HP ProtectTools Security Manager, version 5.0

Manuel de l’utilisateur

Manuel de l’utilisateur HP ProtectTools Security Manager

Ordinateurs d’entreprise HP Compaq

Première édition : septembre 2009

Référence du document : 581746-051

À propos de ce livre

Ce manuel contient les informations de base nécessaires aux mises à niveau de ce modèle.

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

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

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

Sommaire

1 Introduction à la sécurité

Le logiciel HP ProtectTools fournit des fonctions de sécurité conçues pour empêcher tout accès non autorisé à l'ordinateur, aux réseaux et aux données critiques. La fonctionnalité de sécurité évoluée est fournie par plusieurs modules logiciels HP ProtectTools.

HP ProtectTools propose deux versions utilisables : la console d'administration de HP ProtectTools Security Manager et HP ProtectTools Security Manager (pour les utilisateurs). Les versions administrateur et utilisateur sont disponibles dans le menu **Démarrer** > **Tous les programmes**.

Fonction	Caractéristiques
Console d'administration de HP ProtectTools Security Manager	• Nécessite des privilèges administrateur sur le système Microsoft Windows pour y accéder • Permet d'accéder aux modules qui doivent être configurés par un administrateur et qui ne sont pas disponibles pour les utilisateurs • Permet une configuration de sécurité initiale et configure les options ou les éléments obligatoires pour tous les utilisateurs
HP ProtectTools Security Manager (pour les utilisateurs)	• Permet aux utilisateurs de configurer les options fournies par un administrateur • Peut restreindre l'accès et n'autoriser qu'un contrôle limité à certains modules HP ProtectTools pour l'utilisateur

REMARQUE : La configuration du Gestionnaire de mots de passe, de Java Card Security et de Drive Encryption se fait à l'aide de l'assistant de configuration de Security Manager. À l'heure actuelle, les systèmes de bureau HP Professional ne prennent pas en charge les périphériques à empreintes digitales.

Les modules logiciels HP ProtectTools peuvent être préinstallés, préchargés ou disponibles en option à configurer ainsi que séparément. Pour plus d'informations, consultez le site http://www.hp.com.

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

Fonctions HP ProtectTools

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

Module	Principales fonctions
Console d'administration de HP ProtectTools Security Manager	• L'assistant de configuration de Security Manager est utilisé par les administrateurs pour installer et configurer les niveaux de sécurité et les méthodes de connexion de sécurité. • Configuration des options masquées pour les utilisateurs de base. • Activation de Drive Encryption et configuration de l'accès utilisateur. • Configuration de Device Access Manager et des accès utilisateur. • Les outils des administrateurs sont utilisés pour ajouter et supprimer des utilisateurs HP ProtectTools, ainsi que pour afficher l'état des utilisateurs.
HP ProtectTools Security Manager (pour les utilisateurs)	• Organisation, configuration et modification des noms d'utilisateur et des mots de passe. • Configuration et modification des informations d'authentification des utilisateurs, telles que le mot de passe Windows et Smart Card. • Configuration et modification de la destruction, du nettoyage et des paramètres de File Sanitizer. • Affichage des paramètres pour l'état du cryptage et Device Access Manager. • Utilisation de Privacy Manager afin d'accroître la sécurité des courriers électroniques, des documents et de la messagerie instantanée. • Activation de LoJack Pro for HP ProtectTools. • Configuration des préférences et des options de sauvegarde et de restauration.
Password Manager for HP ProtectTools	• Agit comme un coffre à mots de passe personnel qui rationalise le processus de connexion grâce à la fonction Signature unique. Cette dernière enregistre et applique automatiquement les informations d'authentification de l'utilisateur. • Création et organisation de noms d'utilisateur et de mots de passe à signature unique.
Drive Encryption for HP ProtectTools	• Fournit un cryptage complet de tout le volume du disque dur. • Force l'authentification avant le démarrage afin de décrypter et d'accéder aux données du disque dur.
Privacy Manager for HP ProtectTools	• Utilisé pour obtenir des certificats d'autorité qui vérifient la source, l'intégrité et la sécurité des communications effectuées à l'aide de la messagerie électronique Microsoft, des documents Microsoft Office et d'Instant Messenger.
File Sanitizer for HP ProtectTools	• Permet de détruire en toute sécurité les ressources numériques (suppression sécurisée des informations sensibles telles que les fichiers d'application, le contenu historique ou Web ou d'autres données confidentielles) présentes sur votre ordinateur, ainsi que de nettoyer périodiquement le disque dur (écraser des données

Module	Principales fonctions
	précédemment supprimées mais toujours présentes sur le disque dur afin d'en rendre la récupération plus difficile).
Java Card Security for HP ProtectTools	• Fournit une interface logicielle de gestion pour les Java Cards. HP ProtectTools Java Card est un périphérique de sécurité personnel qui protège les données d'authentification et nécessite la carte et un code PIN pour autoriser l'accès. La Java Card peut être utilisée pour accéder au Gestionnaire de mots de passe, à Drive Encryption ou à tout point d'accès tiers. • Modification du code PIN.
Embedded Security for HP ProtectTools	• Utilise une puce de sécurité intégrée TPM qui empêche tout accès non autorisé aux données ou aux informations d'authentification sensibles de l'utilisateur stockées localement sur un PC. • Permet de créer un lecteur sécurisé personnel (PSD), utile pour protéger les fichiers utilisateur et les informations sur les dossiers. • Prend en charge les applications tierces (telles que Microsoft Outlook et Internet Explorer) pour les opérations de certificats numériques protégés.
Device Access Manager for HP ProtectTools	• Permet aux responsables informatiques ou aux administrateurs de contrôler l'accès aux périphériques tels que les ports USB, les unités optiques, les lecteurs de musique personnels, etc. en fonction des profils utilisateur. • Empêche les utilisateurs non autorisés de supprimer des données à l'aide d'un périphérique de stockage externe, ainsi que d'introduire des virus dans le système à partir d'un support externe. • L'administrateur peut interdire l'accès aux périphériques inscriptibles à des utilisateurs ou à des groupes d'utilisateurs sélectionnés.
LoJack Pro for HP ProtectTools	• Assure un suivi des ressources sécurisées. • Permet de surveiller l'activité utilisateur, ainsi que les modifications logicielles et matérielles. • Reste actif même si le disque dur est reformaté ou remplacé. • Pour être activé, nécessite un abonnement séparé au suivi et à la traçabilité.

Accès à HP ProtectTools Security

Pour accéder à HP ProtectTools Security Manager à partir du menu Démarrer de Windows :

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

Pour accéder à la console d'administration de HP ProtectTools Security Manager à partir du menu Démarrer de Windows :

▲ Sous Windows, cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.

REMARQUE : Une fois le module Gestionnaire de mots de passe configuré, vous pouvez également ouvrir HP ProtectTools en vous connectant directement au module Gestionnaire de mots de passe à partir de l'écran de connexion Windows.

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

Ce type d'incident pourrait par exemple être illustré par le vol ciblé d'un ordinateur ou des données confidentielles et des informations clients qu'il contient. Une telle situation peut facilement se produire dans les environnements de bureau ou dans les zones non sécurisées. Les fonctionnalités suivantes permettent de protéger les données en cas de vol de l'ordinateur :

- Si elle est activée, la fonction d'authentification avant le démarrage permet d'empêcher l'accès au système d'exploitation. Consultez les chapitres suivants :
  - Password Manager for HP ProtectTools à la page 23
  - Embedded Security for HP ProtectTools à la page 57
  - Drive Encryption for HP ProtectTools à la page 28
- 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.
- La fonction Lecteur sécurisé personnel, fournie par le module Embedded Security for HP ProtectTools, crypte les données sensibles afin de garantir qu'elles ne sont pas accessibles sans authentification. Consultez le chapitre suivant :
  - Embedded Security for HP ProtectTools à la page 57
- LoJack Pro peut aider à localiser un ordinateur volé. Consultez le chapitre suivant :
  - LoJack Pro for HP ProtectTools à la page 68

Restriction de l'accès à des données confidentielles

Prenons l'exemple d'un auditeur intervenant sur site et qui a accès à un ordinateur afin de vérifier des données financières confidentielles. Vous ne voulez pas que cet auditeur puisse imprimer les fichiers ou qu'il puisse les enregistrer sur un périphérique inscriptible comme un CD. La fonction suivante permet de restreindre l'accès aux données :

Device Access Manager for HP ProtectTools permet aux responsables informatiques de restreindre l'accès aux périphériques inscriptibles de façon à ce que les informations sensibles ne puissent pas

être imprimées ou copiées depuis le disque dur vers un support amovible. Reportez-vous à la section Configuration de classes de périphériques (tâches avancées) à la page 64.

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

Un accès non autorisé à un PC d'entreprise non sécurisé représente un risque réel pour les données confidentielles comme les informations provenant des services financiers, d'un administrateur, ou encore du service R&D, ainsi que pour les informations personnelles, par exemple les dossiers médicaux ou financiers. Les fonctions suivantes permettent d'empêcher tout accès non autorisé :

- Si elle est activée, la fonction d'authentification avant le démarrage permet d'empêcher l'accès au système d'exploitation. Consultez les chapitres suivants :
  - Password Manager for HP ProtectTools à la page 23
  - Embedded Security for HP ProtectTools à la page 57
  - Drive Encryption for HP ProtectTools à la page 28
- Embedded Security for HP ProtectTools aide à renforcer la protection des données utilisateur ou des informations d'authentification sensibles stockées sur un PC. Consultez le chapitre suivant :
  - Embedded Security for HP ProtectTools à la page 57
- Password Manager for HP ProtectTools vise à garantir qu'un utilisateur non autorisé ne peut pas obtenir de mot de passe ni accéder à des applications protégées par des mots de passe. Consultez le chapitre suivant :
  - Password Manager for HP ProtectTools à la page 23
- Device Access Manager for HP ProtectTools permet aux responsables informatiques de restreindre l'accès aux périphériques inscriptibles de façon à ce que les informations sensibles ne puissent pas être copiées depuis le disque dur. Consultez le chapitre suivant :
  - Device Access Manager for HP ProtectTools à la page 63
- La fonction Lecteur sécurisé personnel crypte les données sensibles afin de garantir qu'elles ne sont pas accessibles sans authentification. Consultez la section suivante :
  - Embedded Security for HP ProtectTools à la page 57
- File Sanitizer vous permet de supprimer des données en toute sécurité en détruisant des fichiers et des dossiers critiques ou en nettoyant le disque dur (écraser des données précédemment supprimées mais toujours présentes sur le disque dur afin d'en rendre la récupération plus difficile). Consultez le chapitre suivant :
  - File Sanitizer for HP ProtectTools à la page 49
- Privacy Manager vous permet d'obtenir des certificats d'autorité lors de l'utilisation de la messagerie Microsoft, des documents Office et d'Instant Messenger. Les processus d'envoi et d'enregistrement des informations importantes sont ainsi plus sûrs et plus sécurisés. Consultez le chapitre suivant :
  - Privacy Manager for HP ProtectTools à la page 32

Création de stratégies de mot de passe fort

Si une autorisation qui entre en vigueur nécessite qu'une stratégie de mot de passe fort soit utilisée pour des dizaines d'applications Web et de bases de données, Password Manager for HP ProtectTools fournit un référentiel protégé pour les mots de passe et la Signature unique. Consultez le chapitre suivant :

- Password Manager for HP ProtectTools à la page 23

Éléments de sécurité supplémentaires

Affectation de rôles de sécurité

En ce qui concerne la gestion de la sécurité des ordinateurs, l'une des principales règles consiste à répartir les responsabilités et les droits entre différents 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 mettre en place, telles que Drive Encryption ou Java™ Card.
- 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 au Gestionnaire de mots de passe	Gestionnaire de mots de passe	Ce mot de passe propose 2 options : • Il peut être utilisé pour une connexion séparée afin d'accéder au Gestionnaire de mots de passe après s'être connecté à Windows. • Il peut être utilisé pour remplacer le processus de connexion à Windows, afin d'accéder à Windows et au Gestionnaire de mots de passe simultanément.
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 HP ProtectTools	Défini dans ce module HP ProtectTools	Fonction
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	Peut être utilisé comme option d'authentification à plusieurs facteurs. 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 par l'administrateur informatique	Protège l'accès à l'utilitaire Computer Setup.
Mot de passe de mise sous tension	BIOS	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 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.
- Utilisez Embedded Security for HP ProtectTools afin de sauvegarder les informations d’authentification HP ProtectTools.
- Utilisez l’outil Sauvegarde et restauration de HP ProtectTools Security Manager comme emplacement central à partir duquel vous pourrez sauvegarder et restaurer les informations d’authentification de sécurité des modules HP ProtectTools installés.

2 Console d’administration de HP ProtectTools Security Manager

À propos de la console d’administration de HP ProtectTools Security Manager

L’administration de HP ProtectTools Security Manager est fournie par la console d’administration.

Lorsqu’il utilise la console, l’administrateur local peut :

- activer ou désactiver les fonctions de sécurité,
- gérer les utilisateurs de l’ordinateur,
- régler les paramètres spécifiques au périphérique,
- configurer les applications Security Manager,
- ajouter des applications Security Manager.

Utilisation de la console d’administration

La console d’administration de Security manager constitue l’emplacement central permettant de gérer HP ProtectTools Security Manager.

Pour ouvrir la console :

- Cliquez sur **Démarrer** > **Tous les programmes** > **Console d’administration de HP ProtectTools**, ou
- Cliquez sur le lien **Administration** dans le coin inférieur gauche de la console Security Manager.

La console d’administration est constituée de deux volets : un volet gauche et un volet droit. Le volet gauche comporte les outils d’administration. Le volet droit représente la zone de travail permettant de configurer les outils.

Le volet gauche de la console d’administration est composé des éléments suivants :

- **Accueil** : permet d’accéder facilement aux tâches fréquemment utilisées, parmi lesquelles l’activation des fonctions de sécurité, la définition des informations d’authentification de sécurité ainsi que la gestion des utilisateurs.
- **Système** : permet de gérer, au niveau du système, les fonctions de sécurité, les utilisateurs, ainsi que les périphériques d’authentification comme les lecteurs de Smart Card.

- **Applications** : comprend les outils permettant de configurer le fonctionnement de Security Manager et de ses applications.
- **Données** : comprend les outils permettant de gérer le cryptage de l'unité, ainsi que de sauvegarder et de récupérer les clés de cryptage.
- **Ordinateur** : propose les options de sécurité avancée permettant de rejeter de manière sélective différents types de périphériques susceptibles de compromettre la sécurité de l'ordinateur et de configurer des autorisations d'accès pour différents utilisateurs et différents groupes.
- **Outils de gestion** : ouvre votre navigateur par défaut sur une page Web. Cette page vous permet de découvrir des applications et des outils de gestion supplémentaires pour étendre les fonctions de Security Manager, ainsi que d'être informé dès que de nouvelles applications et mises à jour sont disponibles.
- **Liens** donne accès à :
  - **Assistant de configuration** : lance l'assistant de configuration qui vous guide lors de la configuration initiale de Security Manager.
  - **Aide** : ouvre le fichier d'aide qui comporte les informations relatives à Security Manager et à ses applications.
  - **À propos de** : affiche les informations relatives à HP ProtectTools Security Manager, y compris le numéro de version et les informations concernant les droits d'auteur.

Initiation à l'assistant de configuration

Pour pouvoir procéder à l'administration de HP ProtectTools Security Manager, vous devez être connecté en tant qu'administrateur système.

L'assistant de configuration de HP ProtectTools Security Manager vous guide lors de la configuration des fonctions de sécurité de HP ProtectTools. La console d'administration de HP ProtectTools Security permet de même d'accéder à de nombreuses fonctionnalités supplémentaires. Les paramètres disponibles à partir de l'assistant et des fonctions de sécurité supplémentaires peuvent être configurés par la console. L'accès est possible à partir du menu Démarrer de Windows ou à partir d'un lien disponible dans la console d'administration. Ces paramètres s'appliquent à l'ordinateur ainsi qu'à tous les utilisateurs qui partagent cet ordinateur.

Lorsque vous vous connectez à Windows pour la première fois, vous êtes invité à configurer HP ProtectTools Security Manager. Cliquez sur **OK** pour lancer l'assistant de configuration de Security Manager et être guidé au cours des étapes de base de la configuration du programme.

REMARQUE : Vous pouvez de même lancer l'assistant de sécurité en cliquant sur **Assistant de sécurité** dans la section inférieure du volet gauche de la console d'administration.

Suivez les instructions de l'assistant de configuration à l'écran jusqu'à ce que la configuration soit terminée.

Si vous n'achevez pas la procédure de l'assistant, ce dernier démarrera automatiquement jusqu'à ce que vous cliquiez sur **Ne plus afficher cet assistant**.

Pour utiliser les applications HP ProtectTools Security Manager, lancez HP ProtectTools Security Manager à partir du menu **Démarrer** ou en cliquant sur l'icône **Security Manager** avec le bouton droit de la souris dans la zone de notification de la barre des tâches (barre d'état système). La console

Security Manager et ses applications sont disponibles pour tous les utilisateurs qui partagent cet ordinateur.

Configuration de votre système

Le groupe d'applications **Système** est accessible depuis le menu **Outils** situé sur le côté gauche de la console d'administration.

L'utilisation des applications de ce groupe vous permet de configurer et de gérer les règles et les paramètres pour cet ordinateur, ses utilisateurs et périphériques.

Le groupe Système comprend les applications suivantes :

- **Sécurité** : pour la gestion des fonctions de sécurité, des règles d'authentification, ainsi que d'autres paramètres qui déterminent la façon dont les utilisateurs doivent s'authentifier lorsqu'ils se connectent sur l'ordinateur ou aux applications HP ProtectTools.
- **Utilisateurs** : pour la configuration, la gestion et l'inscription des utilisateurs de cet ordinateur.
- **Périphériques** : pour la gestion des paramètres des périphériques de sécurité intégrés ou connectés à l'ordinateur.

Activation des fonctions de sécurité

Les fonctions de sécurité activées ici s'appliquent à tous les utilisateurs de l'ordinateur.

1. Dans le volet gauche de la console d'administration, développez **Sécurité** puis cliquez sur **Fonctions**.
2. Pour activer une fonction de sécurité, cochez la case correspondante située à côté de **Sécurité de la connexion Windows** et/ou **Drive Encryption**.
    - **Sécurité de la connexion Windows** : protège votre compte Windows en imposant d'utiliser des informations d'authentification spécifiques pour y accéder.
    - **Drive Encryption** : protège vos données par le cryptage de votre disque dur. L'information est ainsi illisible pour les personnes qui ne disposent pas de l'autorisation adéquate.
3. Cliquez sur le bouton **Suivant**.
4. Cliquez sur le bouton **Appliquer**.

Définition des règles d'authentification de Security Manager

Les règles d'authentification de Security Manager pour cet ordinateur sont définies dans les onglets Connexion et Session. Ces onglets spécifient les informations d'authentification nécessaires pour authentifier chaque classe d'utilisateur lors de l'accès à l'ordinateur et aux applications HP ProtectTools pendant une session utilisateur.

Onglet Connexion

Permet de spécifier les informations d'authentification nécessaires pour accéder à l'ordinateur, décrypter le disque dur et se connecter à Windows :

1. Dans le volet gauche de la console d'administration, développez **Sécurité** puis cliquez sur **Authentification**.
2. Dans l'onglet **Connexion**, sélectionnez une catégorie d'utilisateurs dans la liste déroulante.
3. Dans la section **Règle**, spécifiez les informations d'authentification requises pour la catégorie d'utilisateurs sélectionnée en cochant les cases situées à côté de la liste des informations d'authentification. Vous devez spécifier au moins une information d'authentification.
4. Dans la liste déroulante de la section **Règle**, sélectionnez si UNE (une seule) des informations d'authentification, ou si TOUTES les informations d'authentification sont requises pour authentifier un utilisateur.
5. Cliquez sur le bouton **Appliquer**.

REMARQUE : Si la règle est paramétrée sur « TOUTES les informations d'authentification spécifiées sont requises pour l'authentification », que le système est configuré à la fois pour le mot de passe et pour la Java Card et que la Java Card est endommagée ou perdue, tous les administrateurs pourraient être dans l'incapacité d'accéder à Windows et avoir besoin d'outils spécifiques pour pouvoir y accéder à nouveau.

Onglet Session

Pour définir les règles d'authentification requises pour authentifier un utilisateur lorsqu'il se connecte aux applications HP ProtectTools pendant une session Windows :

1. Dans le volet gauche de la console d'administration, développez **Sécurité** puis cliquez sur **Authentification**.
2. Dans l'onglet **Session**, sélectionnez une catégorie d'utilisateurs.
3. Dans la section **Règle**, spécifiez les informations d'authentification requises pour la catégorie d'utilisateurs sélectionnée en cochant les cases situées à côté de la liste des informations d'authentification. Vous devez spécifier au moins une information d'authentification.
4. Dans la liste déroulante de la section **Règle**, sélectionnez si UNE (une seule) des informations d'authentification, ou si TOUTES les informations d'authentification sont requises pour authentifier un utilisateur.
5. Cliquez sur le bouton **Appliquer**.

Définition des paramètres

Vous pouvez spécifier les paramètres de sécurité avancée à autoriser. Pour modifier les paramètres :

1. Dans le volet gauche de la console d'administration, développez **Sécurité** puis cliquez sur **Paramètres**.
2. Cochez la case appropriée pour activer ou désactiver un paramètre spécifique.
3. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications.

REMARQUE : Le paramètre **Autoriser la connexion directe** permet aux utilisateurs de cet ordinateur d'ignorer la connexion Windows si l'authentification est effectuée au niveau du BIOS ou cryptée au niveau du disque.

Gestion des utilisateurs

Dans l'application Utilisateurs, l'administrateur Windows peut gérer les utilisateurs de cet ordinateur ainsi que les règles qui les affectent. Pour accéder à l'application Utilisateurs dans la console d'administration, cliquez sur **Utilisateurs**.

Les utilisateurs de HP ProtectTools sont répertoriés et leurs informations sont comparés aux règles d'authentification paramétrées dans Security Manager ainsi qu'aux informations d'authentification requises pour répondre à ces règles.

Pour afficher les règles en vigueur pour un utilisateur spécifique, sélectionnez l'utilisateur dans la liste puis cliquez sur le bouton **Afficher les règles**.

Pour superviser un utilisateur lorsqu'il inscrit des informations d'authentification, sélectionnez l'utilisateur dans la liste puis cliquez sur le bouton **Inscrire**.

Ajout d'un utilisateur

Ce processus ajoute des utilisateurs à la liste de connexion Drive Encryption. Avant d'ajouter un utilisateur, ce dernier doit déjà disposer d'un compte utilisateur Windows sur l'ordinateur et être présent pendant la procédure suivante pour indiquer le mot de passe.

Pour ajouter un utilisateur à la liste des utilisateurs :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche de la console d'administration, cliquez sur **Utilisateur**.
3. Cliquez sur le bouton **Ajouter**. La boîte de dialogue **Sélectionner l'utilisateur** s'ouvre.
4. Cliquez sur le bouton **Avancé**, puis sur le bouton **Rechercher maintenant** pour rechercher des utilisateurs à ajouter.
5. Cliquez sur l'utilisateur que vous souhaitez ajouter à la liste puis cliquez sur **OK**.
6. Cliquez sur **OK** dans la boîte de dialogue **Sélectionner l'utilisateur**.
7. Entrez le mot de passe Windows du compte sélectionné, puis cliquez sur **Terminer**.

REMARQUE : Vous devez utiliser un compte Windows existant et le saisir de manière exacte. Vous ne pouvez pas modifier ou ajouter un compte utilisateur Windows à l'aide de cette boîte de dialogue.

Suppression d'un utilisateur

REMARQUE : Cette procédure ne supprime pas le compte utilisateur Windows. Elle se contente de supprimer le compte de Security Manager. Pour supprimer entièrement un utilisateur, vous devez supprimer l'utilisateur dans Security Manager et dans Windows.

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche de la console d'administration, cliquez sur **Utilisateur**.

3. Cliquez sur le nom d'utilisateur du compte à supprimer, puis cliquez sur **Supprimer**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

Contrôle de l'état des utilisateurs

La section Utilisateur de la console d'administration présente l'état actuel de chaque utilisateur :

- **Coche verte** : indique que l'utilisateur a configuré la ou les méthodes de connexion de sécurité requises.
- **X rouge** : indique que l'utilisateur n'a pas configuré une méthode de connexion de sécurité requise et sera interdit d'accès à l'ordinateur lors de toute tentative de connexion. L'utilisateur doit exécuter l'assistant de configuration pour configurer la ou les méthodes de connexion requises.
- **Vide** : indique qu'aucune méthode de connexion de sécurité n'est requise.

Spécification des paramètres du périphérique

Dans l'application Périphérique, vous pouvez configurer l'ordinateur pour qu'il soit automatiquement verrouillé lorsqu'une Smart Card est retirée. L'ordinateur se verrouillera uniquement si la Smart Card a été utilisée comme information d'authentification lors de la connexion à Windows.

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche de la console d'administration, développez **Périphériques** puis cliquez sur **Smart Card**.
3. Cochez la case pour activer ou désactiver le verrouillage de l'ordinateur lorsqu'une Smart Card est retirée.

Configuration des paramètres des applications

La fenêtre Paramètres comprend les outils permettant de configurer le fonctionnement de Security Manager et de ses applications. Pour modifier les paramètres :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche de la console d'administration, cliquez sur **Paramètres**.
3. Dans l'onglet **Général**, choisissez les paramètres généraux pour HP ProtectTools Security Manager, puis cliquez sur le bouton **Appliquer**.
4. Dans l'onglet **Applications**, sélectionnez l'application que vous souhaitez activer ou désactiver, puis cliquez sur le bouton **Appliquer**.

REMARQUE : Vous devrez peut-être redémarrer l'ordinateur pour que l'activation ou la désactivation d'une application soit effective.

Cryptage d'unités

Drive Encryption for HP ProtectTools vous permet de crypter les disques durs des ordinateurs afin de les rendre illisibles et inaccessibles aux personnes non autorisées qui pourraient tenter d'y accéder, et ce même si le disque dur a été retiré de l'ordinateur ou envoyé à un service de récupération des données.

Pour activer ou désactiver Drive Encryption, cliquez sur l'assistant de configuration dans la console d'administration.

Pour plus d'informations sur l'utilisation de Drive Encryption for HP ProtectTools, consultez la section Drive Encryption for HP ProtectTools à la page 28.

Gestion de l'accès au périphérique

Device Access Manager for HP ProtectTools propose les options de sécurité avancée permettant de rejeter de manière sélective différents types de périphériques susceptibles de compromettre la sécurité de l'ordinateur. Pour plus d'informations sur l'utilisation de Device Access Manager for HP ProtectTools, consultez la section Device Access Manager for HP ProtectTools à la page 63.

3 HP ProtectTools Security Manager

HP ProtectTools Security Manager vous permet d'accroître de façon significative la sécurité de votre ordinateur. Utiliser les applications Security Manager vous permet de :

- Gérer votre connexion et vos mots de passe
- Modifier facilement votre mot de passe Windows
- Configurer des informations d'authentification, y compris une Smart Card
- Accroître la confidentialité et la sécurité des courriers électroniques, des documents et de la messagerie instantanée
- Détruire ou nettoyer le disque dur
- Afficher l'état du cryptage de l'unité
- Afficher les paramètres d'accès au périphérique
- Activer le logiciel permettant de récupérer un ordinateur volé
- Sauvegarder et restaurer les données de Security Manager

Connexion après la configuration de Security Manager

Les scénarios de connexion peuvent varier en fonction des niveaux de sécurité et des méthodes de connexion de sécurité choisis par l'administrateur Windows pendant la configuration. Voici quelques scénarios possibles :

- Si tous les niveaux de sécurité ont été configurés et que *toutes* les méthodes de connexion de sécurité sont requises, les utilisateurs doivent se connecter à l'aide de toutes les méthodes configurées lors de la première mise sous tension de l'ordinateur. Cette action permet de connecter l'utilisateur à Windows.
- Si tous les niveaux de sécurité ont été configurés et que *l'une* des méthodes de connexion de sécurité est permise, les utilisateurs peuvent se connecter à l'aide de l'une des méthodes de connexion de sécurité configurées lors de la première mise sous tension de l'ordinateur. Cette action permet de connecter l'utilisateur à Windows.
- Si les niveaux de sécurité de HP Drive Encryption et du Gestionnaire de mots de passe HP ont été configurés et que *toutes* les méthodes de connexion de sécurité sont requises, les utilisateurs doivent se connecter à l'aide de toutes les méthodes configurées lors de l'ouverture de l'écran de connexion de HP Drive Encryption. Cette action permet de connecter l'utilisateur à Windows.
- Si les niveaux de sécurité de HP Drive Encryption et du Gestionnaire de mots de passe HP ont été configurés et que *l'une* des méthodes de connexion de sécurité configurées est permise, les

utilisateurs peuvent se connecter à l'aide de l'une des méthodes de connexion de sécurité lors de l'ouverture de l'écran de connexion de HP Drive Encryption. Cette action permet de connecter l'utilisateur à Windows.

- Si le niveau de sécurité du Gestionnaire de mots de passe HP a été configuré et que *toutes* les méthodes de connexion de sécurité sont requises, les utilisateurs doivent se connecter à l'aide de toutes les méthodes configurées lors de l'ouverture de l'écran de connexion du Gestionnaire de mots de passe. Cette action permet de connecter l'utilisateur à Windows.
- Si le niveau de sécurité du Gestionnaire de mots de passe HP a été configuré et que *l'une* des méthodes de connexion de sécurité configurées est permise, les utilisateurs peuvent se connecter à l'aide de l'une des méthodes de connexion de sécurité lors de l'ouverture de l'écran de connexion du Gestionnaire de mots de passe. Cette action permet de connecter l'utilisateur à Windows.

REMARQUE : Si le niveau de sécurité du Gestionnaire de mots de passe HP n'a pas été configuré, les utilisateurs doivent tout de même entrer leur mot de passe Windows au niveau de l'écran de connexion de Windows, quelles que soient les méthodes de connexion de sécurité requises par les autres niveaux de sécurité.

Gestion de mots de passe

Password Manager for HP ProtectTools permet de créer et de gérer des connexions afin que vous puissiez lancer des sites Web et des programmes et vous y connecter en vous authentifiant avec les informations d'authentification inscrites.

Pour plus d'informations sur la gestion des mots de passe, consultez la section Password Manager for HP ProtectTools à la page 23.

Configuration d'informations d'authentification

Vos informations d'authentification Security Manager permettent de vérifier que c'est vous-même qui tentez de vous connecter. L'administrateur local de l'ordinateur peut configurer les informations d'authentification qui doivent être utilisées pour prouver votre identité lorsque vous vous connectez à votre compte Windows, à des sites Web ou à des programmes.

Les informations d'authentification disponibles varient en fonction des périphériques de sécurité intégrés ou connectés à l'ordinateur. Chaque information d'authentification prise en charge doit faire l'objet d'une entrée dans le groupe d'informations d'authentification.

Modification de votre mot de passe Windows

Security Manager vous offre la possibilité de modifier votre mot de passe Windows plus facilement et plus rapidement que par le biais du Panneau de configuration Windows.

Pour modifier votre mot de passe Windows :

1. Dans le volet gauche de HP ProtectTools Security Manager, cliquez sur **Informations d'authentification**.
2. Cliquez sur **Mot de passe Windows**.
3. Entrez votre mot de passe actuel dans la zone **Mot de passe Windows actuel**.

4. Entrez votre nouveau mot de passe dans les zones **Nouveau mot de passe Windows** et **Confirmer le nouveau mot de passe**.

5. Cliquez sur **Modifier**.

Configuration d'une Smart Card

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.

1. Dans le volet gauche de HP ProtectTools Security Manager, cliquez sur **Informations d'authentification**.

2. Cliquez sur **Smart Card**.

3. Si une Smart Card a été sélectionnée en tant que type de périphérique, vérifiez que la Smart Card est insérée.

   REMARQUE : Si la Smart Card n'est pas connectée, le bouton Suivant de la boîte de dialogue Sélectionner un jeton est désactivé.

4. Sur la page **Configurer une Smart Card**, entrez et confirmez un code PIN puis cliquez sur **Enregistrer**.

Gestion de la confidentialité des communications

Privacy Manager for HP ProtectTools vous permet d'utiliser des méthodes de sécurité avancée pour la connexion (authentification) afin de vérifier la source, l'intégrité et la sécurité des communications effectuées par courrier électronique, documents Microsoft Office ou messagerie instantanée.

Pour plus d'informations sur Privacy Manager for HP ProtectTools, consultez la section Privacy Manager for HP ProtectTools à la page 32.

Destruction ou nettoyage des fichiers

File Sanitizer for HP ProtectTools supprime les fichiers en les écrasant avec des données qui n'ont aucune signification. Ce processus, appelé « destruction », améliore considérablement la sécurité de l'information car il est ainsi très difficile de restaurer les fichiers supprimés. File Sanitizer améliore encore plus la sécurité de l'information en écrasant l'espace du disque dur qui a été utilisé à l'aide d'un processus appelé « nettoyage ». Les fichiers supprimés à l'aide de File Sanitizer ne peuvent pas être restaurés par le système d'exploitation ou par les autres logiciels de restauration couramment utilisés.

Pour plus d'informations sur l'utilisation de File Sanitizer for HP ProtectTools, consultez la section File Sanitizer for HP ProtectTools à la page 49.

Affichage de l'état du cryptage de l'unité

Drive Encryption est configuré dans la console d'administration par l'administrateur Windows. Les utilisateurs peuvent afficher l'état des cryptages dans Security Manager.

Pour afficher l'état du cryptage de l'unité :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **État du cryptage**. La page État du cryptage indique si le cryptage de l'unité est actif ou inactif, ainsi que les unités qui sont cryptées et celles qui ne sont pas cryptées.

Affichage de l'accès au périphérique

L'accès au périphérique est configuré par l'administrateur Windows dans la console d'administration. Les utilisateurs peuvent afficher les paramètres de l'accès au périphérique dans Security Manager.

Pour afficher les paramètres d'accès au périphérique :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, développez **Device Access Manager**.
3. Pour afficher les périphériques auxquels vous n'avez pas accès, cliquez sur **Configuration simple**. Vous n'avez pas accès aux périphériques qui sont cochés.
4. Pour afficher les utilisateurs ou les groupes qui n'ont pas accès, cliquez sur **Configuration de classe de périphérique**.
5. Cliquez sur un périphérique pour afficher les utilisateurs ou les groupes qui ont ou qui n'ont pas accès à ce périphérique.

Activation de la récupération d'un ordinateur volé

HP ProtectTools utilise LoJack Pro, crée par Absolute Software, pour commander, gérer et tenter de retrouver votre ordinateur à distance. Si votre ordinateur est perdu ou volé, le service de récupération d'Absolute s'associe avec les services de police pour tenter de retrouver l'ordinateur.

Pour plus d'informations sur l'utilisation de LoJack Pro, consultez la section LoJack Pro for HP ProtectTools à la page 68.

Ajout d'applications

Des applications supplémentaires peuvent être disponibles pour ajouter de nouvelles fonctions à ce programme.

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **En découvrir plus**.

   REMARQUE : Si le lien **En découvrir plus** n'est pas disponible, cela signifie qu'il a été désactivé par l'administrateur de votre ordinateur.

3. Dans l'onglet **Ajouter des applications**, recherchez des applications supplémentaires.
4. Dans l'onglet **Mises à jour et messages**, vous pouvez être informé des nouvelles applications et des mises à jour en cochant la case **Me tenir informé des nouvelles applications et des mises à jour** et en paramétrant un délai (nombre de jours) pour la vérification des mises à jour. Vous pouvez aussi cliquer sur le bouton **Vérifier maintenant** pour vérifier immédiatement les mises à jour.

Configuration des préférences

Sur la page Préférences, vous pouvez cocher la case **Afficher l'icône dans la barre des tâches** pour afficher l'icône Security Manager dans la zone de notification de la barre des tâches (barre d'état système).

Pour accéder à la page Préférences :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **Avancé**, puis sur **Préférences**.
3. Cochez ou décochez la case **Afficher l'icône dans la barre des tâches** puis cliquez sur **Appliquer**.

Sauvegarde et restauration

Il est recommandé de sauvegarder régulièrement les données de Security Manager. La fréquence à laquelle vous devez sauvegarder vos données dépend de la fréquence à laquelle elles sont modifiées. Par exemple, si vous ajoutez chaque jour de nouvelles connexions, il est recommandé d'effectuer une sauvegarde quotidienne.

Les sauvegardes peuvent aussi être utilisées pour le transfert de données d'un ordinateur vers un autre. Ces opérations sont aussi appelées importation et exportation. Il faut cependant rappeler que seules les données sont sauvegardées lors de cette opération.

Si vous restaurez le fichier de sauvegarde sur un autre ordinateur, ou sur le même ordinateur après avoir réinstallé le système d'exploitation, HP ProtectTools Security Manager doit être installé sur le système avant la restauration des données depuis le fichier de sauvegarde.

Sauvegarde des données

Lorsque vous sauvegardez vos données, vous sauvegardez vos informations de connexion et d'authentification sur un fichier crypté protégé par un mot de passe que vous saisissez vous-même.

Pour sauvegarder vos données :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Sauvegarder les données**.
4. Sélectionnez les modules que vous souhaitez inclure dans la sauvegarde. Le plus souvent, vous sélectionnerez tous les modules. Cliquez sur **Suivant**.
5. Entrez votre mot de passe pour vérifier votre identité, puis cliquez sur le bouton fléché.
6. Entrez le chemin et le nom du fichier de stockage. Par défaut, le fichier est enregistré dans le dossier Mes documents. Cliquez sur **Parcourir** pour spécifier un emplacement différent. Cliquez sur **Suivant**.
7. Entrez et confirmez un mot de passe pour protéger le fichier.
8. Cliquez sur **Terminer**.

Restauration de vos données

Vous restaurez vos données à partir d'un fichier crypté et protégé par un mot de passe qui a été crée au préalable avec la fonction Sauvegarder et restaurer de Security Manager.

Pour restaurer vos données :

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **Avancé**, puis sur **Sauvegarder et restaurer**.
3. Cliquez sur **Restaurer les données**.
4. Entrez le chemin et le nom du fichier de stockage ou cliquez sur **Parcourir** et sélectionnez le fichier.
5. Entrez le mot de passe utilisé pour protéger le fichier puis cliquez sur **Suivant**.
6. Sélectionnez les modules dont vous souhaitez restaurer les données. Le plus souvent, il s'agit de tous les modules de la liste. Cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

Modification de votre nom d'utilisateur et de votre image Windows

Votre nom d'utilisateur et votre image Windows sont affichés dans le coin supérieur gauche de Security Manager.

Pour modifier votre nom d'utilisateur et/ou votre image Windows :

1. Cliquez dans le coin supérieur gauche de Security Manager, qui comporte votre nom d'utilisateur et votre image.
2. Pour modifier votre nom d'utilisateur, entrez un nom dans la zone **Nom d'utilisateur Windows**.
3. Pour modifier votre image, cliquez sur le bouton **Choisir une image** pour rechercher une image.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

4 Password Manager for HP ProtectTools

Lorsque vous utilisez le Gestionnaire de mots de passe, votre connexion à Windows, aux sites Web et aux programmes est simplifiée et plus sécurisée.

Le Gestionnaire de mots de passe vous permet de configurer les écrans de connexion aux sites Web et aux programmes pour que l'accès soit plus simple et plus sécurisé. Le Gestionnaire de mots de passe commence par identifier vos connexions et les données spécifiques enregistrées dans les zones de saisie de chaque écran de connexion. Ensuite, lorsque vous êtes sur un écran de connexion et que votre identité a été vérifiée, le Gestionnaire de mots de passe remplit et envoie les données automatiquement.

Pour que l'accès soit encore plus rapide, vous pouvez afficher un menu pour vos connexions : il vous suffit d'utiliser une combinaison de touches de raccourci à configurer (par défaut, la combinaison est Ctrl-Alt-H). Dans le menu, il suffit de sélectionner une connexion et le Gestionnaire de mots de passe ouvre le site Web ou lance le programme, accède à l'écran de connexion et vous connecte automatiquement.

Pour vérifier votre identité, vous devez utiliser vos informations d'authentification HP ProtectTools, comme votre mot de passe Windows ou Smart Card, en fonction de la configuration de votre ordinateur. Cela signifie que vous utilisez les mêmes informations d'authentification pour vous connecter à tous les écrans de connexion que vous avez configurés. Vous pouvez ainsi créer des mots de passe forts que vous n'avez pas besoin de consigner par écrit ou de retenir. Votre compte sera plus sécurisé.

Le Gestionnaire de mots de passe vous permet de vérifier d'un simple coup d'œil si vos mots de passe présentent un danger pour la sécurité. Il permet aussi de générer des mots de passe forts et complexes que vous pourrez utiliser pour les nouveaux sites.

Le Gestionnaire de mots de passe vous permet d'afficher vos connexions, y compris les mots de passe, et de les modifier à tout moment. De nombreuses fonctions du Gestionnaire de mots de passe sont aussi disponibles à partir de l'icône Gestionnaire de mots de passe dès que l'écran de connexion d'un programme configuré est activé, ou sur l'écran de connexion des sites Web. Lorsque vous cliquez sur l'icône, un menu contextuel s'affiche. Les options ci-dessous y sont disponibles.

Pour les pages Web ou les programmes pour lesquels aucune connexion n'a été créée :

Les options suivantes s'affichent dans le menu contextuel :

- Ajouter [nomdedommaine.com] au Gestionnaire de mots de passe : utilisé pour ajouter une connexion pour l'écran de connexion actuel.
- Ouvrir le Gestionnaire de mots de passe : ouvre Security Manager à la page du Gestionnaire de mots de passe.

- Paramètres de l'icône du Gestionnaire de mots de passe : permet de spécifier les conditions d'affichage de l'icône.
- Aide : affiche l'aide en ligne pour l'application du Gestionnaire de mots de passe.

Pour les pages Web ou les programmes pour lesquels une connexion a déjà été créée :

Les options suivantes s'affichent dans le menu contextuel :

- Remplir les données de connexion : renseigne vos données de connexion dans les champs de connexion puis envoie la page (si l'envoi a été spécifié à la création ou lors de la dernière modification de la connexion).
- Modifier une connexion : permet de modifier vos données de connexion pour ce site Web.
- Ajouter une connexion : utilisé pour ajouter une nouvelle connexion pour le même site Web ou le même programme.
- Ouvrir le Gestionnaire de mots de passe : ouvre le tableau de bord Security Manager à la page du Gestionnaire de mots de passe.
- Aide : affiche l'aide en ligne pour l'application du Gestionnaire de mots de passe.

REMARQUE : L'administrateur de l'ordinateur a peut être configuré Security Manager de façon à ce que plusieurs informations d'authentification soient requises pour vérifier votre identité.

Ajout de connexions

Vous pouvez facilement et rapidement ajouter une connexion à un site Web ou à un programme. Il vous suffit d'entrer une seule fois vos données de connexion pour le site ou le programme. Le Gestionnaire de mots de passe entrera ensuite les informations à votre place. Vous pouvez utiliser ces connexions après avoir recherché le site Web ou le programme, ou simplement sélectionner une connexion dans le menu Connexion pour que le Gestionnaire de mots de passe ouvre le site Web ou le programme et vous connecte.

Pour ajouter une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez sur la flèche de l'icône du Gestionnaire de mots de passe, puis sélectionnez l'une des options suivantes. L'option à choisir dépend si l'écran de connexion est pour un site Web ou pour un programme.
   - Pour un site Web : sélectionnez **Ajouter [nomdedomaine] au Gestionnaire de mots de passe**.
   - Pour un programme : sélectionnez **Ajouter cet écran de connexion au Gestionnaire de mots de passe**.
3. Entrez vos données de connexion. Les champs de connexion à l'écran ainsi que les champs correspondants dans la boîte de dialogue comportent une large bordure orange. Vous pouvez choisir d'autres options d'affichage pour cette boîte de dialogue, comme Ajouter une connexion, dans l'onglet **Gestion** du Gestionnaire de mots de passe. Certaines options dépendent des

périphériques de sécurité qui sont connectés à l'ordinateur, comme le raccourci Ctrl-H ou l'insertion d'une Smart Card.

- Cliquez sur les flèches situées à droite d'un champ de connexion pour le renseigner avec un ou plusieurs choix prédéfinis.
- Vous pouvez également cliquer sur **Choisir d'autres champs** pour ajouter des champs supplémentaires à votre connexion depuis l'écran.
- Décochez **Envoyer les données de connexion** si vous souhaitez que les champs de connexion soient renseignés mais que vous ne souhaitez pas qu'ils soient envoyés.
- Si vous souhaitez afficher le mot de passe pour cette connexion, cliquez sur **Afficher le mot de passe**.

4. Cliquez sur **OK**. Le signe plus est supprimé de l'icône du Gestionnaire de mots de passe pour confirmer que la connexion a été créée.

Ensuite, à chaque fois que vous visitez ce site ou que vous lancez ce programme, l'icône du Gestionnaire de mots de passe s'affiche pour indiquer que vous pouvez utiliser les informations d'authentification enregistrées pour vous connecter.

Modification de connexions

Pour modifier une connexion :

1. Ouvrez l'écran de connexion d'un site Web ou d'un programme.
2. Cliquez sur la flèche de l'icône du Gestionnaire de mots de passe, puis sélectionnez **Modifier une connexion** pour afficher une boîte de dialogue et modifier vos informations de connexion. Les champs de connexion à l'écran ainsi que les champs correspondants dans la boîte de dialogue comportent une large bordure orange.
3. Modifiez vos informations de connexion.
   - Cliquez sur les flèches situées à droite d'un champ de connexion pour le renseigner avec un ou plusieurs choix prédéfinis.
   - Vous pouvez également cliquer sur **Choisir d'autres champs** pour ajouter des champs supplémentaires à votre connexion depuis l'écran.
   - Décochez **Envoyer les informations du compte** si vous souhaitez que les champs de connexion soient renseignés mais que vous ne souhaitez pas qu'ils soient envoyés.
   - Si vous souhaitez afficher le mot de passe pour cette connexion, cliquez sur Afficher le mot de passe.
4. Cliquez sur **OK**.

Utilisation du menu Connexions

Le Gestionnaire de mots de passe vous permet de lancer facilement et rapidement les sites Web et les programmes pour lesquels vous avez créé des connexions. Il vous suffit de double-cliquer sur la connexion d'un programme ou d'un site Web depuis le menu Connexions, ou dans l'onglet **Gestion** du Gestionnaire de mots de passe. Le Gestionnaire affiche alors l'écran de connexion correspondant et renseigne vos données de connexion. Par défaut, l'information est de même immédiatement envoyée

au site Web. Vous pouvez cependant choisir de ne pas l'envoyer en décochant **Envoyer les informations du compte** lors de la configuration initiale ou lors de la modification de la connexion.

Lorsque vous créez une connexion, elle est automatiquement ajoutée au menu Connexions du Gestionnaire de mots de passe.

Pour afficher le menu Connexions, appuyez sur le raccourci du Gestionnaire de mots de passe. Le raccourci par défaut est Ctrl-H. Vous pouvez modifier cette combinaison dans **Gestionnaire de mots de passe** > **Paramètres**.

Organisation des connexions en catégories

Utilisez des catégories pour pouvoir classer vos connexions. Il suffit de créer des catégories, puis de faire glisser vos connexions dans les catégories souhaitées.

Pour ajouter une catégorie :

1. Dans le volet gauche de Security Manager, sélectionnez **Gestionnaire de mots de passe**.
2. Sélectionnez l'onglet **Gestion**, puis cliquez sur **Ajouter une catégorie**.
3. Entrez le nom de la catégorie.
4. Cliquez sur **OK**.

Pour ajouter une connexion à une catégorie :

1. Positionnez le pointeur de la souris au-dessus de la connexion que vous souhaitez ajouter.
2. Appuyez sur le bouton gauche de la souris et maintenez-le enfoncé.
3. Faites glisser la connexion dans la liste des catégories. Les catégories s'affichent en surbrillance lorsque vous les survolez.
4. Relâchez le bouton de la souris lorsque la catégorie à laquelle vous souhaitez ajouter la connexion s'affiche en surbrillance.

Vos connexions ne sont pas déplacées vers la catégorie. Elles sont simplement copiées dans la catégorie sélectionnée. Une même connexion peut donc être ajoutée à plusieurs catégories. En cliquant sur **Toutes**, vous pouvez afficher toutes vos connexions.

Gestion de vos connexions

Le Gestionnaire de mots de passe vous permet de gérer vos informations de connexion (noms d'utilisateur, mots de passe et comptes de connexion) de façon intuitive et facile, depuis un emplacement unique.

La liste de vos connexions se situe dans l'onglet **Gestion**. Si plusieurs connexions ont été créées pour un même site Web, chaque connexion figure dans la liste du nom du site et est placée en retrait dans la liste des connexions.

Pour gérer vos connexions :

Dans le volet gauche de Security Manager, sélectionnez **Gestionnaire de mots de passe**, puis cliquez sur l'onglet **Gestion**.

- Ajouter une connexion : cliquez sur **Ajouter une connexion**, puis suivez les instructions affichées à l'écran.
- Modifier une connexion : sélectionnez une connexion puis cliquez sur **Modifier**. Modifiez les données de connexion.
- Supprimer une connexion : sélectionnez une connexion puis cliquez sur **Supprimer**.

Pour ajouter une connexion à un site Web ou à un programme :

1. Lancez l'écran de connexion du site Web ou du programme.
2. Cliquez sur l'icône du Gestionnaire de mots de passe pour en afficher le menu contextuel.
3. Sélectionnez **Ajouter une connexion supplémentaire**, puis suivez les instructions affichées à l'écran.

Évaluation de la force de votre mot de passe

Pour protéger votre identité, il est primordial d'utiliser des mots de passe sûrs pour vous connecter à des programmes et à des sites Web.

Le Gestionnaire de mots de passe permet de contrôler et d'améliorer facilement votre sécurité grâce à une analyse instantanée et automatisée de la force de chacun des mots de passe utilisés pour vous connecter à des sites Web et à des programmes. Vous pouvez vérifier la force des mots de passe que vous utilisez pour vos connexions dans l'onglet **Force des mots de passe**.

Paramètres de l'icône du Gestionnaire de mots de passe

Le Gestionnaire de mots de passe tente d'identifier les écrans de connexion aux sites Web et aux programmes. Lorsque le Gestionnaire identifie un écran de connexion pour lequel vous n'avez pas créé de connexion, il vous invite à ajouter une connexion pour l'écran en affichant l'icône du Gestionnaire de mots de passe avec un signe « + ».

Les paramètres suivants peuvent être configurés :

- Toujours adresser une invite : sélectionnez cette option afin que le Gestionnaire de mots de passe vous invite à ajouter une connexion à chaque fois qu'un écran de connexion n'en dispose pas.
- Ne pas adresser d'invite pour cet écran : sélectionnez cette option afin que le Gestionnaire de mots de passe ne vous invite plus à ajouter une connexion pour cet écran de connexion.
- Ne jamais adresser d'invite : sélectionnez cette option afin que le Gestionnaire de mots de passe ne vous invite jamais à ajouter de connexion pour un écran de connexion qui n'en dispose pas.

Des paramètres supplémentaires sont disponibles pour Privacy Manager en sélectionnant **Gestionnaire de mots de passe** > **Paramètres** dans Security Manager.

5 Drive Encryption for HP ProtectTools

REMARQUE : Drive Encryption for HP ProtectTools est disponible sur certains modèles uniquement.

Aujourd'hui, votre ordinateur ou celui de l'un de vos collègues peut être volé et des informations critiques sur votre entreprise peuvent être gravement compromises. Le cryptage de toutes les données de votre disque dur les rendent illisibles et inaccessibles aux personnes non autorisées qui peuvent tenter d'y accéder même si le disque dur a été retiré de l'ordinateur ou envoyé à un service de récupération des données.

Drive Encryption for HP ProtectTools est le premier logiciel prêt à l'emploi dans le domaine de la capacité de cryptage complet de volume. Il offre une protection complète des données en cryptant le disque dur de votre ordinateur. Lorsque Drive Encryption est activé, vous devez vous connecter sur l'écran de connexion de Drive Encryption qui s'affiche avant le démarrage de Windows.

REMARQUE : Drive Encryption for HP ProtectTools peut être activé uniquement à l'aide de l'assistant de configuration de la console d'administration de HP ProtectTools.

REMARQUE : Drive Encryption n'est pas pris en charge sur les systèmes d'exploitation 64 bits configurés avec RAID sur des systèmes qui utilisent un processeur AMD.

REMARQUE : Drive Encryption ne prend pas en charge la prévention des attaques par dictionnaire si la protection par mot de passe de Embedded Security for HP ProtectTools n'est pas configurée et utilise TPM pour protéger le mot de passe.

Drive Encryption :

- Vous permet de crypter la totalité de vos disques durs internes
- Vous propose un accès par mot de passe et une authentification de préamorçage simples d'utilisation
- Prend en charge Microsoft Windows XP, Windows Vista et Windows 7
- Utilise la puce de sécurité intégrée TPM (Trusted Platform Module)

Plusieurs tâches peuvent être effectuées dans Drive Encryption for HP ProtectTools :

- Gestion de Drive Encryption
  - Activer un mot de passe protégé par TPM
  - Crypter ou décrypter des unités individuelles
- Sauvegarde et récupération
  - Créer des clés de sauvegarde
  - S'inscrire à la restauration en ligne
  - Gérer un compte de restauration en ligne existant
  - Exécuter une restauration

△ **ATTENTION :** Si vous décidez de désinstaller le module Drive Encryption ou si vous utilisez une solution de sauvegarde et de restauration, vous devez tout d'abord déchiffrer toutes les unités chiffrées. Si vous n'effectuez pas ce déchiffrement, vous ne pourrez pas accéder aux données des unités chiffrées à moins d'avoir enregistré le service de récupération Drive Encryption. La réinstallation du module Drive Encryption ne vous permet pas d'accéder aux unités chiffrées.

Procédures de configuration

Ouverture de Drive Encryption

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Cliquez sur **Drive Encryption**.

Tâches générales

Activation de Drive Encryption

Utilisez l'assistant de configuration de la console d'administration de HP ProtectTools pour activer Drive Encryption.

Désactivation de Drive Encryption

Utilisez l'assistant de configuration de la console d'administration de HP ProtectTools pour désactiver Drive Encryption.

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 la sécurité de préamorçage dans la console d'administration de HP ProtectTools, vous êtes connecté à l'ordinateur immédiatement après sa mise sous tension et non pas au niveau de l'écran de connexion Drive Encryption.

1. Sélectionnez votre nom d'utilisateur, puis entrez votre mot de passe Windows ou le code PIN de la Java™ Card.
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 fenêtre Drive Encryption permet aux administrateurs Windows d'afficher et de modifier l'état de Drive Encryption (actif ou inactif) et d'afficher l'état du cryptage de tous les disques durs de l'ordinateur.

Activation d'un mot de passe protégé par TPM

Utilisez Embedded Security for HP ProtectTools pour activer le TPM. Après l'activation, la connexion au niveau de l'écran de connexion Drive Encryption requiert un nom d'utilisateur et un 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 Embedded Security for HP ProtectTools pour activer le TPM.
2. Dans le volet gauche de la console d'administration, développez **Drive Encryption**, puis cliquez sur **Gestion du cryptage**.
3. Cochez la case **Renforcer la sécurité avec TPM**.

Cryptage ou décryptage des unités individuelles

1. Dans le volet gauche de la console d'administration, développez **Drive Encryption**, puis cliquez sur **Gestion du cryptage**.
2. Cliquez sur le bouton **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 fenêtre Sauvegarde et restauration de Drive Encryption permet aux administrateurs Windows de sauvegarder et de restaurer les 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. Dans le volet gauche de la console d’administration, développez **Drive Encryption**, puis cliquez sur **Sauvegarde et restauration**.
2. Cliquez sur le bouton **Clés de sauvegarde**.
3. Sur la page 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.

REMARQUE : Pour plus d’informations sur la gestion et l’exécution d’une restauration, consultez le fichier d’aide de Drive Encryption for HP ProtectTools.

6 Privacy Manager for HP ProtectTools

Privacy Manager est un outil utilisé pour obtenir des certificats d'autorité qui vérifient la source, l'intégrité et la sécurité des communications effectuées à l'aide de la messagerie Microsoft, des documents Microsoft Office et d'Instant Messenger.

Privacy Manager exploite l'infrastructure de sécurité fournie par HP ProtectTools Security Manager. Cette infrastructure comprend les méthodes de connexion de sécurité suivantes :

- mot de passe Windows
- Carte HP ProtectTools Java™ Card
- Clé d'utilisateur de base Embedded Security for HP ProtectTools

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**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **Privacy Manager**.

– ou –

Cliquez avec le bouton droit de la souris sur l'icône **HP ProtectTools** de la zone de notification, à l'extrémité droite de la barre des tâches, sélectionnez **Privacy Manager for HP ProtectTools**, 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 **Envoyer en toute sécurité**, puis cliquez sur **Gestionnaire de certificats** ou sur **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 **Signer et crypter**, puis cliquez sur **Gestionnaire de certificats** ou sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Certificats**.
2. Cliquez sur le bouton **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 **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 **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de certificats**.
2. Cliquez sur un **Certificat Privacy Manager**.
3. Cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de certificats**.
2. Cliquez sur un **Certificat Privacy Manager**.
3. Cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de certificats**.
2. Cliquez sur le certificat Privacy Manager à utiliser comme certificat par défaut, puis cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Migration**.
2. Cliquez sur le bouton **Restaurer**.
3. Sur la page Fichier de migration, cliquez sur **Parcourir** pour rechercher le fichier .dppsm créé lorsque vous avez installé ou exporté le 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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de certificats**.
2. Cliquez sur **Avancé**.
3. Cliquez sur le certificat Privacy Manager à révoquer, puis sur **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. Le destinataire de contact authentifié vous adresse une réponse par courrier électronique. 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 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, rendez-vous sur le site Web DigitalPersona à l'adresse suivante : http://DigitalPersona.com/PrivacyManager.

Ajout d'un contact authentifié

1. Dans le volet gauche de Security Manager, développez **Privacy Manager**, cliquez sur **Contacts authentifiés**, puis cliquez sur le bouton **Inviter des contacts**.

   – ou –

   Dans la barre d'outils de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité**, puis cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, cliquez sur **Contacts authentifiés**, puis cliquez sur le bouton **Inviter des contacts**.

   – ou –

   Dans la barre d'outils de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **Envoyer en toute sécurité**, puis cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de contacts authentifiés**.
2. Cliquez sur un contact authentifié.
3. Cliquez sur **Détails du contact**.
4. Lorsque vous avez terminé de visualiser les détails, cliquez sur **OK**.

Suppression d'un contact authentifié

1. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Gestionnaire de contacts authentifiés**.
2. Cliquez sur le contact authentifié à supprimer.
3. Cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **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 **Vérifier la révocation**.
5. Cliquez sur **Fermer**.

Tâches générales

Utilisation de Privacy Manager dans Microsoft Office

Une fois que vous avez installé le certificat Privacy Manager, le bouton Signer et crypter s'affiche sur la partie droite de la barre d'outils de tous les documents Word, Excel et PowerPoint de Microsoft Office 2007.

REMARQUE : Si vous utilisez Microsoft Office 2007, toutes les mises à jour Microsoft doivent être appliquées afin d'éviter que certains courriers électroniques signés se retrouvent dans le dossier des courriers indésirables.

Configuration de Privacy Manager dans un document Microsoft Office

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

– ou –

1. Dans le volet gauche de Security Manager, développez **Privacy Manager**, cliquez sur **Paramètres**, puis cliquez 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 **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 **Signer et crypter**, puis sur **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 **Signer et crypter**, puis sur **Ajouter une ligne de signature avant de signer**.

   REMARQUE : Une coche apparaît en regard de l'option 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 **Signer et crypter**, puis sur **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 **Fournisseur de signatures Privacy Manager**.

   La boîte de dialogue Configuration de signature s'affiche.
4. Dans la zone sous **Signataire suggéré**, saisissez le nom du signataire suggéré.
5. Dans la zone sous **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 **Afficher la date dans la ligne de signature** pour afficher la date.
7. Cochez la case **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 **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 **Signer et crypter**, puis sur **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 **Signer et crypter**, puis sur **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 Confidentialité apparaît dans la barre d'outils de Microsoft Outlook et un bouton Envoyer en toute sécurité apparaît dans la barre d'outils de chaque message électronique Microsoft Outlook.

REMARQUE : Si vous utilisez Microsoft Office 2007, toutes les mises à jour Microsoft doivent être appliquées afin d'éviter que certains courriers électroniques signés se retrouvent dans le dossier des courriers indésirables.

Configuration de Privacy Manager pour Microsoft Outlook

1. Dans le volet gauche de Security Manager, développez **Privacy Manager**, cliquez sur **Paramètres**, puis cliquez sur l'onglet **Courrier électronique**.

   – ou –

   Dans la barre d'outils principale de Microsoft Outlook, cliquez sur la flèche vers le bas située en regard de **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 **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

1. Dans Microsoft Outlook, cliquez sur **Nouveau** ou sur **Répondre**.

2. Entrez votre message électronique.

3. Cliquez sur la flèche bas située à côté du bouton **Envoyer en toute sécurité**, puis sur **Signer et envoyer**.

4. Authentifiez-vous à l'aide de la méthode de connexion sécurisée de votre choix.

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 **Envoyer en toute sécurité**, puis cliquez sur **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

REMARQUE : Live Messenger est un produit Microsoft. Les modifications apportées par Microsoft à ce produit ne figurent pas dans ce document.

Pour Privacy Manager Chat, HP utilise Live Messenger. Vous devez installer Live Messenger et posséder un compte Live Messenger correspondant à votre certificat Privacy Manager pour utiliser Privacy Manager Chat.

En premier lieu, Live Messenger nécessite que les deux parties établissent un courrier électronique sécurisé et qu'elles utilisent les mêmes comptes de messagerie électronique dans 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 **Activités**, puis sur **Sécurité**.

3. 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 Certificat Privacy Manager. Pour plus d'informations sur l'installation d'un certificat Privacy Manager, consultez Demande et installation d'un certificat Privacy Manager à la page 33.

Il existe plusieurs méthodes pour démarrer Privacy Manager Chat. La procédure suivante utilise l'une des méthodes.

1. Connectez-vous à Live Messenger.
2. Cliquez avec le bouton droit de la souris sur l'icône **Security Manager** située en bas de la barre d'outils, puis sélectionnez **Privacy Manager for HP ProtectTools — Démarrer Chat**.
3. Lorsque vous y êtes invité, entrez votre mot de passe du système et démarrez la conversation avec les **Contacts authentifiés de Privacy Manager**.

La procédure suivante propose des méthodes alternatives pour démarrer Privacy Manager Chat.

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 **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 **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 **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 le volet gauche de Security Manager, développez **Privacy Manager**, cliquez sur **Paramètres**, puis cliquez 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 **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 **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 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 Entrée de messagerie instantanée. Pour afficher de nouveau la fenêtre Communications sécurisées, cliquez sur **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 **Afficher l'historique de** pour sélectionner uniquement des comptes spécifiques.

Démarrage de la visionneuse d'historique de Privacy Manager Chat

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Cliquez sur **Privacy Manager : Sign and Chat**, puis sur **Visionneuse d'historique de messagerie instantanée**.

   – ou –

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

   – ou –

   ▲ Sur la page de configuration de la messagerie instantanée, cliquez sur **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 **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 **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 **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 **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 **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 **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 **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 **Filtre avancé**.

   La boîte de dialogue de filtre avancé s'affiche.
2. Cochez la case **Afficher uniquement les sessions de la plage de dates spécifiée**.
3. Dans les cases **De** et **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 **Filtre avancé**.
2. Cochez la case **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Migration**.
2. Cliquez sur **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. Dans le volet gauche de Security Manager, développez **Privacy Manager**, puis cliquez sur **Migration**.
2. Cliquez sur **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**.

7 File Sanitizer for HP ProtectTools

File Sanitizer est un outil qui vous permet d'effacer en toute sécurité des fichiers et des dossiers critiques (informations ou fichiers personnels, 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 est différente de la suppression Windows standard (aussi appelée suppression simple dans File Sanitizer) dans la mesure où, lorsque vous détruisez une ressource, vous appelez un algorithme qui occulte les données. Il est donc pratiquement impossible de récupérer la ressource originale.

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.

À propos du nettoyage de l'espace libre

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.

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**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **File Sanitizer**.

   – ou –

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

  – ou –

- Cliquez avec le bouton droit de la souris sur l'icône HP ProtectTools de la zone de notification, à l'extrémité droite de la barre des tâches, sélectionnez **File Sanitizer**, puis cliquez sur **Ouvrir File Sanitizer**.

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. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **Nettoyage**.
2. Cochez la case **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 l'icône **Enregistrer**.

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.

Définition d’une planification de destruction

1. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **Détruire**.
2. Sélectionnez une option de destruction :
   - **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 s’affiche quand vous arrêtez Windows, vous demandant si vous souhaitez continuer la destruction des ressources sélectionnées ou si vous souhaitez ignorer la procédure. Cliquez sur Oui pour ignorer la procédure de destruction ou cliquez sur Non pour poursuivre la destruction. Sélectionnez rapidement l’option Oui ou Non car Windows ferme le logiciel pour préparer l’arrêt et affiche un écran d’erreur. Si vous sélectionnez Non pour poursuivre la destruction, Windows peut afficher un écran d’erreur indiquant que File Sanitizer ne répond pas. Laissez File Sanitizer terminer la destruction, puis recommencez la procédure d’arrêt.
   - **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.
   - **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.
   - **Séquence de touches** : choisissez cette option pour activer la destruction à l’aide d’une séquence de touches.
   - **Planificateur** : cochez la case 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 l’icône **Enregistrer**.

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. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **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 **Détruire les éléments suivants**, cochez la case en regard de chaque ressource pour laquelle vous souhaitez demander confirmation avant la destruction.

5. Cliquez sur **Appliquer**.

Personnalisation d'un profil de destruction de sécurité avancé

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. Dans le volet gauche de Security Manager, développez **File Sanitizer**, cliquez sur **Paramètres**, sélectionnez **Paramètres de sécurité avancés**, puis cliquez sur **Afficher les 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 **Options de destruction disponibles**, cliquez sur une ressource, puis sur **Ajouter**.

   b. Pour ajouter une ressource personnalisée, cliquez sur **Ajouter une option personnalisée**, saisissez un nom de fichier ou de dossier ou naviguez vers ce dernier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Ajouter**.

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

4. Sous **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 **Ne pas détruire les éléments suivants**, cliquez sur **Ajouter** pour sélectionner les ressources spécifiques à exclure de la destruction.

6. Une fois que la configuration du profil de destruction est terminée, cliquez sur **Appliquer**.

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. Dans le volet gauche de Security Manager, développez **File Sanitizer**, cliquez sur **Paramètres**, sélectionnez **Paramètres de suppression simple**, puis cliquez sur **Afficher les détails**.
2. Sélectionnez les ressources à supprimer :
   a. Sous **Options de suppression disponibles**, cliquez sur une ressource, puis sur **Ajouter**.
   b. Pour ajouter une ressource personnalisée, cliquez sur **Ajouter une option personnalisée**, saisissez un nom de fichier ou de dossier ou naviguez vers ce dernier, puis cliquez sur **OK**. Cliquez sur la ressource personnalisée, puis sur **Ajouter**.

   REMARQUE : Pour supprimer une ressource des options de suppression disponibles, cliquez sur la ressource, puis sur **Supprimer**.
3. Sous **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 **Ne pas supprimer les éléments suivants**, cliquez sur **Ajouter** pour sélectionner les ressources spécifiques que vous souhaitez exclure de la destruction.
5. Une fois que la configuration du profil de suppression simple est terminée, cliquez sur **Appliquer**.

Tâches générales

Utilisation d'une séquence de touches pour démarrer la destruction

Pour spécifier une séquence de touches, procédez comme suit :

1. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **Détruire**.
2. Cochez la case **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 toute autre combinaison 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 de la souris sur l’icône **HP ProtectTools** de la zone de notification, à l’extrémité droite de la barre des tâches, sélectionnez **File Sanitizer**, puis cliquez sur **Destruction unique**.
2. Lorsque la boîte de dialogue Parcourir s’affiche, naviguez vers la ressource à détruire, puis cliquez sur **Ouvrir**.

   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 **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. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **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 **Ouvrir**.
4. 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 de la souris sur l’icône **HP ProtectTools** de la zone de notification, à l’extrémité droite de la barre des tâches, sélectionnez **File Sanitizer**, puis cliquez sur **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 **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 de la souris sur l'icône **HP ProtectTools** de la zone de notification, à l'extrémité droite de la barre des tâches, sélectionnez **File Sanitizer**, puis cliquez sur **Nettoyer maintenant**.
2. Un message de notification apparaît pour vérifier qu'une opération de nettoyage a commencé.

– ou –

1. Dans le volet gauche de Security Manager, développez **File Sanitizer**, puis cliquez sur **Nettoyage**.
2. Cliquez sur **Nettoyer maintenant**.
3. Un message de notification apparaît pour vérifier qu'une opération de nettoyage a commencé.

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 s'affiche 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 d'achèvement) et 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

8 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools permet de gérer l'installation et la configuration de la Java Card afin de l'utiliser avec le clavier HP Smart Card. Java Card HP est un périphérique de sécurité personnel qui protège les données d'authentification et nécessite la carte et un code PIN pour autoriser l'accès, comme lorsqu'on utilise une carte ATM avec un code PIN. La Java Card peut être utilisée pour accéder au Gestionnaire de mots de passe, à Drive Encryption, au BIOS HP ou à tout point d'accès tiers.

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

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

Attribution d'un code PIN à la Java Card

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

Pour attribuer un code PIN à une Java Card :

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

1. Sélectionnez **Démarrer** > **Tous les programmes** > **HP ProtectTools Security Manager**.
2. Dans le volet gauche de Security Manager, cliquez sur **Informations d'authentification**, puis sur **Smart Card**.
3. Insérez une nouvelle Java Card dans le lecteur de cartes.
4. Entrez votre mot de passe Windows, puis entrez le code PIN d'une Smart Card.
5. Cliquez sur **Enregistrer**.

9 Embedded Security for HP ProtectTools

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

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

- Cryptage amélioré de fichiers et de dossiers EFS (Encryption File System) de Microsoft (EFS n'est pas disponible sur les versions de Windows Home)
- 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
- Certains modèles proposent une authentification à la mise sous tension de la sécurité intégrée
- 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 (Trusted Platform Module) améliore et active d'autres fonctions de sécurité de HP ProtectTools Security Manager. Par exemple, Password Manager for HP ProtectTools peut utiliser la puce intégrée comme facteur d'authentification lorsque l'utilisateur se connecte à Windows.

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 dans Computer Setup

La puce de sécurité intégrée peut être activée dans l'assistant d'initialisation rapide ou dans l'utilitaire Computer Setup, comme décrit ci-après. Cette procédure ne peut pas être effectuée dans BIOS Configuration for HP ProtectTools.

Pour activer la puce de sécurité intégrée dans Computer Setup :

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 **Security** (Sécurité), **Setup password** (Définir le mot de passe), puis appuyez sur Entrée.
3. Entrez votre mot de passe dans les champs **New password** (Nouveau mot de passe) et **Verify new password** (Vérifier le nouveau mot de passe), puis appuyez sur F10.
4. Dans le menu **Security** (Sécurité), utilisez les touches de direction pour sélectionner **TPM Embedded Security** (Sécurité intégrée TPM), puis appuyez sur Entrée.
5. Sous **Embedded Security** (Sécurité intégrée), si le périphérique est masqué, sélectionnez **Available** (Disponible).
6. Sélectionnez **Embedded security device state** (État du périphérique de sécurité intégrée) et modifiez l'état sur **Enable** (Activer).
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.

Installation de Embedded Security for HP ProtectTools

Pour installer Embedded Security for HP ProtectTools :

1. Cliquez sur **Démarrer**, sur **Tous les programmes**, puis sur **Installer Embedded Security for HP ProtectTools**.
2. Sélectionnez **Accepter** pour l'avertissement UAC (User Account Control).
3. Cliquez sur **Suivant**, puis entrez le nom d'utilisateur et le nom de la société si nécessaire.
4. Cliquez sur **Suivant**, sur **Installer**, puis sur **Terminer** lorsque vous avez fini.
5. Sélectionnez **Oui** ou **Non** pour la demande de réamorçage.

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 de la souris sur l'icône HP ProtectTools Security Manager de la zone de notification, à l'extrémité droite de la barre des tâches, et sélectionnez **Initialisation de Embedded Security**.

   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 sécurité intégrée n'est pas ouvert, 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 **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.

REMARQUE : Le cryptage de fichiers et de dossiers n'est pas pris en charge par les versions de Windows Home.

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.

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**, **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 **Configurer**. L'assistant de sauvegarde de HP Embedded Security for HP ProtectTools s'ouvre.
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**, **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 **Tout restaurer**. L'assistant de sauvegarde de HP Embedded Security for HP ProtectTools s'ouvre.
4. Suivez les instructions à l'écran.

Modification du mot de passe propriétaire

Pour modifier le mot de passe propriétaire

1. Cliquez sur **Démarrer**, **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.

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.

10 Device Access Manager for HP ProtectTools

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

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

REMARQUE : Device Access Manager utilise Utilisateurs locaux et groupes de Windows pour gérer l'accès. Les versions de Windows Home ne prenant pas en charge Utilisateurs locaux et groupes, Device Access Manager ne fonctionnera pas correctement. Device Access Manager fonctionnera cependant avec la version Microsoft Windows Vista Home si vous utilisez les commandes DOS pour la configuration utilisateur. Consultez le fichier d'aide de Device Access Manager pour plus de détails.

Démarrage du service en arrière-plan

Pour les profils de périphériques à appliquer, le service d'arrière-plan HP ProtectTools Device Locking/Auditing doit être en cours d'exécution. Lorsque vous tentez d'appliquer des profils de périphérique pour la première fois, la console d'administration de HP ProtectTools ouvre une boîte de dialogue vous demandant si vous souhaitez démarrer le service d'arrière-plan. Cliquez sur **Oui** pour démarrer le service d'arrière-plan et le définir pour un démarrage à chaque démarrage du système.

Configuration simple

Device Access Manager crée un nouveau groupe d'utilisateurs durant l'initialisation, appelé Administrateurs de périphériques, qui permet d'accéder aux périphériques et de les explorer comme un administrateur. Placez dans ce groupe les utilisateurs auxquels vous souhaitez accorder un accès administrateur aux périphériques que vous contrôlez avec la configuration simple de Device Access Manager.

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

- Les périphériques USB pour tous les non-administrateurs de périphériques
- Tous les supports amovibles (disquettes, lecteurs de musique personnels, clés, etc.) pour tous les non-administrateurs de périphériques
- Tous les lecteurs de DVD/CD-ROM pour tous les non-administrateurs de périphériques
- Tous les ports parallèles et en série pour tous les non-administrateurs de périphériques

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

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
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 l'icône **Enregistrer**.

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**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Configuration de classe de périphérique**.
3. Dans la liste de périphériques, cliquez sur la classe de périphériques à configurer.
4. Cliquez sur **Ajouter**. La boîte de dialogue **Sélection d'utilisateurs ou groupes** s'affiche.
5. Cliquez sur **Avancé**, puis sur **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**, **Tous les programmes**, puis sur **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Configuration de classe de périphérique**.
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**.

Refus ou autorisation d’accès à un utilisateur ou à un groupe

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d’administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Configuration de classe de périphérique**.
3. Dans la liste de périphériques, cliquez sur la classe de périphériques à configurer.
4. Sous **Utilisateur/Groupe**, cliquez sur l’utilisateur ou groupe auquel refuser l’accès.
5. Cliquez sur **Refuser** en regard de l’utilisateur ou groupe auquel refuser l’accès.
6. Cliquez sur l’icône **Enregistrer**, puis cliquez sur **OK**.

Paramètres d’accès utilisateur (avancé)

Les paramètres d’accès utilisateur permettent aux administrateurs de spécifier les utilisateurs et les groupes qui sont autorisés à utiliser les affichages Configuration simple et Configuration de classe de périphérique.

Un utilisateur ou un groupe doit disposer de l’accès **Afficher (en lecture seule) les paramètres de configuration** pour afficher les informations de la configuration simple et de la configuration de classe de périphérique.

Un utilisateur ou un groupe doit disposer de l’accès **Modifier les paramètres de configuration** pour modifier les informations de la configuration simple et de la configuration de classe de périphérique.

Un utilisateur ou un groupe doit disposer de l’accès **Droits complets d’administrateur utilisateur** pour modifier les paramètres des affichages de la configuration simple et de la configuration de classe de périphérique.

Ajout d’un utilisateur ou d’un groupe

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d’administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Paramètres d’accès utilisateur**.
3. Cliquez sur **Ajouter**. La boîte de dialogue **Sélectionner les utilisateurs ou les groupes** s’ouvre.
4. Cliquez sur **Avancé**, puis sur **Rechercher maintenant** pour rechercher des utilisateurs ou des groupes à ajouter.
5. Cliquez sur l’utilisateur ou le groupe que vous souhaitez ajouter à la liste des utilisateurs et des groupes disponibles, puis cliquez sur **OK**.
6. Cliquez sur **OK**.
7. Cliquez sur l’icône **Enregistrer**.

Suppression d’un utilisateur ou d’un groupe

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d’administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Paramètres d’accès utilisateur**.
3. Cliquez sur l’utilisateur ou le groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Cliquez sur l’icône **Enregistrer**.

Accord ou refus d’autorisations

1. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **Console d’administration de HP ProtectTools**.
2. Dans le volet gauche, développez **Device Access Manager**, puis cliquez sur **Paramètres d’accès utilisateur**.
3. Dans la zone **Groupe ou noms d’utilisateur**, sélectionnez un nom d’utilisateur ou de groupe.

4. Dans la zone **Autorisations**, cochez les cases **Autoriser** ou **Refuser** pour les autorisations appropriées.
5. Cliquez sur l'icône **Enregistrer**.

11 LoJack Pro for HP ProtectTools

LoJack Pro for HP ProtectTools est un outil qui permet de surveiller, gérer et repérer votre ordinateur à distance.

Une fois que LoJack Pro for HP ProtectTools est activé, il est configuré à partir du centre d'assistance d'Absolute Software. À partir du centre d'assistance, l'administrateur peut configurer LoJack for HP ProtectTools pour commander ou gérer l'ordinateur. Si le système est égaré ou volé, le centre d'assistance peut aider les autorités locales à localiser et récupérer l'ordinateur. Si LoJack Pro est configuré, il peut continuer à fonctionner même si le disque dur est effacé ou remplacé.

Pour activer LoJack Pro for HP ProtectTools :

1. Connectez-vous à Internet.
2. Cliquez sur **Démarrer**, **Tous les programmes**, puis sur **HP ProtectTools Security Manager**.
3. Dans le volet gauche de Security Manager, cliquez sur **Récupération d'un ordinateur volé**.
4. Pour lancer l'assistant d'activation de LoJack Pro, cliquez sur le bouton **Activer maintenant**.
5. Entrez vos informations de contact ainsi que les informations relatives à votre carte de crédit ou entrez une clé de produit pré-payée.

L'assistant d'activation traite la transaction en toute sécurité et installe votre compte utilisateur sur le site Web du centre d'assistance d'Absolute Software. Une fois que l'installation est terminée, vous recevez un courrier électronique vous confirmant les informations relatives à votre compte.

Si vous avez déjà exécuté l'assistant d'activation de LoJack Pro et que vous possédez déjà un compte utilisateur auprès du centre d'assistance, contactez votre représentant HP pour acheter des licences supplémentaires.

Pour vous connecter au centre d'assistance :

1. Accédez à l'adresse https://cc.absolute.com/.
2. Dans les champs **Identifiant de connexion** et **Mot de passe**, entrez les informations d'authentification reçues dans le courrier électronique de confirmation, puis cliquez sur le bouton **Connexion**.

Le centre d'assistance vous permet de :

- Contrôler vos ordinateurs.
- Protéger vos données distantes.
- Signaler le vol d'un ordinateur protégé par LoJack Pro.

Cliquez sur **En savoir plus** pour obtenir plus d'informations sur LoJack Pro for HP ProtectTools.

Glossaire

activation : La tâche doit être terminée pour que les fonctions de Drive Encryption soient accessibles. Le module Drive Encryption est activé à l'aide de l'assistant de configuration de la console d'administration de HP ProtectTools Security Manager. Seul un administrateur peut activer Drive Encryption. Le processus d'activation consiste à activer le logiciel, chiffrer l'unité, créer un compte utilisateur et créer la clé de chiffrement de sauvegarde initiale sur un périphérique de stockage 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.

autorité de certification : Service qui émet les certificats requis pour exécuter une infrastructure de clés publiques.

bouton 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 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.

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.

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.

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.

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 : Voir **nettoyage de l'espace libre**.

nettoyage de l'espace libre : Inscription sécurisée de données aléatoires par-dessus des ressources supprimées du disque dur afin de déformer le contenu des ressources supprimées et rendre leur récupération plus difficile.

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

puce de sécurité intégrée du module TPM (Trusted Platform Module) : 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.

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. Matériel et microprogramme offrant une sécurité contre les attaques orientées vers les données et les logiciels d'un ordinateur.

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