption nécessite la saisie de vos nom d'utilisateur et mot de passe Windows.

REMARQUE : Le mot de passe étant protégé par une puce de sécurité TPM, si le disque dur est déplacé sur un autre ordinateur, il n'est possible d'accéder aux données que si les paramètres TPM sont transférés vers cet ordinateur.

1. Utilisez l'outil Embedded Security de HP ProtectTools pour activer la TPM.
2. Ouvrez Drive Encryption et cliquez sur **Gestion du cryptage**.
3. Cochez la case **TPM-protected password** (Mot de passe protégé par TPM).

Cryptage ou décryptage des unités individuelles

1. Ouvrez Drive Encryption et cliquez sur **Gestion du cryptage**.
2. Cliquez sur **Modifier le cryptage**.
3. Dans la boîte de dialogue Modifier le cryptage, cochez ou décochez la case en regard de chaque disque dur que vous souhaitez crypter ou décrypter, puis cliquez sur **OK**.

REMARQUE : Lors du cryptage ou du décryptage du disque, la barre de progression affiche le temps restant avant la fin du processus de la session en cours. Si l’ordinateur est éteint ou se met en mode veille ou veille prolongée pendant le processus de cryptage puis redémarre, l’affichage du Temps restant se réinitialise, mais le cryptage reprend bien à l'endroit où il s'était arrêté. Le temps restant et l’affichage de la progression changeront plus rapidement de façon à refléter la progression précédente.

Sauvegarde et restauration (tâche de l'administrateur)

La page "Restauration" permet aux administrateurs Windows de sauvegarder et de restaurer des clés de cryptage.

Création de clés de sauvegarde

ATTENTION : Assurez-vous de conserver le périphérique de stockage contenant la clé de sauvegarde en lieu sûr, car en cas de perte de votre mot de passe ou de votre Java Card, ce périphérique sera votre seul moyen d'accéder à votre disque dur.

1. Ouvrez Drive Encryption, puis cliquez sur **Restauration** (Recovery).
2. Cliquez sur **Backup Keys** (Sauvegarder les clés).
3. Sur la page “Select Backup Disk” (Sélection du disque de sauvegarde), cliquez sur le nom du périphérique à utiliser pour stocker la clé de cryptage, puis cliquez sur **Suivant**.

4. Lisez les informations affichées sur la page qui suit, puis cliquez sur **Suivant**.

   La clé de cryptage est enregistrée sur le périphérique de stockage que vous avez sélectionné.

5. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Inscription à la restauration en ligne

Le service de restauration de clé Drive Encryption en ligne (Online Drive Encryption Key Recovery Service) stocke une copie de votre clé de cryptage, qui vous permet d'accéder à votre ordinateur en cas de perte de votre mot de passe si vous n'avez pas accès à votre sauvegarde locale.

REMARQUE : Vous devez être connecté à Internet et disposer d'une adresse électronique valide pour vous inscrire et récupérer votre mot de passe à l'aide de ce service.

1. Ouvrez Drive Encryption, puis cliquez sur **Restauration** (Recovery).
2. Cliquez sur **Enregistrer** (Register).
3. Cliquez sur l'une des options suivantes :
   - Je souhaite créer un compte de restauration pour ce PC. Si vous choisissez cette option, entrez votre adresse électronique et d'autres informations, puis cliquez sur **Suivant**.
   - Je souhaite ajouter ce PC à mon compte de restauration Web existant
4. Créez un mot de passe et confirmez-le, sélectionnez les questions de sécurité et saisissez les réponses, puis cliquez sur **Suivant**.

   REMARQUE : Un code d'activation de compte vous sera envoyé à l'adresse électronique indiquée.

5. Entrez le code d'activation et cliquez sur **Suivant**.
6. Entrez le numéro de série de l'ordinateur et cliquez sur **Suivant**.

   REMARQUE : Pour trouver le numéro de série de l'ordinateur, cliquez sur **Démarrer**, puis sur **Aide et support**.

7. Si vous n'avez pas de coupon d'abonnement, cliquez sur le lien **Click here to purchase coupons** (Cliquez ici pour acheter des coupons).

   Ce lien vous permet d'accéder au site Web du service de récupération SafeBoot. Ne quittez pas l'assistant.

8. Cliquez sur **Purchase Coupon Codes** (Acheter des codes de coupon).
9. Sélectionnez votre pays, le type d'ordinateur et cliquez sur **Démarrer**.
10. Cliquez sur **Acheter** situé en regard de l'option d'abonnement d'un an ou de 3 ans.
11. Cliquez sur **Procéder au paiement**.
12. Lisez les termes et conditions et cliquez sur **Accepter**.
13. Saisissez les coordonnées de facturation et cliquez sur **Continuer**.
14. Saisissez vos coordonnées bancaires et cliquez sur **Procéder au paiement** .

15. Notez le code du coupon et retournez sur la page “Account Activation” (Activation de compte) dans l’assistant.
16. Entrez le code d’activation de compte et cliquez sur **Suivant**.
17. Lorsque la boîte de dialogue de confirmation s’affiche, cliquez sur **OK**.

Gestion d’un compte de restauration existant en ligne

Après avoir créé un compte de restauration en ligne, vous pouvez accéder au site Web du service de restauration SafeBoot pour restaurer l'accès à l'ordinateur en cas de perte de votre mot de passe, modifier vos paramètres, redéfinir le mot de passe utilisé pour le compte de restauration en ligne et afficher ou renouveler votre compte.

1. Ouvrez Drive Encryption, puis cliquez sur **Restauration** (Recovery).
2. Cliquez sur **Gérer**.
3. Lorsque la page Web “SafeBoot Recovery Service” (Service de restauration SafeBoot) s’affiche, cliquez sur **Compte du service de restauration** (Recovery Service Account) ou **Recovery Process**(Processus de restauration).
4. Sur la page de connexion au service de restauration, entrez votre adresse électronique, votre mot de passe et les numéros et lettres qui apparaissent dans le champ.
5. Cliquez sur **Logon** (Connexion).
6. Cliquez sur **Profil** pour mettre à jour vos données personnelles, telles que numéro de téléphone et adresse de facturation.

   – ou –

   Cliquez sur **Reset Password** (Réinitialiser mot de passe) pour réinitialiser ou modifier votre mot de passe.

   – ou –

   Cliquez sur **My Subscriptions** (Mes abonnements) pour afficher les données sur les abonnements en cours.

REMARQUE : La page « Mes abonnements » permet également de renouveler vos abonnements. Cliquez sur **Renew Subscription** (Renouveler abonnement) pour réaliser cette opération.

Exécution d'une restauration

Réalisation d’une restauration locale

1. Mettez l'ordinateur sous tension.
2. Insérez le périphérique de stockage amovible contenant la clé de sauvegarde.
3. Lorsque la boîte de dialogue de connexion Drive Encryption for HP ProtectTools s’affiche, cliquez sur **Annuler**.
4. Cliquez sur **Options** dans le coin inférieur gauche de l’écran puis sur **Restauration**.
5. Cliquez sur **Local recovery** (Restauration locale), puis sur **Suivant**.

6. Sélectionnez le fichier contenant la clé de sauvegarde ou cliquez sur **Parcourir** pour la rechercher, puis cliquez sur **Suivant**.

7. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **OK**.

   Le processus de restauration est terminé et l'ordinateur démarre.

REMARQUE : Il est vivement recommandé de réinitialiser le mot de passe après la restauration.

Exécution d'une restauration en ligne

REMARQUE : Cette section décrit comment exécuter une restauration en ligne à partir d'un ordinateur différent avec une connexion Internet. Si vous n'avez pas accès à un tel ordinateur, contactez l'assistance technique HP.

1. Mettez l'ordinateur sous tension.
2. Lorsque la boîte de dialogue de connexion Drive Encryption for HP ProtectTools s'affiche, cliquez sur **Annuler**.
3. Cliquez sur **Options** dans le coin inférieur gauche de l'écran puis sur **Restauration**.
4. Cliquez sur **Restauration Web**, puis sur **Suivant**.
5. Enregistrez le code client et cliquez sur **Suivant**.
6. Sur un autre ordinateur avec connexion Internet, accédez au site Web du service de restauration SafeBoot à l'adresse http://www.safeboot-hp.com.
7. Cliquez sur **Recovery Process** (Processus de restauration).
8. Sur la page de connexion au service de restauration, entrez votre adresse électronique, votre mot de passe et les numéros et lettres qui apparaissent dans le champ.
9. Cliquez sur **Connexion** (Logon).
10. Cliquez sur **Recovery Process** (Processus de restauration).
11. Entrez le code client enregistré depuis l'ordinateur que vous restaurez et entrez les chiffres et les lettres qui apparaissent dans le champ.
12. Cliquez sur **Submit** (Envoyer).
13. Enregistrez chaque ligne de la clé de réponse.
14. Sur l'ordinateur que vous restaurez, entrez la ligne 1 de la clé de réponse enregistrée depuis le site Web du service de restauration SafeBoot et cliquez sur **Entrée**.
15. Entrez la ligne 2 de la clé de réponse et cliquez sur **Entrée**.
16. Entrez la ligne 3 de la clé de réponse et cliquez sur **Entrée**.
17. Entrez la ligne 4 de la clé de réponse et cliquez sur **Entrée**.

    REMARQUE : La ligne 4 de la clé de réponse est plus courte que les 3 premières lignes.

18. Cliquez sur **Terminer**.

REMARQUE : Il est vivement recommandé de réinitialiser le mot de passe après la restauration.

4 Privacy Manager for HP ProtectTools (sur certains modèles uniquement)

Privacy Manager for HP ProtectTools vous permet d'utiliser des méthodes de connexion sécurisée (authentification) évoluées pour vérifier la source, l'intégrité et la sécurité des communications avec le courrier électronique, les documents Microsoft® Office ou la messagerie instantanée.

Privacy Manager s'appuie sur l'infrastructure de sécurité fournie par HP ProtectTools Security Manager, contenant les méthodes de connexion sécurisée suivantes :

- Authentification par empreinte digitale
- Mot de passe Windows®
- Carte HP ProtectTools Java™ Card

Parmi les méthodes précitées, vous pouvez utiliser la méthode de votre choix dans Privacy Manager.

Ouverture de Privacy Manager

Pour ouvrir Privacy Manager :

1. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Cliquez sur **Privacy Manager : Sign and Chat**.

– ou –

Cliquez avec le bouton droit sur l'icône **HP ProtectTools** située dans la zone de notification, à l'extrémité droite de la barre des tâches, puis sélectionnez **Privacy Manager : Sign and Chat**, puis cliquez sur **Configuration**.

– ou –

Au niveau de la barre d'outils d'un message électronique Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis cliquez sur **Certificate Manager** (Gestionnaire de certificats) ou sur **Trusted Contact Manager** (Gestionnaire de contacts authentifiés).

– ou –

Au niveau de la barre d'outils d'un document Microsoft Office, cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis cliquez sur **Certificate Manager** (Gestionnaire de certificats) ou sur **Trusted Contact Manager** (Gestionnaire de contacts authentifiés).

Procédures de configuration

Gestion des certificats Privacy Manager

Les certificats Privacy Manager protègent les données et les messages à l'aide d'une technologie cryptographique appelée PKI (Infrastructure de clé publique). La technologie PKI exige que les utilisateurs obtiennent des clés cryptographiques et un certificat Privacy Manager émis par une autorité de certification (CA). Contrairement à la plupart des logiciels d'authentification et de cryptage des données qui exigent simplement une authentification périodique, Privacy Manager exige une authentification à chaque fois que vous signez un courrier électronique ou un document Microsoft Office à l'aide d'une clé cryptographique. Avec Privacy Manager, l'enregistrement et l'envoi de vos informations importantes sont sûrs et sécurisés.

Demande et installation d'un certificat Privacy Manager

Avant de pouvoir utiliser les fonctions de Privacy Manager, vous devez demander et installer un certificat Privacy Manager (depuis le programme Privacy Manager) à l'aide d'une adresse électronique valide. Cette adresse électronique doit être configurée sous la forme d'un compte dans Microsoft Outlook sur le même ordinateur que celui qui demande le certificat Privacy Manager.

Demande d'un certificat Privacy Manager

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur **Request a Privacy Manager Certificate** (Demander un certificat Privacy Manager).
3. Sur la page de bienvenue, lisez le texte, puis cliquez sur **Suivant**.
4. Sur la page du contrat de licence, lisez les termes du contrat.
5. Vérifiez que la case en regard du texte **Check here to accept the terms of this license agreement** (Cochez cette case pour accepter les termes du contrat de licence) est cochée, puis cliquez sur **Suivant**.
6. Sur la page des détails de votre certificat, saisissez les informations requises, puis cliquez sur **Suivant**.
7. Sur la page d'acceptation de la demande de certificat, cliquez sur **Terminer**.

   Vous recevrez un courrier électronique Microsoft Outlook avec votre certificat Privacy Manager joint.

Installation d'un certificat Privacy Manager

1. À réception du courrier électronique contenant votre certificat Privacy Manager en pièce jointe, ouvrez le courrier électronique et cliquez sur le bouton **Setup** (Installer) situé dans le coin inférieur droit du message.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
3. Sur la page indiquant que le certificat est installé, cliquez sur **Suivant**.
4. Sur la page de sauvegarde du certificat, saisissez un nom et un emplacement pour le fichier de sauvegarde ou cliquez sur **Parcourir** pour rechercher un emplacement.

△ **ATTENTION :** Vérifiez que vous enregistrez le fichier à un emplacement autre que votre disque dur et placez-le en lieu sûr. Ce fichier doit être réservé à votre utilisation propre. Il est requis si vous devez restaurer votre certificat Privacy Manager et les clés associées.

5. Saisissez et confirmez un mot de passe, puis cliquez sur **Suivant**.
6. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
7. Si vous choisissez de démarrer le processus d'invitation de contact authentifié, suivez les instructions à l'écran.

   – ou –

   Si vous cliquez sur Annuler, reportez-vous à la section Gestion des contacts authentifiés pour plus d'informations sur l'ajout ultérieur d'un contact authentifié.

Affichage des détails d'un certificat Privacy Manager

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur un certificat Privacy Manager.
3. Cliquez sur **Certificate details** (Détails du certificat).
4. Lorsque vous avez terminé de visualiser les détails, cliquez sur **OK**.

Renouvellement d'un certificat Privacy Manager

Lorsque votre certificat Privacy Manager approche de l'expiration, vous recevez une notification indiquant que vous devez le renouveler :

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur un certificat Privacy Manager.
3. Cliquez sur **Renew certificate** (Renouveler le certificat).
4. Suivez les instructions à l'écran pour acheter un nouveau certificat Privacy Manager.

REMARQUE : Le processus de renouvellement d'un certificat Privacy Manager ne remplace pas l'ancien certificat Privacy Manager. Vous devez acheter un nouveau certificat Privacy Manager et l'installer à l'aide des mêmes procédures que dans la section Demande et installation d'un certificat Privacy Manager.

Définition d'un certificat Privacy Manager par défaut

Seuls les certificats Privacy Manager sont visibles dans le programme Privacy Manager, même si d'autres certificats émis par d'autres autorités de certification sont installés sur votre ordinateur.

Si vous possédez plusieurs certificats Privacy Manager sur votre ordinateur installés depuis le programme Privacy Manager, vous pouvez spécifier que l'un d'entre eux est le certificat par défaut :

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur le certificat Privacy Manager à utiliser comme certificat par défaut, puis cliquez sur **Set default** (Définir par défaut).
3. Cliquez sur **OK**.

REMARQUE : Il n'est pas obligatoire d'utiliser votre certificat Privacy Manager par défaut. Dans les diverses fonctions de Privacy Manager, vous pouvez sélectionner le certificat Privacy Manager de votre choix.

Suppression d'un certificat Privacy Manager

Si vous supprimez un certificat Privacy Manager, vous ne pourrez ni ouvrir les fichiers, ni afficher les données que vous aviez cryptés à l'aide de ce certificat. Si vous supprimez accidentellement un certificat Privacy Manager, vous pouvez le restaurer à l'aide du fichier de sauvegarde créé au moment de l'installation du certificat.

Pour supprimer un certificat Privacy Manager :

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur le certificat Privacy Manager à supprimer, puis sur **Avancé**.
3. Cliquez sur **Supprimer**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.
5. Cliquez sur **Fermer**, puis sur **Appliquer**.

Restauration d'un certificat Privacy Manager

Si vous supprimez accidentellement un certificat Privacy Manager, vous pouvez le restaurer à l'aide du fichier de sauvegarde créé au moment de l'installation ou de l'exportation du certificat :

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Import migration file** (Importer le fichier de migration).
3. Sur la page du fichier de migration, cliquez sur **Parcourir** pour rechercher le fichier .dppsm que vous avez créé lors de l'installation ou de l'exportation du certificat Privacy Manager, puis cliquez sur **Suivant**.
4. Sur la page d'importation du fichier de migration, cliquez sur **Terminer**.
5. Cliquez sur **Fermer**, puis sur **Appliquer**.

REMARQUE : Reportez-vous à la section Installation d'un certificat Privacy Manager ou Exportation d'un certificat Privacy Manager pour plus d'informations.

Révocation de votre certificat Privacy Manager

Si vous pensez que la sécurité de votre certificat Privacy Manager a été compromise, vous pouvez révoquer votre propre certificat :

REMARQUE : Un certificat Privacy Manager révoqué n'est pas supprimé. Le certificat reste utilisable pour afficher les fichiers cryptés.

1. Ouvrez Privacy Manager, puis cliquez sur **Certificate Manager** (Gestionnaire de certificats).
2. Cliquez sur **Avancé**.
3. Cliquez sur le certificat Privacy Manager à révoquer, puis sur **Revoke** (Révoquer).
4. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

5. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

6. Suivez les instructions à l'écran.

Gestion des contacts authentifiés

Les contacts authentifiés sont des utilisateurs avec lesquels vous avez échangé des certificats Privacy Manager, ce qui vous permet de communiquer avec eux en toute sécurité.

Ajout de contacts authentifiés

1. Vous envoyez une invitation par courrier électronique à un destinataire Contact authentifié.

2. Le destinataire Contact authentifié répond au courrier électronique.

3. Vous recevez la réponse par courrier électronique du destinataire Contact authentifié et vous cliquez sur Accepter.

Vous pouvez envoyer par courrier électronique des invitations de Contact authentifié à des destinataires individuels, ou adresser l'invitation à tous les contacts de votre carnet d'adresses Microsoft Outlook.

REMARQUE : Pour pouvoir répondre à votre invitation à devenir un Contact authentifié, les destinataires doivent disposer d'une copie de Privacy Manager installée sur leur ordinateur ou du client auxiliaire. Pour plus d'informations sur l'installation du client auxiliaire, consultez le site Web de DigitalPersona à l'adresse suivante : http://DigitalPersona.com/PrivacyManager.

Ajout d'un contact authentifié

1. Ouvrez Privacy Manager, cliquez sur **Trusted Contacts Manager** (Gestionnaire de contacts authentifiés), puis sur **Invite Contacts** (Inviter des contacts).

   – ou –

   Dans la barre d'outils de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis cliquez sur **Invite Contacts** (Inviter des contacts).

2. Si la boîte de dialogue de sélection du certificat s'affiche, cliquez sur le certificat Privacy Manager à utiliser, puis sur **OK**.

3. Lorsque la boîte de dialogue d'invitation d'un contact authentifié s'affiche, lisez le texte, puis cliquez sur **OK**.

   Un courrier électronique est automatiquement généré.

4. Saisissez une ou plusieurs adresses électroniques correspondant aux destinataires que vous souhaitez ajouter en tant que contacts authentifiés.

5. Modifiez le texte et signez avec votre nom (facultatif).

6. Cliquez sur **Envoyer**.

REMARQUE : Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous informe que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur OK pour lancer l'assistant de demande de certificat.

7. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

8. Lorsque vous recevez une réponse par courrier électronique d'un destinataire acceptant l'invitation à devenir un contact authentifié, cliquez sur Accepter dans le coin inférieur droit du courrier électronique.

   Une boîte de dialogue s'affiche pour confirmer que le destinataire a été correctement ajouté à la liste des contacts authentifiés.

9. Cliquez sur **OK**.

Ajout de contacts authentifiés à l'aide de votre carnet d'adresses Microsoft Outlook

1. Ouvrez Privacy Manager, cliquez sur **Trusted Contacts Manager** (Gestionnaire de contacts authentifiés), puis sur **Invite Contacts** (Inviter des contacts).

   – ou –

   Dans la barre d'outils de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis cliquez sur **Invite All My Outlook Contacts** (Inviter tous mes contacts Outlook).

2. Lorsque la page d'invitation de contact authentifié s'affiche, sélectionnez l'adresse électronique des destinataires que vous souhaitez ajouter en tant que contacts authentifiés, puis cliquez sur **Suivant**.

3. Lorsque la page d'envoi d'invitation s'affiche, cliquez sur **Terminer**.

   Un courrier électronique répertoriant les adresses électroniques Microsoft Outlook sélectionnées est généré automatiquement.

4. Modifiez le texte et signez avec votre nom (facultatif).

5. Cliquez sur **Envoyer**.

   REMARQUE : Si vous n'avez pas obtenu de certificat Privacy Manager, un message vous informe que vous devez disposer d'un certificat Privacy Manager pour envoyer une demande de contact authentifié. Cliquez sur **OK** pour lancer l'assistant de demande de certificat.

6. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

   REMARQUE : Lorsque le destinataire Contact authentifié reçoit le courrier électronique, il doit l'ouvrir et cliquer sur Accepter dans le coin inférieur droit du courrier électronique, puis sur OK lorsque la boîte de dialogue de confirmation s'affiche.

7. Lorsque vous recevez une réponse par courrier électronique d'un destinataire acceptant l'invitation à devenir un contact authentifié, cliquez sur Accepter dans le coin inférieur droit du courrier électronique.

   Une boîte de dialogue s'affiche pour confirmer que le destinataire a été correctement ajouté à la liste des contacts authentifiés.

8. Cliquez sur **OK**.

Affichage des détails d'un contact authentifié

1. Ouvrez Privacy Manager, puis cliquez sur **Trusted Contacts Manager** (Gestionnaire de contacts authentifiés).

2. Cliquez sur un contact authentifié.

3. Cliquez sur **Contact details** (Détails du contact).
4. Lorsque vous avez terminé de visualiser les détails, cliquez sur **OK**.

Suppression d'un contact authentifié

1. Ouvrez Privacy Manager, puis cliquez sur **Trusted Contacts Manager** (Gestionnaire de contacts authentifiés).
2. Cliquez sur le contact authentifié à supprimer.
3. Cliquez sur **Delete contact** (Supprimer le contact).
4. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Vérification de l'état de révocation d'un contact authentifié

1. Ouvrez Privacy Manager, puis cliquez sur **Trusted Contacts Manager** (Gestionnaire de contacts authentifiés).
2. Cliquez sur un contact authentifié.
3. Cliquez sur le bouton **Avancé**.

   La boîte de dialogue de gestion avancée des contacts authentifiés s'affiche.
4. Cliquez sur **Check Revocation** (Vérifier la révocation).
5. Cliquez sur **Fermer**.

Tâches générales

Utilisation de Privacy Manager dans Microsoft Office

Après l'installation de votre certificat Privacy Manager, un bouton Sign and Encrypt (Signer et crypter) apparaît sur le côté droit de la barre d'outils de tous les documents Microsoft Word, Microsoft Excel et Microsoft PowerPoint.

Configuration de Privacy Manager dans un document Microsoft Office

1. Ouvrez Privacy Manager, cliquez sur **Paramètres**, puis sur l'onglet **Documents**.

   – ou –

   Dans la barre d'outils d'un document Microsoft Office, cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Paramètres**.

2. Sélectionnez les actions à configurer, puis cliquez sur **OK**.

Signature d'un document Microsoft Office

1. Dans Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, créez et enregistrez un document.
2. Cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Sign Document** (Signer le document).
3. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
4. Lorsque la boîte de dialogue de confirmation s'affiche, lisez le texte, puis cliquez sur **OK**.

Si vous décidez par la suite de modifier le document, procédez comme suit :

1. Cliquez sur le bouton **Office** dans l'angle supérieur gauche de l'écran.
2. Cliquez sur **Préparer**, puis sur **Marquer comme final**.
3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui** et continuez à travailler.
4. Lorsque les modifications sont terminées, signez de nouveau le document.

Ajout d'une ligne de signature pour la signature d'un document Microsoft Word ou Microsoft Excel

Privacy Manager permet d'ajouter une ligne de signature lorsque vous signez un document Microsoft Word ou Microsoft Excel :

1. Dans Microsoft Word ou Microsoft Excel, créez et enregistrez un document.
2. Cliquez sur le menu **Accueil**.
3. Cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Add Signature Line Before Signing** (Ajouter une ligne de signature avant de signer).

REMARQUE : Une coche apparaît en regard de l'option Add Signature Line Before Signing (Ajouter une ligne de signature avant de signer) lorsque cette option est sélectionnée. Par défaut, cette option est activée.

4. Cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Sign Document** (Signer le document).

5. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Ajout de signataires suggérés à un document Microsoft Word ou Microsoft Excel

Vous pouvez ajouter plusieurs lignes de signature à votre document en désignant des signataires suggérés. Un signataire suggéré est un utilisateur désigné par le propriétaire d'un document Microsoft Word ou Microsoft Excel pour ajouter une ligne de signature au document. Les signataires suggérés peuvent être vous-même, ou toute autre personne que vous souhaitez indiquer comme pouvant signer votre document. Si par exemple vous préparez un document devant être signé par tous les membres de votre service, vous pouvez inclure des lignes de signature pour ces utilisateurs en bas de la dernière page du document avec des instructions de signature pour une date précise.

Pour ajouter un signataire suggéré à un document Microsoft Word ou Microsoft Excel :

1. Dans Microsoft Word ou Microsoft Excel, créez et enregistrez un document.

2. Cliquez sur le menu **Insertion**.

3. Dans le groupe **Texte** de la barre d'outils, cliquez sur la flèche située en regard de **Ligne de signature**, puis sur **Privacy Manager Signature Provider** (Fournisseur de signatures Privacy Manager).

   La boîte de dialogue Signature Setup (Configuration de signature) s'affiche.

4. Dans la zone sous **Suggested signer** (Signataire suggéré), saisissez le nom du signataire suggéré.

5. Dans la zone sous **Instructions to the signer** (Instructions destinées au signataire), saisissez un message pour ce signataire suggéré.

REMARQUE : Ce message apparaît en remplacement d'un titre. Il est supprimé ou remplacé par le titre de l'utilisateur au moment de la signature du document.

6. Cochez la case **Show sign date in signature line** (Afficher la date dans la ligne de signature) pour afficher la date.

7. Cochez la case **Show signer's title in signature line** (Afficher le titre du signataire dans la ligne de signature) pour afficher le titre.

REMARQUE : Puisque le propriétaire du document attribue des signataires suggérés à son document, si les cases à cocher **Afficher la date dans la ligne de signature** et/ou **Show signer's title in signature line** (Afficher le titre du signataire dans la ligne de signature) ne sont pas cochées, le signataire suggéré ne peut pas afficher la date et/ou son titre dans la ligne de signature, même si les paramètres du document du signataire suggéré sont configurés dans cette optique.

8. Cliquez sur **OK**.

Ajout d'une ligne de signature de signataire suggéré

Lorsqu'un signataire suggéré ouvre le document, il voit son nom apparaître entre crochets, ce qui indique que sa signature est requise.

Pour signer le document :

1. Double-cliquez sur la ligne de signature appropriée.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

   La ligne de signature apparaît en fonction des paramètres spécifiés par le propriétaire du document.

Cryptage d'un document Microsoft Office

Vous pouvez crypter un document Microsoft Office pour vous et vos contacts authentifiés. Lorsque vous cryptez un document et le fermez, vous et le(s) contact(s) authentifié(s) sélectionné(s) dans la liste devez vous authentifier avant l'ouverture.

Pour crypter un document Microsoft Office :

1. Dans Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, créez et enregistrez un document.
2. Cliquez sur le menu **Accueil**.
3. Cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Encrypt Document** (Crypter le document).

   La boîte de dialogue de sélection des contacts authentifiés s'affiche.
4. Cliquez sur le nom d'un contact authentifié qui pourra ouvrir le document et afficher son contenu.

REMARQUE : Pour sélectionner plusieurs noms de contacts authentifiés, maintenez la touche ctrl enfoncée et cliquez sur chaque nom.

5. Cliquez sur **OK**.
6. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Si vous décidez par la suite de modifier le document, suivez les étapes présentées à la section **Signature d'un document Microsoft Office**. Lorsque le cryptage est supprimé, vous pouvez modifier le document. Suivez les étapes de cette section pour crypter à nouveau le document.

Suppression du cryptage d'un document Microsoft Office

Lorsque vous supprimez le cryptage d'un document Microsoft Office, vous et vos contacts authentifiés n'avez plus besoin de vous authentifier pour ouvrir le document et afficher son contenu.

Pour supprimer le cryptage d'un document Microsoft Office :

1. Ouvrez un document Microsoft Word, Microsoft Excel ou Microsoft PowerPoint crypté.
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
3. Cliquez sur le menu **Accueil**.
4. Cliquez sur la flèche vers le bas située en regard de **Sign and Encrypt** (Signer et crypter), puis sur **Remove Encryption** (Supprimer le cryptage).

Envoi d'un document Microsoft Office crypté

Vous pouvez joindre un document Microsoft Office crypté à un message électronique sans avoir à signer ni à crypter le message en lui-même. Pour cela, créez et envoyez un courrier électronique contenant

un document signé et crypté exactement de la même façon que pour un courrier électronique classique contenant une pièce jointe.

Cependant, pour une sécurité optimale, il est recommandé de crypter le courrier électronique lorsque vous joignez un document Microsoft Office signé ou crypté.

Pour envoyer un courrier électronique scellé avec un document Microsoft Office signé et/ou crypté en pièce jointe, procédez comme suit :

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.
3. Joignez le document Microsoft Office.
4. Pour obtenir des instructions supplémentaires, reportez-vous à la section Scellage et envoi d'un message électronique.

Affichage d'un document Microsoft Office signé

REMARQUE : Vous devez posséder un certificat Privacy Manager pour afficher un document Microsoft Office signé.

Lorsqu'un document Microsoft Office signé est ouvert, une boîte de dialogue Signatures s'ouvre en regard du document et affiche le nom de l'utilisateur ayant signé le document ainsi que la date de signature. Vous pouvez cliquer avec le bouton droit sur le nom pour afficher des détails supplémentaires.

Affichage d'un document Microsoft Office crypté

Pour afficher un document Microsoft Office crypté sur un autre ordinateur, Privacy Manager doit être installé sur celui-ci. En outre, vous devez importer le certificat Privacy Manager utilisé pour crypter le fichier.

Un contact authentifié souhaitant afficher un document Microsoft Office crypté doit posséder un certificat Privacy Manager ainsi qu'une copie installée de Privacy Manager sur son ordinateur. De plus, le contact authentifié doit être sélectionné par le propriétaire du document Microsoft Office crypté.

Utilisation de Privacy Manager dans Microsoft Outlook

Lorsque Privacy Manager est installé, un bouton Privacy (Confidentialité) apparaît dans la barre d'outils de Microsoft Outlook et un bouton Send Securely (Envoyer en toute sécurité) apparaît dans la barre d'outils de chaque message électronique Microsoft Outlook.

Configuration de Privacy Manager pour Microsoft Outlook

1. Ouvrez **Privacy Manager**, cliquez sur **Paramètres**, puis sur l'onglet **E-mail** (Courrier électronique).

   – ou –

   Dans la barre d'outils principale de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Privacy** (Confidentialité), puis sur **Paramètres**.

   – ou –

   Dans la barre d'outils d'un message électronique Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis sur **Paramètres**.

2. Sélectionnez les actions à effectuer lors de l'envoi d'un courrier électronique sécurisé, puis cliquez sur **OK**.

Signature et envoi d'un message électronique

- Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
- Saisissez votre message électronique.
- Cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis cliquez sur **Sign and Send** (Signer et envoyer).
- Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Scellage et envoi d'un message électronique

Les messages électroniques scellés que vous signez et scellez numériquement (cryptez) ne peuvent être affichés que par les personnes choisies dans votre liste de contacts authentifiés.

Pour sceller et envoyer un message électronique à un contact authentifié :

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.
2. Saisissez votre message électronique.
3. Cliquez sur la flèche vers le bas située en regard de **Send Securely** (Envoyer en toute sécurité), puis cliquez sur **Seal for Trusted Contacts and Send** (Sceller pour les contacts authentifiés et envoyer).
4. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

Affichage d'un message électronique scellé

Lorsque vous ouvrez un message électronique scellé, l'étiquette de sécurité s'affiche dans l'en-tête du message. L'étiquette de sécurité propose les informations suivantes :

- Informations d'authentification utilisées pour vérifier l'identité de la personne ayant signé le courrier électronique
- Produit utilisé pour vérifier les informations d'authentification de la personne ayant signé le courrier électronique

Utilisation de Privacy Manager dans Windows Live Messenger

Ajout d'une activité Privacy Manager Chat

Pour ajouter la fonction Privacy Manager Chat à Windows Live Messenger, procédez comme suit :

1. Connectez-vous à l'Accueil Windows Live.
2. Cliquez sur l'icône **Windows Live**, puis sur **Services Windows Live**.
3. Cliquez sur **Galerie**, puis sur **Messenger**.
4. Cliquez sur **Activités**, puis sur **Sécurité**.
5. Cliquez sur **Privacy Manager Chat**, puis suivez les instructions à l'écran.

Démarrage de Privacy Manager Chat

REMARQUE : Pour utiliser Privacy Manager Chat, les deux parties doivent installer Privacy Manager et posséder un certificat Privacy Manager. Pour plus d'informations sur l'installation d'un certificat Privacy Manager, voir la rubrique Demande et installation d'un certificat Privacy Manager à la page 5.

1. Pour démarrer Privacy Manager Chat dans Windows Live Messenger, appliquez l'une des procédures suivantes :

   a. Cliquez avec le bouton droit sur un contact en ligne dans Live Messenger, puis sélectionnez **Démarrer une activité**.

   b. Cliquez sur **Start Privacy Manager Chat** (Démarrer Privacy Manager Chat).

   – ou –

   a. Double-cliquez sur un contact en ligne dans Live Messenger, puis cliquez sur le menu **Conversation**.

   b. Cliquez sur **Action**, puis sur **Start Privacy Manager Chat** (Démarrer Privacy Manager Chat).

   Privacy Manager envoie une invitation au contact pour le démarrage de Privacy Manager Chat. Lorsque le contact invité accepte, la fenêtre Privacy Manager Chat s'ouvre. Si le contact invité ne possède pas Privacy Manager, il est invité à le télécharger.

2. Cliquez sur **Start** (Démarrer) pour commencer une session de messagerie instantanée sécurisée.

Configuration de Privacy Manager Chat pour Windows Live Messenger

1. Dans Privacy Manager Chat, cliquez sur le bouton **Paramètres**.

   – ou –

   Dans Privacy Manager, cliquez sur **Paramètres**, puis sur l'onglet **Chat**.

   – ou –

   Dans la visionneuse d'historique de Privacy Manager, cliquez sur le bouton **Paramètres**.

2. Pour préciser la durée devant s'écouler avant que Privacy Manager Chat ne verrouille votre session, sélectionnez un nombre dans la zone **Lock session after _ minutes of inactivity** (Verrouiller la session après _ minutes d'inactivité).

3. Pour spécifier un dossier d'historique pour vos sessions de messagerie instantanée, cliquez sur **Parcourir** pour rechercher un dossier, puis cliquez sur **OK**.

4. Pour crypter et enregistrer automatiquement vos sessions lorsque vous les fermez, cochez la case **Automatically save secure chat history** (Enregistrer automatiquement l'historique de conversation sécurisée).

5. Cliquez sur **OK**.

Messagerie instantanée dans la fenêtre Privacy Manager Chat

Après le démarrage de Privacy Manager Chat, une fenêtre Privacy Manager Chat s'ouvre dans Windows Live Messenger. L'utilisation de Privacy Manager Chat est similaire à l'utilisation de base de Windows Live Messenger, à ceci près que les fonctions supplémentaires suivantes sont disponibles dans la fenêtre Privacy Manager Chat :

- **Enregistrer** : cliquez sur ce bouton pour enregistrer votre session de messagerie instan,tanée dans le dossier spécifié au niveau des paramètres de configuration. Vous pouvez également configurer Privacy Manager Chat de manière à ce que chaque session soit automatiquement enregistrée à la fermeture.
- **Masquer tout** et **Afficher tout** : cliquez sur le bouton approprié pour développer ou réduire les messages présentés dans la fenêtre Secure Communications (Communications sécurisées). Vous pouvez également masquer ou afficher des messages individuels en cliquant sur l'en-tête du message.
- **Es-tu là ?** : cliquez sur ce bouton pour demander à votre contact de s'authentifier.
- **Verrouiller** : cliquez sur ce bouton pour fermer la fenêtre Privacy Manager Chat et retourner dans la fenêtre Chat Entry (Entrée de messagerie instantanée). Pour afficher de nouveau la fenêtre Secure Communications (Communications sécurisées), cliquez sur **Resume the session** (Reprendre la session), puis authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
- **Envoyer** : cliquez sur ce bouton pour envoyer un message crypté à votre contact.
- **Envoyer le message signé** : cochez cette case pour signer et crypter électroniquement vos messages. Si par la suite le message est falsifié, il est marqué comme non valide lorsque le destinataire le reçoit. Vous devez vous authentifier chaque fois que vous envoyez un message signé.
- **Envoyer le message masqué** : cochez cette case pour crypter et envoyer un message affichant uniquement le titre du message. Votre contact doit s'authentifier pour lire le contenu du message.

Affichage de l'historique de messagerie instantanée

La visionneuse d'historique de Privacy Manager Chat affiche les fichiers cryptés des sessions Privacy Manager Chat. Les sessions peuvent être enregistrées en cliquant sur Enregistrer dans la fenêtre Privacy Manager Chat ou en configurant un enregistrement automatique au niveau de l'onglet Chat de Privacy Manager. Dans la visionneuse, chaque session présente le nom d'écran (crypté) du contact ainsi que les dates et heures de début et de fin de la session. Par défaut, les sessions sont présentées pour tous les comptes de messagerie configurés. Vous pouvez utiliser le menu **Display history for** (Afficher l'historique de) pour sélectionner uniquement des comptes spécifiques.

Démarrage de la visionneuse d'historique de Privacy Manager Chat

1. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.

2. Cliquez sur **Privacy Manager : Sign and Chat**, puis sur **Chat History Viewer** (Visionneuse d'historique de messagerie instantanée).

– ou –

▲ Dans une session de messagerie instantanée, cliquez sur **History Viewer** (Visionneuse d'historique) ou sur **History** (Historique).

– ou –

▲ Sur la page de configuration de la messagerie instantanée, cliquez sur **Start Live Messenger History Viewer** (Démarrer la visionneuse d'historique Live Messenger).

Révélation de toutes les sessions

La fonction de révélation de toutes les sessions permet d'afficher le nom d'écran décrypté des contacts pour la ou les sessions actuellement sélectionnées ou pour toutes les sessions du même compte.

1. Dans la visionneuse d'historique de messagerie instantanée, cliquez avec le bouton droit sur une session de votre choix, puis sélectionnez **Reveal All Sessions** (Révéler toutes les sessions).
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

   Les noms d'écran des contacts sont décryptés.
3. Double-cliquez sur une session de votre choix pour afficher son contenu.

Révélation des sessions d'un compte spécifique

La fonction de révélation d'une session permet d'afficher le nom d'écran décrypté du contact pour la session actuellement sélectionnée.

1. Dans la visionneuse d'historique de messagerie instantanée, cliquez avec le bouton droit sur une session de votre choix, puis sélectionnez **Reveal Session** (Révéler la session).
2. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

   Les noms d'écran des contacts sont décryptés.
3. Double-cliquez sur la session révélée pour afficher son contenu.

REMARQUE : D'autres sessions cryptées avec le même certificat présentent une icône de déverrouillage, ce qui indique que vous pouvez les afficher en double-cliquant sur l'une de ces sessions sans avoir à vous authentifier de nouveau. Les sessions cryptées à l'aide d'un certificat différent présentent une icône de verrouillage, ce qui indique qu'une authentification est requise pour ces sessions avant l'affichage des noms d'écran des contacts ou du contenu.

Affichage d'un ID de session

▲ Dans l'affichage de l'historique de messagerie instantanée, cliquez avec le bouton droit sur une session révélée de votre choix, puis sélectionnez **View session ID** (Afficher l'ID de session).

Affichage d'une session

L'affichage d'une session ouvre le fichier pour visualisation. Si la session n'a pas été précédemment révélée (nom d'écran du contact apparaissant décrypté), elle l'est à ce stade.

1. Dans la visionneuse d'historique de messagerie instantanée, cliquez avec le bouton droit sur une session révélée de votre choix, puis sélectionnez **Afficher**.
2. Si vous y êtes invité, authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.

   Le contenu de la session est décrypté.

Recherche de texte spécifique dans des sessions

Vous pouvez uniquement rechercher du texte dans les sessions révélées (décryptés) affichées dans la fenêtre de la visionneuse. Il s'agit des sessions pour lesquelles le nom d'écran du contact apparaît en texte normal.

1. Dans la visionneuse d'historique de messagerie instantanée, cliquez sur le bouton **Search** (Rechercher).
2. Saisissez le texte de la recherche, configurez les paramètres de recherche souhaités, puis cliquez sur **OK**.

   Les sessions contenant le texte recherché sont surlignées dans la fenêtre de la visionneuse.

Suppression d'une session

1. Sélectionnez une session d'historique de messagerie instantanée.
2. Cliquez sur **Supprimer**.

Ajout ou suppression de colonnes

Par défaut, les trois colonnes les plus utilisées sont affichées dans la visionneuse d'historique de messagerie instantanée. Vous pouvez ajouter des colonnes supplémentaires à l'affichage ou en supprimer.

Pour ajouter des colonnes à l'affichage :

1. Cliquez avec le bouton droit sur un titre de colonne, puis sélectionnez **Add/Remove Columns** (Ajouter/supprimer des colonnes).
2. Sélectionnez un titre de colonne dans le volet de gauche, puis cliquez sur **Ajouter** pour le déplacer vers le volet de droite.

Pour supprimer des colonnes de l'affichage :

1. Cliquez avec le bouton droit sur un titre de colonne, puis sélectionnez **Add/Remove Columns** (Ajouter/supprimer des colonnes).
2. Sélectionnez un titre de colonne dans le volet de droite, puis cliquez sur **Supprimer** pour le déplacer vers le volet de gauche.

Sessions affichées par filtre

Une liste des sessions de tous vos comptes est affichée dans la visionneuse d'historique de messagerie instantanée.

Affichage des sessions d'un compte spécifique

- Dans la visionneuse d'historique de messagerie instantanée, sélectionnez un compte dans le menu **Display history for** (Afficher l'historique de).

Affichage des sessions pour une plage de dates

1. Dans l'affichage de l'historique de messagerie instantanée, cliquez sur l'icône **Advanced Filter** (Filtre avancé).

   La boîte de dialogue de filtre avancé s'affiche.

2. Cochez la case **Display only sessions within specified date range** (Afficher uniquement les sessions de la plage de dates spécifiée).

3. Dans les cases **From date** (De) et **To date** (A), saisissez le jour, le mois et/ou l'année ou cliquez sur la flèche située en regard du calendrier pour sélectionner les dates.

4. Cliquez sur **OK**.

Affichage des sessions enregistrées dans un dossier autre que le dossier par défaut

1. Dans l'affichage de l'historique de messagerie instantanée, cliquez sur l'icône **Advanced Filter** (Filtre avancé).

2. Cochez la case **Use an alternate history files folder** (Utiliser un autre dossier de fichiers d'historique).

3. Saisissez l'emplacement du dossier ou cliquez sur **Parcourir** pour rechercher un dossier.

4. Cliquez sur **OK**.

Tâches avancées

Migration de certificats Privacy Manager et de contacts authentifiés vers un autre ordinateur

Vous pouvez assurer en toute sécurité la migration de vos certificats Privacy Manager et contacts authentifiés vers un autre ordinateur. Pour cela, exportez-les sous la forme d'un fichier protégé par mot de passe vers un emplacement réseau ou tout périphérique de stockage amovible, puis importez le fichier sur le nouvel ordinateur.

Exportation de certificats Privacy Manager et de contacts authentifiés

Pour exporter vos certificats Privacy Manager et contacts authentifiés vers un fichier protégé par mot de passe, procédez comme suit :

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Export migration file** (Exporter le fichier de migration).
3. Sur la page de sélection des données, sélectionnez les catégories de données à inclure dans le fichier de migration, puis cliquez sur **Suivant**.
4. Sur la page du fichier de migration, saisissez un nom de fichier ou cliquez sur **Parcourir** pour rechercher un emplacement, puis cliquez sur **Suivant**.
5. Saisissez et confirmez un mot de passe, puis cliquez sur **Suivant**.

REMARQUE : Conservez le mot de passe en lieu sûr, car il sera nécessaire pour importer le fichier de migration.

6. Authentifiez-vous à l'aide de la méthode de connexion sécurisée choisie.
7. Sur la page d'enregistrement du fichier de migration, cliquez sur **Terminer**.

Importation de certificats Privacy Manager et de contacts authentifiés

Pour importer vos certificats Privacy Manager et contacts authentifiés dans un fichier protégé par mot de passe, procédez comme suit :

1. Ouvrez Privacy Manager, puis cliquez sur **Migration**.
2. Cliquez sur **Import migration file** (Importer le fichier de migration).
3. Sur la page de sélection des données, sélectionnez les catégories de données à inclure dans le fichier de migration, puis cliquez sur **Suivant**.
4. Sur la page du fichier de migration, saisissez un nom de fichier ou cliquez sur **Parcourir** pour rechercher un emplacement, puis cliquez sur **Suivant**.
5. Sur la page d'importation du fichier de migration, cliquez sur **Terminer**.

5 File Sanitizer for HP ProtectTools

File Sanitizer est un outil qui vous permet de détruire des ressources en toute sécurité (informations personnelles ou fichiers, données historiques ou de navigation sur le Web ou autres composants de données) sur votre ordinateur et de nettoyer régulièrement votre disque dur.

REMARQUE : Actuellement, File Sanitizer fonctionne uniquement sur le disque dur.

A propos de la destruction

La suppression d'une ressource sous Windows ne retire pas intégralement le contenu de la ressource de votre disque dur. Windows supprime uniquement la référence à la ressource. Le contenu de la ressource reste présent sur le disque dur jusqu'à ce qu'une autre ressource remplace cette même zone du disque dur par de nouvelles informations.

La destruction diffère d'une suppression standard sous Windows® (ou suppression simple dans File Sanitizer), dans le sens où lorsque vous détruisez une ressource, un algorithme de brouillage des données est appelé afin de rendre virtuellement impossible la récupération de la ressource d'origine.

Lorsque vous choisissez un profil de destruction (High Security, Medium Security ou Low Security), une liste prédéfinie de ressources et une méthode d'effacement sont automatiquement sélectionnées pour la destruction. Vous pouvez également personnaliser un profil de destruction, ce qui vous permet de spécifier le nombre de cycles de destruction, les ressources à inclure dans la destruction, les ressources exigeant une confirmation avant la destruction et les ressources à exclure de la destruction.

Vous pouvez configurer une planification de destruction automatique, ou détruire manuellement des ressources lorsque vous le souhaitez.

Le nettoyage de l'espace libre vous permet d'écrire en toute sécurité des données aléatoires par-dessus les ressources supprimées, afin d'empêcher les utilisateurs d'en consulter le contenu d'origine.

A propos du nettoyage de l'espace libre

REMARQUE : Le nettoyage de l'espace libre concerne les ressources supprimées à l'aide de la Corbeille de Windows ou par le biais d'une suppression manuelle. Le nettoyage de l'espace libre n'apporte aucune sécurité supplémentaire aux ressources détruites.

Vous pouvez configurer une planification de nettoyage de l'espace libre automatique ou activer manuellement le nettoyage à l'aide de l'icône HP ProtectTools de la zone de notification, à l'extrémité droite de la barre des tâches.

Procédures de configuration

Ouverture de File Sanitizer

Pour ouvrir File Sanitizer :

1. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Cliquez sur **File Sanitizer**.

   – ou –

- Double-cliquez sur l'icône **File Sanitizer**.

  – ou –

- Cliquez avec le bouton droit sur l'icône HP ProtectTools située dans la zone de notification, à l'extrémité droite de la barre des tâches, cliquez sur File Sanitizer, puis sur Open File Sanitizer (Ouvrir File Sanitizer).

Configuration d'une planification de destruction

1. Ouvrez File Sanitizer, puis cliquez sur **Shred** (Détruire).
2. Sélectionnez une option de destruction :

   - **Windows startup** (Démarrage de Windows) : choisissez cette option pour détruire toutes les ressources sélectionnées au démarrage de Windows.
   - **Windows shutdown** (Arrêt de Windows) : choisissez cette option pour détruire toutes les ressources sélectionnées à l'arrêt de Windows.

     REMARQUE : Lorsque cette option est sélectionnée, une boîte de dialogue apparaît à l'arrêt de Windows pour vous demander si vous souhaitez continuer la destruction des ressources sélectionnées ou ignorer la procédure. Cliquez sur **Oui** pour ignorer la procédure de destruction ou sur **Non** pour continuer la destruction.

   - **Web browser open** (Ouverture de navigateur Web) : choisissez cette option pour détruire toutes les ressources Web sélectionnées, par exemple l'historique des URL de navigateur, à l'ouverture d'un navigateur Web.
   - **Web browser quit** (Fermeture de navigateur Web) : choisissez cette option pour détruire toutes les ressources Web sélectionnées, par exemple l'historique des URL de navigateur, à la fermeture d'un navigateur Web.
   - **Scheduler** (Planificateur) : cochez la case Activate Scheduler (Activer le planificateur), saisissez votre mot de passe Windows, puis saisissez un jour et une heure pour la destruction des ressources sélectionnées.
3. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration d'une planification de nettoyage de l'espace libre

REMARQUE : Le nettoyage de l'espace libre concerne les ressources supprimées à l'aide de la Corbeille de Windows ou celles supprimées manuellement. Le nettoyage de l'espace libre n'apporte aucune sécurité supplémentaire aux ressources détruites.

Pour configurer une planification de nettoyage de l'espace libre :

1. Ouvrez File Sanitizer, puis cliquez sur **Free Space Bleaching** (Nettoyage de l'espace libre).
2. Cochez la case **Activate Scheduler** (Activer le planificateur), saisissez votre mot de passe Windows, puis saisissez un jour et une heure pour le nettoyage de votre disque dur.
3. Cliquez sur **Appliquer**, puis sur **OK**.

REMARQUE : L'opération de nettoyage de l'espace libre peut être longue. Bien que le nettoyage de l'espace libre soit exécuté en arrière-plan, votre ordinateur peut être plus lent en raison de l'utilisation plus importante du processeur.

Sélection ou création d'un profil de destruction

Vous pouvez préciser une méthode d'effacement et sélectionner les ressources à détruire en sélectionnant un profil prédéfini ou en créant votre propre profil.

Sélection d'un profil de destruction prédéfini

Lorsque vous choisissez un profil de destruction prédéfini (High Security, Medium Security ou Low Security), une méthode d'effacement et une liste de ressources prédéfinies sont automatiquement sélectionnées. Vous pouvez cliquer sur le bouton Détails pour afficher la liste prédéfinie des ressources sélectionnées pour la destruction.

Pour sélectionner un profil de destruction prédéfini :

1. Ouvrez **File Sanitizer** et cliquez sur **Settings** (Paramètres).
2. Cliquez sur un profil de destruction prédéfini.
3. Cliquez sur **Détails** pour afficher la liste prédéfinie des ressources sélectionnées pour la destruction.
4. Sous **Shred the following** (Détruire les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la destruction.
5. Cliquez sur **Annuler**, puis sur **OK**.

Personnalisation d'un profil de destruction

Lorsque vous créez un profil de destruction, vous spécifiez le nombre de cycles de destruction, les ressources à inclure dans la destruction, les ressources exigeant une confirmation avant la destruction et les ressources à exclure de la destruction :

1. Ouvrez File Sanitizer, puis cliquez sur **Settings** (Paramètres). Cliquez sur **Advanced Security Settings** (Paramètres de sécurité avancés), puis sur **Détails**.
2. Spécifiez le nombre de cycles de destruction.

REMARQUE : Le nombre sélectionné pour les cycles de destruction s'applique à chaque ressource. Par exemple, si vous choisissez trois cycles de destruction, un algorithme de brouillage des données est appliqué à trois reprises. Si vous choisissez les cycles de destruction de sécurité élevée, la destruction peut durer un certain temps. Cependant, plus le nombre de cycles de destruction est élevé, plus votre ordinateur est sécurisé.

3. Sélectionnez les ressources à détruire :
   a. Sous **Available shred options** (Options de destruction disponibles), cliquez sur une ressource, puis sur **Add** (Ajouter).
   b. Pour ajouter une ressource personnalisée, cliquez sur Add Custom Option (Ajouter une option personnalisée), saisissez un nom de fichier ou de dossier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Add** (Ajouter).

REMARQUE : Pour supprimer une ressource des options de destruction disponibles, cliquez sur la ressource, puis sur **Supprimer**.

4. Sous **Shred the following** (Détruire les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la destruction.

REMARQUE : Pour retirer une ressource de la liste de destruction, cliquez sur la ressource, puis sur **Supprimer**.

5. Sous **Do not shred the following** (Ne pas détruire les éléments suivants), cliquez sur **Add** (Ajouter) pour sélectionner les ressources spécifiques à exclure de la destruction.

REMARQUE : Seules les extensions de fichiers peuvent être exclues de la destruction. Par exemple, si vous ajoutez l'extension de fichier .BMP, tous les fichiers portant l'extension .BMP seront exclus de la destruction.

Pour retirer une ressource de la liste des exclusions, cliquez sur la ressource, puis sur **Supprimer**.

6. Lorsque vous avez terminé la configuration du profil de destruction, cliquez sur **Appliquer**, puis sur **OK**.

Personnalisation d'un profil de suppression simple

Le profil de suppression simple effectue une suppression standard des ressources, sans destruction. Lorsque vous personnalisez un profil de suppression simple, vous spécifiez les ressources à inclure dans la suppression simple, les ressources exigeant une confirmation avant l'exécution de la suppression simple et les ressources à exclure de la suppression simple :

REMARQUE : Il est fortement recommandé d'exécuter régulièrement un nettoyage de l'espace libre si vous utilisez l'option de suppression simple.

1. Ouvrez **File Sanitizer**, cliquez sur **Settings** (Paramètres), cliquez sur **Simple Delete Setting** (Paramètre de suppression simple), puis sur **Détails**.
2. Sélectionnez les ressources à supprimer :
   a. Sous **Available delete options** (Options de suppression disponibles), cliquez sur une ressource, puis sur **Add** (Ajouter).
   b. Pour ajouter une ressource personnalisée, cliquez sur **Add Custom Option** (Ajouter une option personnalisée), saisissez un nom de fichier ou de dossier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Add** (Ajouter).

   REMARQUE : Pour supprimer une ressource des options de suppression disponibles, cliquez sur la ressource, puis sur **Supprimer**.
3. Sous **Delete the following** (Supprimer les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la suppression.

REMARQUE : Pour retirer une ressource de la liste de suppression, cliquez sur la ressource, puis sur **Supprimer**.

4. Sous **Do not shred the following** (Ne pas détruire les éléments suivants), cliquez sur **Add** (Ajouter) pour sélectionner les ressources spécifiques à exclure de la destruction.

REMARQUE : Seules les extensions de fichiers peuvent être exclues de la suppression. Par exemple, si vous ajoutez l'extension de fichier .BMP, tous les fichiers portant l'extension .BMP seront exclus de la suppression.

Pour retirer une ressource de la liste des exclusions, cliquez sur la ressource, puis sur **Supprimer**.

5. Lorsque vous avez terminé la configuration du profil de suppression simple, cliquez sur **Appliquer**, puis sur **OK**.

Configuration d'une planification de destruction

1. Ouvrez File Sanitizer, puis cliquez sur **Shred** (Détruire).
2. Sélectionnez une option de destruction :
   - **Windows startup** (Démarrage de Windows) : choisissez cette option pour détruire toutes les ressources sélectionnées au démarrage de Windows.
   - **Windows shutdown** (Arrêt de Windows) : choisissez cette option pour détruire toutes les ressources sélectionnées à l'arrêt de Windows.

     REMARQUE : Lorsque cette option est sélectionnée, une boîte de dialogue apparaît à l'arrêt de Windows pour vous demander si vous souhaitez continuer la destruction des ressources sélectionnées ou ignorer la procédure. Cliquez sur Oui pour ignorer la procédure de destruction ou sur Non pour continuer la destruction.
   - **Web browser open** (Ouverture de navigateur Web) : choisissez cette option pour détruire toutes les ressources Web sélectionnées, par exemple l'historique des URL de navigateur, à l'ouverture d'un navigateur Web.

- **Web browser quit** (Fermeture de navigateur Web) : choisissez cette option pour détruire toutes les ressources Web sélectionnées, par exemple l'historique des URL de navigateur, à la fermeture d'un navigateur Web.
- **Scheduler** (Planificateur) : cochez la case Activate Scheduler (Activer le planificateur), saisissez votre mot de passe Windows, puis saisissez un jour et une heure pour la destruction des ressources sélectionnées.

3. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration d'une planification de nettoyage de l'espace libre

REMARQUE : Le nettoyage de l'espace libre concerne les ressources supprimées à l'aide de la Corbeille de Windows ou celles supprimées manuellement. Le nettoyage de l'espace libre n'apporte aucune sécurité supplémentaire aux ressources détruites.

Pour configurer une planification de nettoyage de l'espace libre :

1. Ouvrez File Sanitizer, puis cliquez sur **Free Space Bleaching** (Nettoyage de l'espace libre).
2. Cochez la case **Activate Scheduler** (Activer le planificateur), saisissez votre mot de passe Windows, puis saisissez un jour et une heure pour le nettoyage de votre disque dur.
3. Cliquez sur **Appliquer**, puis sur **OK**.

REMARQUE : L'opération de nettoyage de l'espace libre peut être longue. Bien que le nettoyage de l'espace libre soit exécuté en arrière-plan, votre ordinateur peut être plus lent en raison de l'utilisation plus importante du processeur.

Sélection ou création d'un profil de destruction

Sélection d'un profil de destruction prédéfini

Lorsque vous choisissez un profil de destruction prédéfini (High Security, Medium Security ou Low Security), une méthode d'effacement et une liste de ressources prédéfinies sont automatiquement sélectionnées. Vous pouvez cliquer sur le bouton Détails pour afficher la liste prédéfinie des ressources sélectionnées pour la destruction.

Pour sélectionner un profil de destruction prédéfini :

1. Ouvrez **File Sanitizer** et cliquez sur **Settings** (Paramètres).
2. Cliquez sur un profil de destruction prédéfini.
3. Cliquez sur **Détails** pour afficher la liste prédéfinie des ressources sélectionnées pour la destruction.
4. Sous **Shred the following** (Détruire les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la destruction.
5. Cliquez sur **Annuler**, puis sur **OK**.

Personnalisation d'un profil de destruction

Lorsque vous créez un profil de destruction, vous spécifiez le nombre de cycles de destruction, les ressources à inclure dans la destruction, les ressources exigeant une confirmation avant la destruction et les ressources à exclure de la destruction :

1. Ouvrez File Sanitizer, puis cliquez sur **Paramètres**. Cliquez sur **Advanced Security Settings** (Paramètres de sécurité avancés), puis sur **Détails**.
2. Spécifiez le nombre de cycles de destruction.

REMARQUE : Le nombre sélectionné pour les cycles de destruction s'applique à chaque ressource. Par exemple, si vous choisissez trois cycles de destruction, un algorithme d'obscurcissement des données est exécuté à trois reprises séparées. Si vous choisissez les cycles de destruction de sécurité élevée, la destruction peut durer un certain temps. Cependant, plus le nombre de cycles de destruction est élevé, plus votre ordinateur est sécurisé.

3. Sélectionnez les ressources à détruire :
   a. Sous **Available shred options** (Options de destruction disponibles), cliquez sur une ressource, puis sur **Add** (Ajouter).
   b. Pour ajouter une ressource personnalisée, cliquez sur Add Custom Option (Ajouter une option personnalisée), saisissez un nom de fichier ou de dossier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Add** (Ajouter).

REMARQUE : Pour supprimer une ressource des options de destruction disponibles, cliquez sur la ressource, puis sur **Supprimer**.

4. Sous **Shred the following** (Détruire les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la destruction.

REMARQUE : Pour retirer une ressource de la liste de destruction, cliquez sur la ressource, puis sur **Supprimer**.

5. Sous **Do not shred the following** (Ne pas détruire les éléments suivants), cliquez sur **Add** (Ajouter) pour sélectionner les ressources spécifiques à exclure de la destruction.

REMARQUE : Seules les extensions de fichiers peuvent être exclues de la destruction. Par exemple, si vous ajoutez l'extension de fichier .BMP, tous les fichiers portant l'extension .BMP seront exclus de la destruction.

Pour retirer une ressource de la liste des exclusions, cliquez sur la ressource, puis sur **Supprimer**.

6. Lorsque vous avez terminé la configuration du profil de destruction, cliquez sur **Appliquer**, puis sur **OK**.

Personnalisation d'un profil de suppression simple

Le profil de suppression simple effectue une suppression standard des ressources, sans destruction. Lorsque vous personnalisez un profil de suppression simple, vous spécifiez les ressources à inclure dans la suppression simple, les ressources exigeant une confirmation avant l'exécution de la suppression simple et les ressources à exclure de la suppression simple :

REMARQUE : Il est fortement recommandé d'exécuter régulièrement un nettoyage de l'espace libre si vous utilisez l'option de suppression simple.

1. Ouvrez **File Sanitizer**, cliquez sur **Settings** (Paramètres), cliquez sur **Simple Delete Setting** (Paramètre de suppression simple), puis sur **Détails**.
2. Sélectionnez les ressources à supprimer :
   - Sous **Available delete options** (Options de suppression disponibles), cliquez sur une ressource, puis sur **Add** (Ajouter).
   - Pour ajouter une ressource personnalisée, cliquez sur **Add Custom Option** (Ajouter une option personnalisée), saisissez un nom de fichier ou de dossier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Add** (Ajouter).

   REMARQUE : Pour supprimer une ressource des options de suppression disponibles, cliquez sur la ressource, puis sur **Supprimer**.
3. Sous **Delete the following** (Supprimer les éléments suivants), cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la suppression.

REMARQUE : Pour retirer une ressource de la liste de suppression, cliquez sur la ressource, puis sur **Supprimer**.

4. Sous **Do not shred the following** (Ne pas supprimer les éléments suivants), cliquez sur **Add** (Ajouter) pour sélectionner les ressources spécifiques à exclure de la destruction.

REMARQUE : Seules les extensions de fichiers peuvent être exclues de la suppression. Par exemple, si vous ajoutez l'extension de fichier .BMP, tous les fichiers portant l'extension .BMP seront exclus de la suppression.

Pour retirer une ressource de la liste des exclusions, cliquez sur la ressource, puis sur **Supprimer**.

5. Lorsque vous avez terminé la configuration du profil de suppression simple, cliquez sur **Appliquer**, puis sur **OK**.

Tâches générales

Utilisation d'une séquence de touches pour démarrer la destruction

Pour spécifier une séquence de touches, procédez comme suit :

1. Ouvrez **File Sanitizer**, puis cliquez sur **Shred** (Détruire).
2. Cochez la case **Key sequence** (Séquence de touches).
3. Saisissez un caractère dans la case disponible, puis cochez la case **CTRL**, **ALT** ou **MAJ** ou bien les trois.

   Par exemple, pour démarrer une destruction automatique à l'aide de la touche s et des touches ctrl+maj, saisissez s dans la case, puis cochez les options **CTRL** et **MAJ**.

REMARQUE : Pensez à vérifier que vous avez sélectionné une séquence de touches différente des autres séquences configurées.

Pour démarrer une destruction à l'aide d'une séquence de touches :

1. Maintenez la touche ctrl, alt ou maj enfoncée (ou la combinaison que vous avez spécifiée) tout en appuyant sur le caractère choisi.
2. Si une boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Utilisation de l'icône File Sanitizer

ATTENTION : Les ressources détruites ne peuvent pas être récupérées. Soyez très attentif dans la sélection des éléments lors d'une destruction manuelle.

1. Naviguez vers le document ou le dossier à détruire.
2. Faites glisser la ressource sur l'icône File Sanitizer du bureau.
3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Destruction manuelle d'une ressource

ATTENTION : Les ressources détruites ne peuvent pas être récupérées. Soyez très attentif dans la sélection des éléments lors d'une destruction manuelle.

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools** située dans la zone de notification, à l'extrémité droite de la barre des tâches, cliquez sur **File Sanitizer**, puis sur **Shred One** (Destruction unique).
2. Lorsque la boîte de dialogue Parcourir s'affiche, naviguez vers la ressource à détruire, puis cliquez sur **OK**.

   REMARQUE : La ressource sélectionnée peut être un fichier ou un dossier unique.

3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

– ou –

1. Cliquez avec le bouton droit sur l'icône **File Sanitizer** du bureau, puis cliquez sur **Shred One** (Destruction unique).
2. Lorsque la boîte de dialogue Parcourir s'affiche, naviguez vers la ressource à détruire, puis cliquez sur **OK**.
3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

– ou –

1. Ouvrez File Sanitizer, puis cliquez sur **Shred** (Détruire).
2. Cliquez sur le bouton **Parcourir**.
3. Lorsque la boîte de dialogue Parcourir s'affiche, naviguez vers la ressource à détruire, puis cliquez sur **OK**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

– ou –

1. Ouvrez File Sanitizer, puis cliquez sur **Shred** (Détruire).
2. Cliquez sur le bouton **Shred Now** (Détruire maintenant).
3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Destruction manuelle de tous les éléments sélectionnés

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools** située dans la zone de notification, à l'extrémité droite de la barre des tâches, cliquez sur **File Sanitizer**, puis sur **Shred Now** (Détruire maintenant).
2. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

– ou –

1. Cliquez avec le bouton droit sur l'icône **File Sanitizer** du bureau, puis cliquez sur **Shred Now** (Détruire maintenant).
2. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Activation manuelle du nettoyage de l'espace libre

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools** située dans la zone de notification, à l'extrémité droite de la barre des tâches, cliquez sur **File Sanitizer**, puis sur **Bleach Now** (Nettoyer maintenant).
2. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

– ou –

1. Ouvrez File Sanitizer, puis cliquez sur **Free Space Bleaching** (Nettoyage de l'espace libre).
2. Cliquez sur **Bleach Now** (Nettoyer maintenant).
3. Lorsque la boîte de dialogue de confirmation s'affiche, cliquez sur **Oui**.

Annulation d'une opération de destruction ou de nettoyage de l'espace libre

Lorsqu'une opération de destruction ou de nettoyage de l'espace libre est en cours, un message apparaît au-dessus de l'icône HP ProtectTools Security Manager dans la zone de notification. Le message contient des détails sur le processus de destruction ou de nettoyage de l'espace libre (pourcentage terminé) et vous offre la possibilité d'annuler l'opération.

Pour annuler l'opération :

▲ Cliquez sur le message, puis sur **Arrêter** pour annuler l'opération.

Affichage des fichiers journaux

Chaque fois qu'une opération de destruction ou de nettoyage de l'espace libre est effectuée, des fichiers journaux contenant les erreurs ou les échecs sont générés. Les fichiers journaux sont toujours mis à jour par rapport à la dernière opération de destruction ou de nettoyage de l'espace libre.

REMARQUE : Les fichiers correctement détruits ou nettoyés n'apparaissent pas dans les fichiers journaux.

Un fichier journal est créé pour les opérations de destruction et un autre fichier journal est créé pour les opérations de nettoyage de l'espace libre. Ces deux types de fichiers journaux se trouvent sur le disque dur aux emplacements suivants :

- C:\Program Files\Hewlett-Packard\File Sanitizer\[NomUtilisateur]_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\[NomUtilisateur]_DiskBleachLog.txt

6 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 administrateur.
- Configuration des autres fonctionnalités d'authentification à la mise sous tension, telles que l'authentification de la sécurité intégrée.
- Activation et désactivation de fonctions matérielles, telles que l'amorçage par CD-ROM ou les 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 de l'ordinateur qui, sinon, seraient uniquement accessibles via une pression sur la touche f10 au démarrage afin d'ouvrir l'utilitaire Computer Setup.

Accès au module BIOS Configuration

Pour accéder au module BIOS Configuration :

1. Cliquez sur **Démarrer**, sur **Paramètres**, puis sur **Panneau de configuration**.
2. Cliquez sur **HP ProtectTools Security Manager**, puis sur **BIOS Configuration**.

   Vous pouvez également accéder au module BIOS Configuration à partir d'une icône dans la zone de notification, à l'extrémité droite de la barre des tâches :

   REMARQUE : Pour afficher l'icône HP ProtectTools Security Manager, il peut être nécessaire de cliquer sur l'icône **Afficher les icônes cachées** (**<** ou **<<**) de la zone de notification.

   - Cliquez avec le bouton droit sur l'icône **HP ProtectTools Security Manager** dans la zone de notification.
   - Cliquez sur **BIOS Configuration**.
3. Si vous êtes utilisateur de HP ProtectTools, entrez votre mot de passe Windows.
   - Si le mot de passe Windows est saisi correctement, mais que vous n'êtes pas administrateur BIOS, votre capacité à apporter des modifications varie en fonction des paramètres du niveau de sécurité. Voir Configuration d'options de configuration système à la page 68.

     REMARQUE : Un utilisateur de HP ProtectTools n'est pas nécessairement un administrateur BIOS.
   - Si le mot de passe Windows n'est pas saisi correctement, vous pouvez simplement afficher les paramètres de la configuration BIOS, mais vous ne pouvez pas les modifier.
4. Si vous n'êtes pas utilisateur de HP ProtectTools, le logiciel BIOS Configuration vérifie si un mot de passe d'administrateur BIOS a été configuré.
   - Si aucun mot de passe de l'administrateur de BIOS n'a été défini, vous devez le saisir maintenant.
     - Si le mot de passe d'administrateur BIOS est saisi correctement, vous pouvez à la fois afficher et modifier les paramètres de la configuration BIOS.
     - Si un mot de passe d'administrateur BIOS a été défini, mais que vous ne parvenez pas à le saisir ou que vous ne le saisissez pas correctement, vous pouvez afficher les paramètres de la configuration BIOS, mais vous ne pouvez pas les modifier.
   - Si aucun mot de passe d'administrateur BIOS n'a été défini, vous pouvez afficher et modifier les paramètres de la configuration BIOS.

Affichage ou modification des paramètres

Pour afficher ou modifier les paramètres de configuration :

1. Cliquez sur l'une des pages BIOS Configuration :
   - File (Fichier)
   - Security (Sécurité)
   - System Configuration (Configuration système)
2. Apportez les modifications souhaitées, puis cliquez sur **Appliquer** pour enregistrer vos modifications et laisser la fenêtre ouverte.

   – ou –

   Apportez les modifications souhaitées, puis cliquez sur **OK** pour enregistrer vos modifications et fermer la fenêtre.
3. Quittez et redémarrez l'ordinateur.

   Vos modifications prennent effet au redémarrage de l'ordinateur.

REMARQUE : Les modifications du mot de passe prennent effet immédiatement sans nécessiter le redémarrage de l'ordinateur.

Affichage des informations système

Utilisez la page "Fichier" pour visualiser les types d'informations suivants :

- Informations d'identification relatives à l'ordinateur (notamment le numéro de série) et aux batteries dans le système
- Caractéristiques relatives au processeur, à la taille du cache et de la mémoire, à la version de la carte graphique et du contrôleur de clavier, ainsi qu'à la mémoire ROM du système

REMARQUE : La page "File" est uniquement disponible à titre d'information. Aucune des informations affichées n'est modifiable.

Pour afficher les informations système :

▲ Accédez au module BIOS Configuration, puis cliquez sur **Fichier**.

Tâches avancées

Configuration des options de sécurité

Utilisez la page "Security" de l'utilitaire de configuration du BIOS pour étendre la sécurité de votre ordinateur.

REMARQUE : Toutes les options ne sont pas disponibles sur tous les ordinateurs, et des options supplémentaires peuvent également être incluses.

Pour configurer les options de sécurité :

1. Accédez au module BIOS Configuration, puis cliquez sur **Sécurité**.
2. Sélectionnez l'une des options répertoriées dans le tableau ci-après.
3. Modifiez les paramètres suivant les besoins.
4. Cliquez sur **Appliquer** pour valider les nouveaux paramètres et laisser la fenêtre ouverte.

   – ou –

   Cliquez sur **OK** pour appliquer les nouveaux paramètres et fermer la fenêtre.

Sécurité

Option	Action
Mot de passe administrateur BIOS **REMARQUE :** Cette option peut être appelée “Setup Password”.	Cliquer sur le bouton **Définir** pour configurer un mot de passe d'administrateur BIOS.

ID du système

Option	Action
Code propriétaire du portable	Saisir, afficher ou modifier.
Numéro de suivi du portable	Saisir, afficher ou modifier.

Sécurité intégrée TPM

REMARQUE : Cette fonction est uniquement prise en charge sur les ordinateurs équipés de la puce de sécurité intégrée (TPM) HP ProtectTools.

Option	Action
Réinitialiser TPM à partir du système d'exploitation	Activer ou désactiver.
Gestion du système d'exploitation de TPM	Activer ou désactiver.
Disponibilité du périphérique de sécurité intégré	Sélectionner les éléments disponibles ou masqués.
Prise en charge de l'authentification au démarrage	Activer ou désactiver la prise en charge de l'authentification de Smart Card au démarrage.

Option	Action
	REMARQUE : Cette fonction est uniquement prise en charge sur les ordinateurs dotés d'un lecteur de Smart Card en option.
Prise en charge Drivelock automatique	Activer ou désactiver.

Outils de l'administrateur

Option	Action
HP SpareKey	Activer ou désactiver.
Réinitialisation du lecteur d'empreintes digitales au réamorçage (si connecté)	Activer ou désactiver.

Règles de mot de passe

Option	Action
Au moins un symbole est requis	Activer ou désactiver.
Au moins un nombre est requis	Activer ou désactiver.
Au moins une majuscule est requise	Activer ou désactiver.
Au moins une minuscule est requise	Activer ou désactiver.
Les espaces sont-ils autorisés dans les mots de passe	Activer ou désactiver.

Rapport de nettoyage de disque dur

Option	Action
Nettoyage de disque dur	Si le nettoyage du disque dur a été exécuté au moins une fois, vous pouvez afficher des informations sur les procédures de nettoyage de disque dur les plus récentes réalisées sur l'ordinateur. **REMARQUE :** Cette option efface les données sensibles d'un disque dur d'ordinateur. Si un disque a été nettoyé, puis retiré de l'ordinateur, les informations concernant le processus de nettoyage sont toujours disponibles.

Configuration d'options de configuration système

Utilisez la page "Configuration du système" pour afficher et modifier les paramètres de la configuration système.

REMARQUE : Toutes les options ne sont pas disponibles sur tous les ordinateurs, et des options supplémentaires peuvent également être incluses.

Pour configurer des options de configuration système :

1. Accédez au module **BIOS Configuration**, puis cliquez sur **Configuration système**.
2. Sélectionnez l'une des options suivantes, comme décrit dans le tableau ci-après :
   - **Options de port**
   - **Options de démarrage**
   - **Options de configuration de périphérique**
   - **Options de périphérique intégré :**
   - **Options AMT (sur certains modèles uniquement)**
   - **Options de niveau de sécurité**
3. Modifiez les paramètres suivant les besoins.
4. Cliquez sur **Appliquer** pour valider les nouveaux paramètres sur le système et laisser la fenêtre ouverte.

   – ou –

   Cliquez sur **OK** dans la fenêtre HP ProtectTools Security Manager pour appliquer les nouveaux paramètres au système et fermer la fenêtre.

Options de port

Option	Action
Lecteur flash	Activer ou désactiver.
Ports USB	Activer ou désactiver.
Port 1394	Activer ou désactiver.
Emplacement pour Express Card	Activer ou désactiver.

Options de démarrage

Option	Action
Retard de vérification du démarrage (sec)	Définir le retard de vérification du démarrage (en secondes).
Logo personnalisé	Activer ou désactiver.
Retard d'amorçage express (sec)	Définir le retard d'amorçage express (en secondes).
Démarrage CD-ROM	Activer ou désactiver.
Démarrage carte SD	Activer ou désactiver.
Démarrage à partir du fichier EFI	Activer ou désactiver.
Démarrage disquette	Activer ou désactiver.
Démarrage par carte réseau interne PXE	Activer ou désactiver.
Ordre de démarrage	Définir l'ordre dans lequel les périphériques système seront démarrés.

Options de configuration de périphérique

Option	Action
Support USB Legacy	Activer ou désactiver.
Mode de port parallèle	Sélectionner un mode de port parallèle : standard, bidirectionnel, EPP (Enhanced Parallel Port) ou ECP (Enhanced Capabilities Port).
Ventilateur toujours activé si alimentation secteur	Activer ou désactiver le ventilateur système en cas de raccordement au secteur.
Prévention d'exécution des données	Activer/désactiver l'option permettant de surveiller l'utilisation de la mémoire et de mettre fin aux programmes suspects.
Mode du périphérique SATA	Sélectionner IDE, AHCI ou RAID.
Processeur double cœur	Activer ou désactiver.
Chargement rapide batterie secondaire	Activer ou désactiver.
HP QuickLook 2	Activer ou désactiver.
Technologie TXT	Activer ou désactiver.
Afficher URL de diagnostic	Activer ou désactiver.
Mode de conversion disque dur	Sélectionner Bit-shift ou Assistance LBA.
Technologie de virtualisation	Activer ou désactiver cette option pour permettre à plusieurs machines virtuelles d'être exécutées côte à côte sur le même ordinateur.

Options de périphérique intégré :

Option	Action
Etat bouton des périphériques sans fil	Activer ou désactiver.
Radio de périphérique WAN sans fil intégré	Activer ou désactiver.
Lecteur d'empreintes digitales	Activer ou désactiver.
Compartiment MultiBay du portable	Activer ou désactiver.
Contrôleur d'interface réseau (LAN)	Activer ou désactiver.
Capteur de lumière ambiante	Activer ou désactiver.
Radio de périphérique Bluetooth® intégré	Activer ou désactiver.
Remise sous tension Wake on LAN	Activer ou désactiver cette option pour mettre l'ordinateur sous tension à distance à partir d'un autre ordinateur connecté au même réseau.

Options AMT (sur certains modèles uniquement)

Option	Action
Mode d'émulation de terminal	Sélectionner ANSI ou VT100.
Prolixité du microprogramme	Activer ou désactiver.

Option	Action
Prise en charge des événements de progression du microprogramme	Activer ou désactiver.
Déconfigurer AMT au prochain démarrage	Activer ou désactiver.

Options de niveau de sécurité

REMARQUE : Ces paramètres contrôlent le niveau d'accès associé aux utilisateurs de HP ProtectTools.

Option	Action
Niveau de sécurité du démarrage à partir du CD-ROM	Modifier, afficher ou masquer.
Niveau de sécurité du démarrage à partir de la disquette	Modifier, afficher ou masquer.
Niveau de sécurité de l'amorçage à partir de la carte réseau interne	Modifier, afficher ou masquer.
Niveau de sécurité du support USB Legacy	Modifier, afficher ou masquer.
Allumage constant du ventilateur si alimentation secteur	Modifier, afficher ou masquer.
Niveau de sécurité du lecteur flash	Modifier, afficher ou masquer.
Niveau de sécurité du retard de vérification du démarrage (sec)	Modifier, afficher ou masquer.
Niveau de sécurité du mode de port parallèle	Modifier, afficher ou masquer.
Niveau de sécurité du retard d'amorçage express (sec)	Modifier, afficher ou masquer.
Niveau de sécurité de la commutation LAN/WLAN	Modifier, afficher ou masquer.
Niveau de sécurité de la radio de périphérique Bluetooth intégré	Modifier, afficher ou masquer.
Niveau de sécurité de la radio de périphérique WAN sans fil intégré	Modifier, afficher ou masquer.
Niveau de sécurité de la prise en charge de l'authentification au démarrage	Modifier, afficher ou masquer.
Niveau de sécurité de la prise en charge Drivelock automatique	Modifier, afficher ou masquer.
Niveau de sécurité de la prévention d'exécution des données	Modifier, afficher ou masquer.
Niveau de sécurité du mode du périphérique SATA	Modifier, afficher ou masquer.
Niveau de sécurité des ports USB	Modifier, afficher ou masquer.
Niveau de sécurité du port 1394	Modifier, afficher ou masquer.
Niveau de sécurité du connecteur Express Card	Modifier, afficher ou masquer.
Niveau de sécurité du processeur double cœur	Modifier, afficher ou masquer.

Niveau de sécurité de la remise sous tension Wake on LAN	Modifier, afficher ou masquer.
Niveau de sécurité du capteur de lumière ambiante	Modifier, afficher ou masquer.
Niveau de sécurité de la charge rapide de la batterie secondaire	Modifier, afficher ou masquer.
Niveau de sécurité de la disponibilité du périphérique de sécurité intégré	Modifier, afficher ou masquer.
Niveau de sécurité du mode de conversion de disque dur	Modifier, afficher ou masquer.
Niveau de sécurité du lecteur d'empreintes digitales	Modifier, afficher ou masquer.
Niveau de sécurité de l'unité de disque optique	Modifier, afficher ou masquer.
Niveau de sécurité du contrôleur d'interface réseau (LAN)	Modifier, afficher ou masquer.
Niveau de sécurité de la gestion du système d'exploitation de TPM	Modifier, afficher ou masquer.
Niveau de sécurité de la réinitialisation de TPM à partir du système d'exploitation	Modifier, afficher ou masquer.
Niveau de sécurité de la technologie de virtualisation	Modifier, afficher ou masquer.
Niveau de sécurité du mode d'émulation de terminal	Modifier, afficher ou masquer.
Niveau de sécurité de la prolixité du microprogramme	Modifier, afficher ou masquer.
Niveau de sécurité de la prise en charge des événements de progression du microprogramme	Modifier, afficher ou masquer.
Niveau de sécurité de la déconfiguration de l'AMT	Modifier, afficher ou masquer.
Niveau de sécurité du numéro de suivi du portable	Modifier, afficher ou masquer.
Niveau de sécurité du code propriétaire du portable	Modifier, afficher ou masquer.
Niveau de sécurité de l'ordre de démarrage	Modifier, afficher ou masquer.
Règles de logo personnalisé	Modifier, afficher ou masquer.
Niveau de sécurité de la déconfiguration de l'AMT au prochain démarrage	Modifier, afficher ou masquer.
Niveau de sécurité du démarrage à partir de la carte SD	Modifier, afficher ou masquer.
Niveau de sécurité du démarrage à partir du fichier EFI	Modifier, afficher ou masquer.
Niveau de sécurité de HP QuickLook 2	Modifier, afficher ou masquer.
Niveau de sécurité de l'état du bouton des périphériques sans fil	Modifier, afficher ou masquer.
Niveau de sécurité du modem	Modifier, afficher ou masquer.
Niveau de sécurité de la réinitialisation du lecteur d'empreintes digitales	Modifier, afficher ou masquer.
Niveau de sécurité de HP SpareKey	Modifier, afficher ou masquer.
Niveau de sécurité de la technologie TXT	Modifier, afficher ou masquer.
Niveau de sécurité de l'URL de diagnostic	Modifier, afficher ou masquer.

7 Embedded Security for HP ProtectTools (sur certains modèles uniquement)

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 défini aucun mot de passe d'administration, utilisez les touches fléchées pour sélectionner les options **Sécurité**, **Setup password** (Définir le mot de passe), 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 sauvegarder vos préférences et quitter l'utilitaire Computer Setup, utilisez les touches fléchées pour sélectionner **File** (Fichier) et cliquez sur **Save Changes and Exit** (Enregistrer les modifications et quitter). Puis, suivez 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 d'initialisation de Embedded Security User Initialization n'est pas ouvert, cliquez sur **Démarrer**, puis **Tous les programmes** et cliquez sur **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 la messagerie électronique sécurisée, vous devez d'abord configurer le client de messagerie en vue d'utiliser un certificat numérique créé via le module Embedded Security. Si aucun certificat numérique n'est disponible, vous devez en obtenir un à partir d'une autorité de certification. Pour obtenir des instructions de configuration de votre messagerie électronique, ainsi qu'un certificat numérique, reportez-vous à l'aide relative au logiciel 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

Le module Embedded Security vous permet d'envoyer et recevoir des courriers électroniques cryptés, mais les procédures requises varient selon le programme que vous utilisez pour accéder à votre courrier électronique. Pour plus d'informations, reportez-vous à l'aide sur le logiciel Embedded Security, ainsi qu'à celle relative à votre programme de messagerie.

Modification du mot de passe de la clé utilisateur de base

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

1. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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 sur le logiciel.

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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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 de détails sur la migration, consultez l'aide sur le logiciel Embedded Security.

8 Device Access Manager for HP ProtectTools (sur certains modèles uniquement)

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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Advanced** (Avancés), puis sur **Find Now** (Rechercher maintenant) pour rechercher des utilisateurs ou des 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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **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. Cliquez sur **Advanced** (Avancés), puis sur **Find Now** (Rechercher maintenant) pour rechercher des utilisateurs ou des 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**.

9 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 cartes Smart Card et jetons USB ne sont pas disponibles dans le module Credential Manager s'ils sont installés après le module Credential Manager.	Pour pouvoir utiliser des cartes Smart Card ou des jetons USB dans Credential Manager, vous devez installer les composants logiciels de prise en charge (pilotes, fournisseurs PKCS#11, etc.) avant l'installation de Credential Manager. Si le module Credential Manager est installé, procédez comme suit après l'installation du logiciel de prise en charge de la Smart Card ou du jeton :	Connectez-vous à Credential Manager. Dans HP ProtectTools Security Manager, cliquez sur **Credential Manager**, **Advanced Settings** (Paramètres avancés), puis sur l'onglet **Smart Cards and Tokens** (Smart Cards et jetons). Une liste des jetons disponibles s'affiche sous "Local Tokens". Accédez à un menu en incrustation en cliquant sur le noeud Local Tokens et sélectionnez l'option "Scan for New Smart Cards and Tokens" (Rechercher de nouvelles Smart Cards ou de nouveaux jetons). Si vous y êtes invité, redémarrez votre ordinateur.
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 spécifique en désactivant l'option correspondante. Consultez la documentation complète sur l'authentification unique disponible dans les fichiers d'aide sur le logiciel 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).	Le module Credential Manager ne permet pas de modifier le mot de passe d'un compte d''utilisateur via la fonction **Change Windows password** (Changer le mot de passe Windows). Credential Manager permet uniquement de modifier les mots de passe du compte de l'ordinateur local. L'utilisateur du domaine peut modifier son mot de passe à l'aide de l'option **Modifier le mot de passe** de la boîte de dialogue **Sécurité de Windows**, mais comme celui-ci ne possède pas de compte physique sur le PC local, Credential Manager peut uniquement modifier le mot de passe utilisé pour 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 en appliquant le correctif Service Pack 2 via Windows Update. Pour plus d'informations sur l'origine du problème, consultez la base de connaissances de Microsoft (article 813301) à l'adresse 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 fléchées pour sélectionner **Security** (Sécurité), puis cliquez sur **Setup Password** (Configurer le mot de passe). 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. Cliquez sur **Enable** (Activer), puis sur **Save changes and exit** (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 (sur certains modèles uniquement)

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 entre Embedded Security EFS et le logiciel Symantec Antivirus ou McAfee Total Protection allonge les temps de cryptage/décryptage et de numérisation.	Les fichiers cryptés interfèrent avec l'analyse virale de Symantec Antivirus ou McAfee Total Protection. Le cryptage de fichiers à l'aide de Embedded Security EFS prend plus longtemps lorsque le logiciel Symantec Antivirus ou McAfee Total Protection est activé.	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 le temps nécessaire au cryptage et au décryptage des données avec Embedded Security EFS, il convient que l'utilisateur désactive l'option Auto-Protect de Symantec Antivirus ou de McAfee Total Protection.
L'archive de restauration d'urgence ne peut pas être	Si l'utilisateur insère une carte mémoire MultiMediaCard ou Secure Digital (SD)	Le système est ainsi conçu.

Brève description	Détails	Solution
sauvegardée sur un support amovible.	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 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 **Security** (Sécurité), puis **Embedded Security** (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** et cliquez sur **Save Changes and Exit** (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 les utilisateurs qui ont des droits d'administrateur sur le système.	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
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.
Un blocage intermittent du système se produit après la création d'un lecteur sécurisé personnel sur	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	La cause semble due à un problème de synchronisation dans les configurations à faible quantité de mémoire.

Brève description	Détails	Solution
des comptes à deux utilisateurs et l'utilisation de la fonction de changement rapide d'utilisateur dans des configurations système 128 Mo.	rapide d'utilisateur est sollicitée sur un système doté d'une RAM minimum.	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 **Security > Device security** (Sécurité et sécurité des périphériques), puis modifiez la valeur du champ **Hidden** (Caché) sur **Available** (disponible).
La sauvegarde automatique ne fonctionne pas avec une unité mappée.	Lorsqu'un administrateur configure la sauvegarde automatique dans Embedded Security, il crée une entrée dans **Windows** > **Tâches** > **Tâche planifiée**. Cette tâche planifiée Windows est définie en vue d'utiliser les droits NT AUTHORITY\SYSTEM lors de l'exécution de la sauvegarde. Cette configuration fonctionne correctement avec 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,	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
	l'icône TNA de Embedded Security 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 **HP ProtectTools Device Locking/Auditing**. Assurez-vous que ce service est démarré et que le type de démarrage **Automatique** est sélectionné.
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. Cliquez sur **Security Manager**, puis sur **Device Access Manager** et **Device Class Configuration**. Développez les niveaux de l'arborescence des classes de périphériques et consultez les paramètres applicables à l'utilisateur. Recherchez les droits d'accès “Deny” éventuellement définis pour l'utilisateur dans l'un des groupes Windows dont il peut être membre (ex : Utilisateurs, Administrateurs).
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 de FW n'est pas 2.18, téléchargez et mettez à jour le micrologiciel TPM. Le téléchargement de TPM Firmware SoftPaq est accessible sur le site 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

activation : Tâche à exécuter avant de pouvoir accéder à l'une des fonctions de Drive Encryption. Drive Encryption est activé à l'aide de l'assistant d'installation de HP ProtectTools Security Manager. Seul un administrateur peut activer Drive Encryption. Le processus d'activation consiste à activer le logiciel, à crypter le disque, à créer un compte utilisateur et à générer la clé de cryptage de sauvegarde initiale sur un périphérique amovible.

administrateur : Voir : administrateur Windows.

administrateur Windows : Utilisateur disposant des droits permettant de modifier les autorisations et de gérer d'autres utilisateurs.

archive de récupération 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.

ATM (Automatic Technology Manager) : Permet aux administrateurs réseau de gérer des systèmes à distance au niveau du BIOS.

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 à la 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 : Fonctionnalité permettant d'enregistrer les informations d'authentification et d'utiliser le module Credential Manager pour accéder à Internet et aux applications Windows nécessitant 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.

bouton Send Securely (Envoyer en toute sécurité) : Bouton de logiciel présent dans la barre d'outils des messages électroniques Microsoft Outlook. Lorsque vous cliquez sur ce bouton, vous pouvez signer et/ou crypter un message électronique Microsoft Outlook.

bouton Sign and Encrypt (Signer et crypter) : Bouton de logiciel présent dans la barre d'outils des applications Microsoft Office. Lorsque vous cliquez sur ce bouton, vous pouvez signer, crypter ou supprimer le cryptage d'un document Microsoft Office.

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.

certificat Privacy Manager : Certificat numérique qui exige une authentification chaque fois que vous l'utilisez pour effectuer des opérations cryptographiques, telles que la signature ou le cryptage de messages électroniques et de documents Microsoft Office.

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.

contact authentifié : Personne ayant accepté une invitation de contact authentifié.

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.

cycle de destruction : Nombre d'exécution de l'algorithme de destruction sur chaque ressource. Plus le nombre de cycles de destruction est élevé, plus votre ordinateur est sécurisé.

déchiffrement : Procédure utilisée en cryptographie pour convertir des données cryptées en un texte normal.

destinataire Contact authentifié : Personne recevant une invitation à devenir un contact authentifié.

destruction : Exécution d'un algorithme de brouillage des données contenues dans une ressource.

destruction automatique : Destruction planifiée que l'utilisateur configure dans File Sanitizer for HP ProtectTools.

destruction manuelle : Destruction immédiate d'une ressource ou de ressources sélectionnées qui passe outre la planification de destruction automatique.

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.

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

DriveLock Fonction de sécurité qui lie l'unité de disque dur à un utilisateur et nécessite que celui-ci entre 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.

Écran de connexion de Drive Encryption : Écran de connexion affiché avant le démarrage de Windows. Les utilisateurs doivent saisir leurs nom d'utilisateur et mot de passe Windows ou le code confidentiel de leur Java Card. Dans la plupart des cas, la saisie des informations correctes sur l'écran de connexion de Drive Encryption permet d'accéder directement à Windows sans avoir à se reconnecter via l'écran de connexion Windows.

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

expéditeur authentifié : Contact authentifié envoyant des courriers électroniques et des documents Microsoft Office signés et/ou cryptés.

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

historique de messagerie instantanée : Fichier crypté contenant un enregistrement des conversations entre deux participants lors d'une session de messagerie instantanée.

HP SpareKey : Copie de sauvegarde de la clé Drive Encryption :

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.

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

invitation de contact authentifié : Courrier électronique envoyé à une personne pour lui demander de devenir un contact authentifié.

Java Card : Type de carte amovible insérée dans l'ordinateur : Cette carte contient les informations d'identification nécessaires à la connexion. La connexion avec une Java Card à partir de l'écran de connexion de Drive Encryption nécessite l'insertion de la Java Card, suivie de la saisie de votre nom d'utilisateur et du code confidentiel de la Java Card.

jeton : Voir : méthode de connexion sécurisée.

Jeton USB : Périphérique de sécurité qui stocke des informations d'identification concernant un utilisateur. Comme une Java Card ou un lecteur de données biométriques, il sert à authentifier le propriétaire sur un ordinateur.

jeton virtuel : Fonction de sécurité de principe similaire à l'utilisation d'une Java Card et d'un lecteur de cartes. Le jeton est sauvegardé sur le disque dur de l'ordinateur ou dans le registre Windows. Lorsque vous vous connectez à un jeton virtuel, vous êtes invité à entrer un code confidentiel pour procéder à l'authentification.

lecteur sécurisé personnel (PSD) : Fournit une zone de stockage protégée pour des informations confidentielles.

ligne de signature : Espace réservé pour l'affichage visuel d'une signature numérique. Lorsqu'un document est signé, le nom du signataire et la méthode de vérification sont affichés. La date de signature et le titre du signataire peuvent également être inclus.

liste des contacts authentifiés : Liste complète des contacts authentifiés.

message authentifié : Session de communication au cours de laquelle des messages authentifiés sont envoyés par un expéditeur authentifié vers un contact authentifié.

méthode de connexion sécurisée : Méthode utilisée pour se connecter à l'ordinateur.

migration : Tâche permettant de gérer, de restaurer et de transférer des certificats Privacy Manager et des contacts authentifiés.

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.

mode du périphérique SATA : Mode de transfert de données entre un ordinateur et des périphériques de stockage de masse comme les disques durs et les unités optiques.

Mot de passe administrateur BIOS : Mot de passe de *configuration* de Computer Setup.

mot de passe de révocation : Mot de passe créé lorsqu'un utilisateur demande un certificat numérique. Le mot de passe est requis lorsque l'utilisateur souhaite révoquer son certificat numérique. Ainsi, l'utilisateur est le seul à pouvoir révoquer le certificat.

nettoyage de l'espace libre : Ecriture sécurisée de données aléatoires par-dessus les ressources supprimées permettant de déformer le contenu de la ressource supprimée.

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

profil de destruction : Spécification d'une méthode d'effacement et d'une liste de ressources.

Puce de sécurité intégrée TPM (Trusted Platform Module) (certains modèles) Terme générique faisant référence à la puce de sécurité intégrée de HP ProtectTools. Une puce de sécurité intégrée permet d'authentifier un ordinateur, et non un utilisateur, en stockant des informations spécifiques au système hôte, comme les clés de cryptage, les certificats numériques et les mots de passe. Une puce de sécurité intégrée réduit les risques que les données de l'ordinateur soient compromises par un vol physique ou par une attaque externe menée par un pirate.

réamorçage : Processus de redémarrage de l'ordinateur.

ressource : Composant de données (informations personnelles ou fichiers, historiques et données Web, etc.) se trouvant sur le disque dur.

révélation : Tâche permettant à l'utilisateur de décrypter une ou plusieurs sessions d'historique de messagerie instantanée, ce qui affiche les noms d'écran des contacts en texte normal et rend la session disponible pour visualisation.

scellage pour les contacts authentifiés : Tâche permettant d'ajouter une signature numérique, de crypter le courrier électronique et de l'envoyer après votre authentification, selon la méthode de connexion sécurisée choisie.

sécurité stricte : Fonction de sécurité de BIOS Configuration qui fournit une protection renforcée des mots de passe à la mise sous tension et d'administration, ainsi que d'autres formes d'authentification à la mise sous tension.

séquence de touches : Combinaison de touches spécifique dont l'utilisation permet de démarrer une destruction automatique ; par exemple ctrl+alt+s.

Service de restauration de clé Drive Encryption : Service de restauration SafeBoot : Il permet de stocker une copie de la clé de cryptage, ce qui vous permet d'accéder à votre ordinateur en cas de perte de votre mot de passe si vous n'avez pas accès à votre clé de sauvegarde locale. Vous devez créer un compte avec le service pour configurer un accès en ligne à votre clé de sauvegarde.

session de communication de messagerie instantanée authentifiée : Session de communication au cours de laquelle des messages authentifiés sont envoyés par un expéditeur authentifié vers un contact authentifié.

signataire suggéré : Utilisateur désigné par le propriétaire d'un document Microsoft Word ou Microsoft Excel pour ajouter une ligne de signature au document.

signature numérique : Données transmises avec un fichier, servant à vérifier l'expéditeur du matériel et à contrôler que le fichier n'a pas été modifié 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.

suppression simple : Suppression de la référence Windows à une ressource. Le contenu de la ressource reste présent sur le disque dur jusqu'à ce que des données de brouillage soient inscrites par-dessus ce contenu lors d'un nettoyage de l'espace libre.

TXT : Trusted Execution Technology (technologie d'exécution sécurisée).

utilisateur : Toute personne inscrite à Drive Encryption est un utilisateur. Les utilisateurs qui ne sont pas des administrateurs disposent de droits limités dans Drive Encryption. Ils ne peuvent que s'inscrire (avec l'accord de l'administrateur) et se connecter.

Visionneuse d'historique de messagerie instantanée : Composant de Privacy Manager Chat permettant de rechercher et d'afficher des sessions d'historique de messagerie instantanée cryptées.

Index