Logiciel de sécurité HP ProtectTools for Small Business, version 5.10

Manuel de l'utilisateur

Manuel de l'utilisateur du logiciel de sécurité HP ProtectTools for Small Business version 5.10

HP Business PC

Deuxième édition : mai 2010

Référence du document : 610663-052

À propos de ce livre

Ce manuel fournit des informations sur le logiciel de sécurité HP ProtectTools for Small Business.

⚠ **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 1
Fonctions HP ProtectTools 2

2 Guide de configuration simple pour les options les plus utiles 4
Initiation 4
Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) 6
Affichage et gestion des authentifications enregistrées dans Credential Manager 8
File Sanitizer for HP ProtectTools 11
Device Access Manager for HP ProtectTools 14
Drive Encryption for HP ProtectTools 16

3 Avantages de HP ProtectTools for Small Business 18
Accès au logiciel de sécurité HP ProtectTools for Small Business 18
Objectifs de sécurité fondamentaux 18
Restriction de l'accès à des données confidentielles 18
Protection contre des accès non autorisés depuis des sites internes ou externes 19
Création de stratégies de mot de passe fort 19
Éléments de sécurité supplémentaires 19
Affectation de rôles de sécurité 19
Gestion de mots de passe HP ProtectTools 20
Création d'un mot de passe sécurisé 20
Sauvegarde des informations d’authentification et des paramètres 21

4 Console d'administration de HP ProtectTools Security Manager 22
À propos de la console d'administration de HP ProtectTools Security Manager 22
Utilisation de la console d'administration 22
Mise en route avec l'assistant de configuration 23
Configuration de votre système 24
Activation des fonctions de sécurité 24
Définition des règles d'authentification de Security Manager 24
Onglet Connexion 24
Onglet Session 25
Définition des paramètres 25

Gestion des utilisateurs 25
Ajout d'un utilisateur 26
Suppression d'un utilisateur 26
Contrôle de l'état des utilisateurs 26
Configuration des paramètres des applications 27
Cryptage d’unités 27
Gestion de l'accès au périphérique 27

5 HP ProtectTools Security Manager 28
Gestion de mots de passe 28
Configuration d'informations d'authentification 28
Modification de votre mot de passe Windows 28
Destruction ou nettoyage des fichiers 29
Affichage de l’état du cryptage de l’unité 29
Affichage de l'accès au périphérique 29
Ajout d'applications 30
Configuration des préférences 30
Sauvegarde et restauration 30
Sauvegarde des données 31
Restauration de vos données 31
Modification de votre nom d'utilisateur et de votre image Windows 31

6 Drive Encryption for HP ProtectTools 33
Procédures de configuration 34
Ouverture de Drive Encryption 34
Tâches générales 34
Activation de Drive Encryption 34
Désactivation de Drive Encryption 34
Connexion après activation de Drive Encryption 34
Tâches avancées 34
Gestion de Drive Encryption (administrateur uniquement) 34
Cryptage ou décryptage des unités individuelles 35
Sauvegarde et restauration (tâche de l’administrateur) 35
Création de clés de sauvegarde 35

7 Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) 36
Ajout de connexions 37
Modification de connexions 38
Utilisation du menu Connexions 38
Organisation des connexions en catégories 39
Gestion de vos connexions 39
Évaluation de la force de votre mot de passe 40
Paramètres de l'icône du Gestionnaire de mots de passe 40

8 File Sanitizer for HP ProtectTools 41
Procédures de configuration 42
Ouverture de File Sanitizer 42
Configuration d'une planification de nettoyage de l'espace libre 42
Définition d'une planification de destruction 42
Sélection ou création d'un profil de destruction 43
Sélection d'un profil de destruction prédéfini 43
Personnalisation d'un profil de destruction de sécurité avancé 43
Personnalisation d'un profil de suppression simple 44
Tâches générales 45
Utilisation d'une séquence de touches pour démarrer la destruction 45
Utilisation de l'icône File Sanitizer 45
Destruction manuelle d'une ressource 45
Destruction manuelle de tous les éléments sélectionnés 46
Activation manuelle du nettoyage de l'espace libre 46
Annulation d'une opération de destruction ou de nettoyage de l'espace libre 46
Affichage des fichiers journaux 47

9 Device Access Manager for HP ProtectTools 48
Démarrage du service en arrière-plan 48
Configuration simple 48
Configuration de classes de périphériques (tâches avancées) 49
Ajout d'un utilisateur ou groupe 49
Suppression d'un utilisateur ou groupe 49
Refus ou autorisation d'accès à un utilisateur ou à un groupe 50
Paramètres d'accès utilisateur (avancé) 51
Ajout d'un utilisateur ou d'un groupe 51
Suppression d'un utilisateur ou d'un groupe 51
Accord ou refus d'autorisations 51

Glossaire 53

Index 55

1 Introduction à la sécurité

HP comprend que votre temps est extrêmement précieux et que vous devez vous concentrer sur l'exécution et le développement de vos affaires au lieu d'avoir à vous inquiéter de disposer des logiciels de sécurité appropriés pour protéger vos PC, vos données et votre entreprise.

Il est donc important d'envisager proactivement des solutions de sécurité simples à utiliser mais garantissant une forte protection de vos ressources professionnelles. La sécurité n'est pas un plus, mais bel et bien une nécessité absolue.

HP fournit une protection simple à mettre en œuvre et conviviale, nommée HP ProtectTools for Small Business.

HP ProtectTools for Small Business est un logiciel de sécurité qui fournit des fonctions conçues pour empêcher tout accès non autorisé à l'ordinateur et aux données critiques. La fonctionnalité de sécurité évoluée est fournie par les divers modules logiciels HP ProtectTools.

HP ProtectTools for Small Business offre deux versions qui peuvent être utilisées : la console d'administration de HP ProtectTools Security Manager et HP ProtectTools Security Manager (pour les utilisateurs lambda). Les versions administrateur et utilisateur sont toutes deux 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 lambda)	• 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

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.

Fonctions HP ProtectTools

Le tableau suivant détaille les fonctions clés des modules HP ProtectTools for Small Business :

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. • 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 lambda)	• 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 de Device Access Manager. • Configuration des préférences et des options de sauvegarde et de restauration.
Credential Manager for HP ProtectTools (Gestionnaire de mots de passe)	• Est conçu pour enregistrer, organiser et protéger les noms d'utilisateur et mots de passe. • Vous permet de configurer les écrans de connexion aux sites Web et aux programmes pour garantir un accès rapide et sécurisé. • Lorsque vous accédez à divers sites Web et que vous voulez enregistrer vos noms d'utilisateur et mots de passe, entrez-les dans le Gestionnaire de mots de passe afin de ne pas avoir à vous les rappeler par la suite. La prochaine fois que vous visiterez un de ces sites, le Gestionnaire de mots de passe remplira et enverra les données automatiquement. • Vous permet de créer des mots de passe forts que vous n'avez pas besoin de consigner par écrit ni de retenir, et d'avoir ainsi des comptes plus sécurisés.
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. • Vous permet de respecter les exigences légales ou industrielles relatives à la protection des données confidentielles et sensibles. • Protège vos données contre les accès non autorisés en chiffrant l'intégralité du disque dur. Les données ne seraient ainsi pas compromises si l'ordinateur venait à être volé ou si le disque dur était retiré du système d'origine et placé dans un autre système.

Module	Principales fonctions
File Sanitizer for HP ProtectTools	• La suppression de données sous Windows ne supprime pas totalement le contenu de votre disque dur. Windows supprime uniquement les références aux données. Les données restent sur le disque dur jusqu'à ce qu'un autre fichier écrase la même zone du disque dur avec de nouvelles informations. Cependant, avec File Sanitizer, vous pouvez effacer complètement et automatiquement les documents, l'historique du navigateur Web, les fichiers temporaires, etc. • Vous permet d'effacer (ou détruire) en toute sécurité des fichiers et des dossiers critiques (informations ou fichiers personnels, données d'historique ou de navigation sur le Web ou autres composants de données) sur votre ordinateur et de nettoyer régulièrement votre disque dur (écraser les données précédemment supprimées).
Device Access Manager for HP ProtectTools	• Peut être utilisé pour contrôler l'accès aux unités multimédia, aux périphériques USB et aux autres périphériques matériels en fonction des profils utilisateur. • Vous permet de limiter l'aptitude d'un utilisateur à stocker des données critiques. • Empêche les utilisateurs d'utiliser des périphériques de stockage externes, tels qu'un lecteur de musique personnel, afin de copier des données à partir d'un PC ou du réseau. • Empêche les utilisateurs d'introduire des virus dans le système à partir de supports externes. • Vous permet de désactiver de manière sélective un groupe de périphériques (clés USB, périphériques inscriptibles, lecteurs de musique personnels, etc.) par utilisateur ou par groupe d'utilisateurs. La personne disposant d'un mot de passe administrateur peut se connecter et copier des informations à partir du PC, mais les autres utilisateurs ne le peuvent pas.

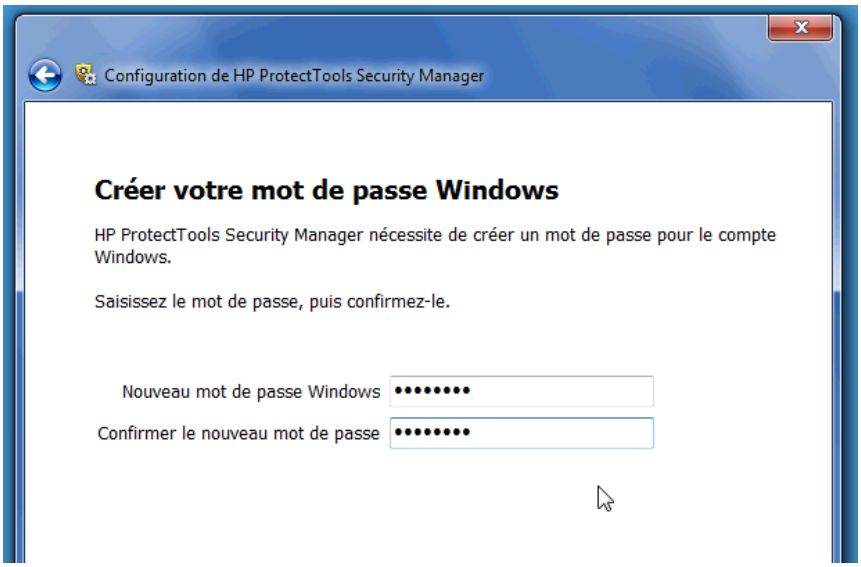
2 Guide de configuration simple pour les options les plus utiles

Ce Guide de configuration simple est conçu pour faire la démonstration des étapes de base à suivre pour activer les options les plus courantes et les plus utiles de HP ProtectTools for Small Business. Ce logiciel comprend de nombreux outils et options qui vous permettront d'affiner vos préférences et de configurer votre contrôle d'accès. Le Guide de configuration simple vise principalement à vous permettre d'exécuter chaque module avec un minimum d'efforts et de temps. Pour plus d'informations, il vous suffit de sélectionner le module qui vous intéresse et de cliquer sur le bouton « ? » ou Aide dans l'angle supérieur droit. Ce bouton fournit automatiquement des informations d'aide sur la fenêtre active.

Initiation

1. Ouvrez HP ProtectTools Security Manager à partir de l'icône Gadget ou à partir de l'icône de la barre des tâches (bouclier doré), ou cliquez sur **Démarrer** > **Tous les programmes** > **HP**.

2. Entrez votre mot de passe Windows ou créez-en un.

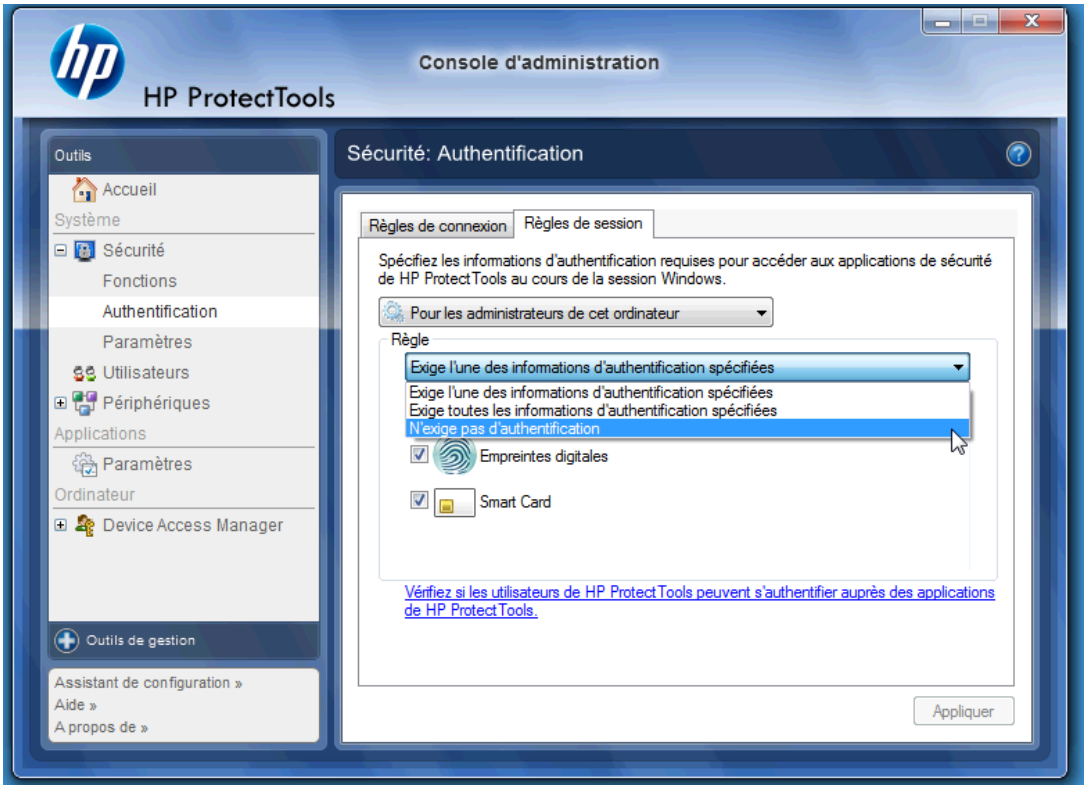


3. Terminez l'exécution de l'assistant de configuration.

REMARQUE : Par défaut, HP ProtectTools Security Manager est défini avec une stratégie d'authentification forte.

Ce paramètre est conçu pour éviter les accès non autorisés lorsque vous êtes connecté à Windows et doit être utilisé lorsqu'une sécurité élevée est nécessaire ou si les utilisateurs s'éloignent fréquemment de leur poste pendant la journée. Si vous souhaitez modifier ce paramètre, cliquez sur l'onglet Règles de session et faites vos sélections.

Pour configurer HP ProtectTools Security Manager afin d'utiliser uniquement la connexion Windows initiale pour la session entière, modifiez la configuration suivante.



Pour que HP ProtectTools Security Manager s'authentifie une seule fois pendant la connexion Windows, procédez comme suit :

1. Cliquez sur **Démarrer** > **Tous les programmes** > **HP** > **Console d'administration de HP ProtectTools**.
2. Dans le volet gauche **Outils**, sélectionnez **Authentification** dans le groupe **Sécurité**.
3. Cliquez sur l'onglet **Règles de session** et sélectionnez **N'exige pas d'authentification** dans le menu déroulant sous **Règle**.
4. Cliquez sur le bouton **Appliquer** lorsque vous avez fini.

Credential Manager for HP ProtectTools (Gestionnaire de mots de passe)

Les mots de passe ! Nous en avons tous un certain nombre, en particulier si vous accédez régulièrement à des sites Web ou utilisez des applications qui nécessitent une connexion. L'utilisateur lambda soit utilise le même mot de passe pour toutes les applications et tous les sites Web, soit fait preuve d'une grande créativité mais oublie rapidement quel mot de passe s'applique à quelle application.

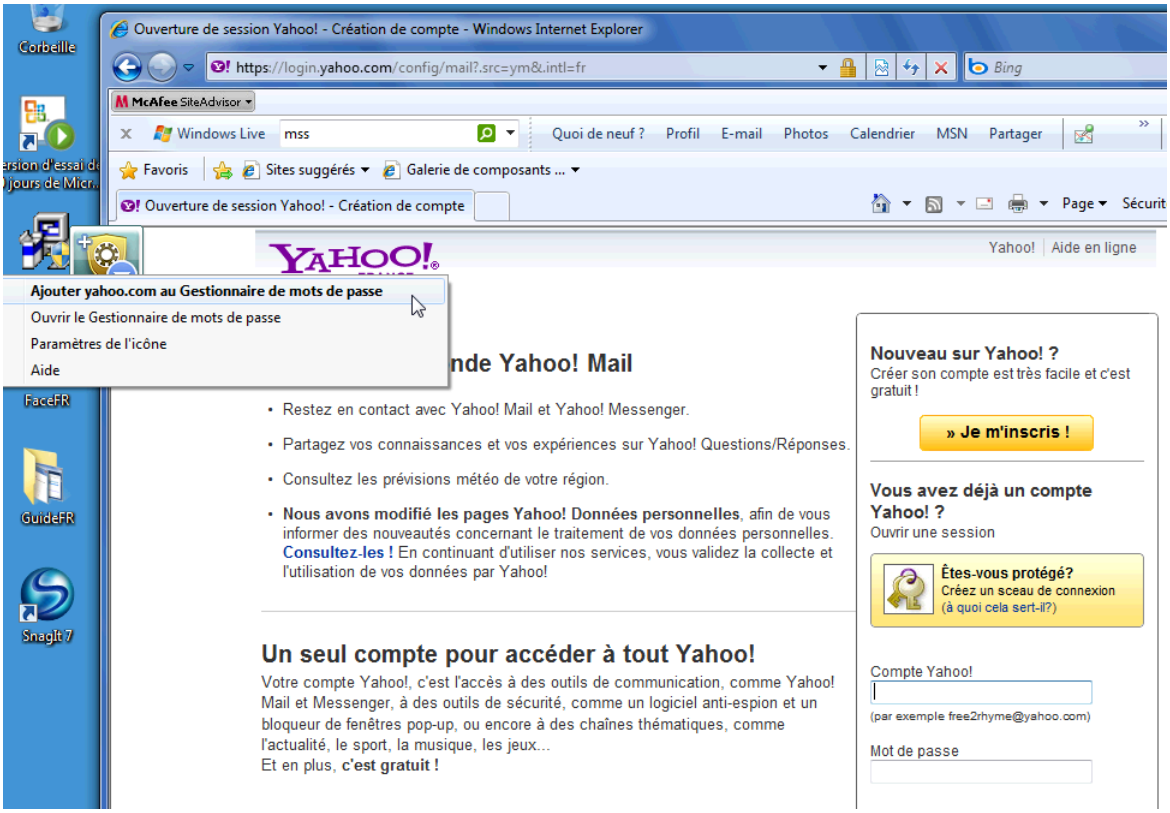
Ne serait-il pas agréable qu'un logiciel mémorise automatiquement vos mots de passe d'accès aux sites qui ne sont pas critiques ou vous donne la possibilité de distinguer les sites à mémoriser de ceux à omettre ? Credential Manager for HP ProtectTools est la solution. Credential Manager est en effet le gestionnaire de mots de passe qui vous donne cette possibilité. Une fois que vous êtes connecté au PC, Credential Manager vous fournit vos mots de passe et informations d'authentification en fonction des besoins.

Lorsque vous accédez à une application ou à un site Web nécessitant des informations d'authentification, Credential Manager reconnaît automatiquement le site et vous demande si vous

souhaitez que le logiciel mémorise vos informations. Si vous acceptez, vous n'aurez plus jamais besoin de vous souvenir de ce mot de passe. Vous pouvez décliner la proposition de mémoriser vos informations si vous souhaitez exclure certains sites.

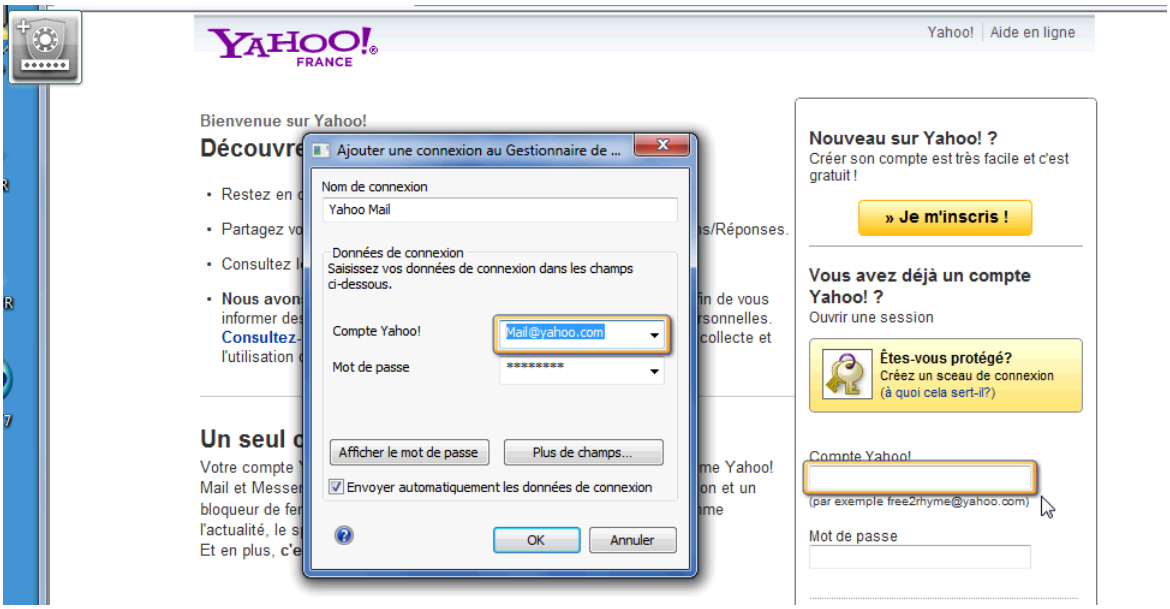
Pour commencer à enregistrer des emplacements, des noms d'utilisateur et des mots de passe, procédez comme suit :

1. Par exemple, accédez à votre compte de messagerie Web et demandez à Credential Manager (cliquez sur l'icône) d'ajouter l'authentification Web.



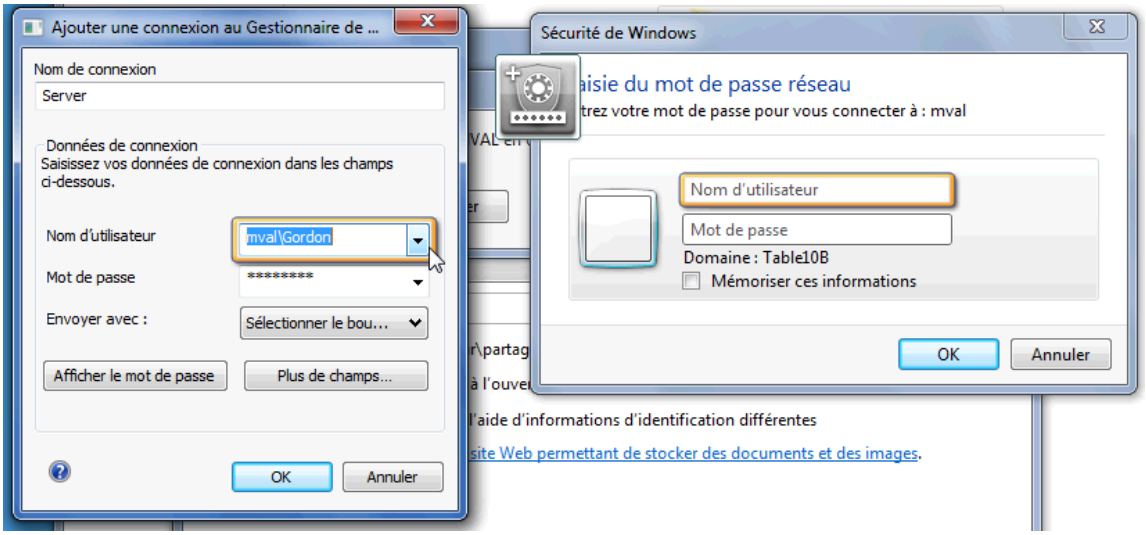
2. Nommez le lien (facultatif) et entrez un nom d'utilisateur et un mot de passe dans Credential Manager.

REMARQUE : La page Web va mettre en surbrillance les zones que Credential Manager va utiliser maintenant et lors des visites ultérieures.



3. Lorsque vous avez fini, cliquez sur le bouton **OK**.

4. Credential Manager peut également enregistrer vos noms d'utilisateur et mots de passe pour les partages réseau ou le mappage des unités réseau.



Affichage et gestion des authentifications enregistrées dans Credential Manager

Credential Manager présente l'avantage de vous permettre d'afficher, de gérer, de sauvegarder et de lancer vos authentifications à partir d'un emplacement central. Credential Manager prend également en charge le lancement des sites enregistrés à partir de Windows.

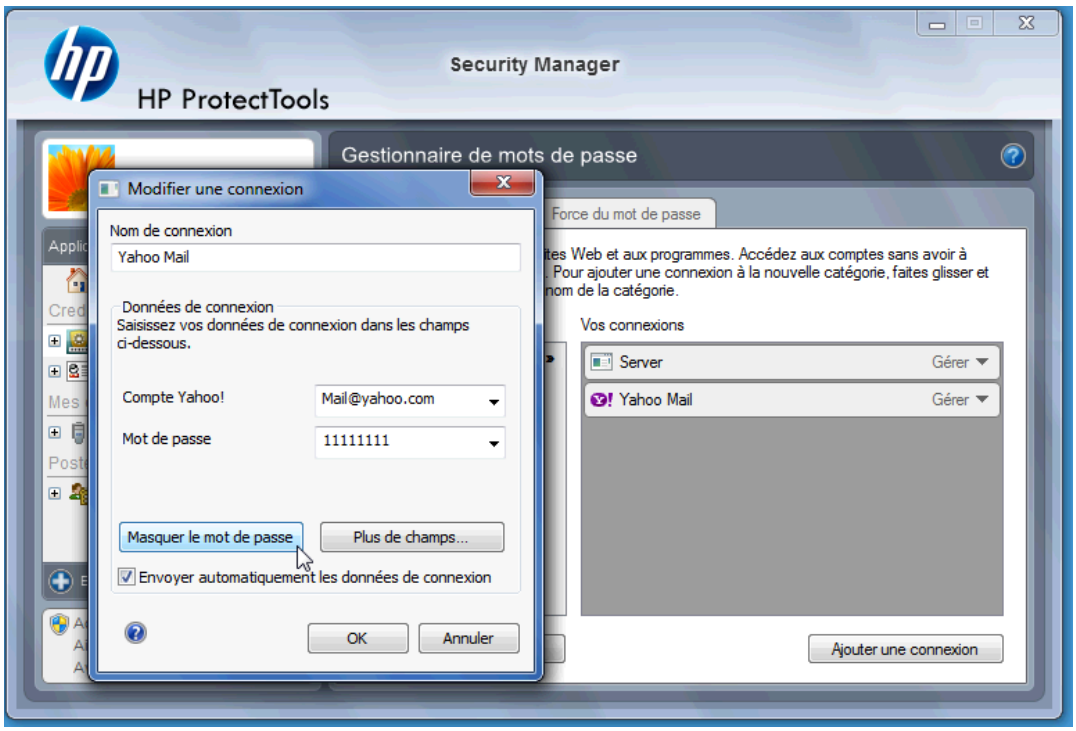
Pour ouvrir le Gestionnaire de mots de passe, utilisez l'une des deux méthodes suivantes :

- Utilisez la combinaison de touches Ctrl + Windows + H pour ouvrir le Gestionnaire de mots de passe. La sélection de l'option **Ouvrir** lance et authentifie rapidement le raccourci enregistré.

OU

- Sélectionnez l'onglet **Gérer** dans le Gestionnaire de mots de passe pour ouvrir HP ProtectTools Security Manager où les informations d'authentification peuvent être modifiées.

L'option **Modifier** de Credential Manager vous permet d'afficher et de modifier le nom, le nom de connexion et même de révéler les mots de passe.



HP ProtectTools for Small Business permet également la sauvegarde et/ou la copie de tous les paramètres et informations d'authentification sur un autre PC.

File Sanitizer for HP ProtectTools

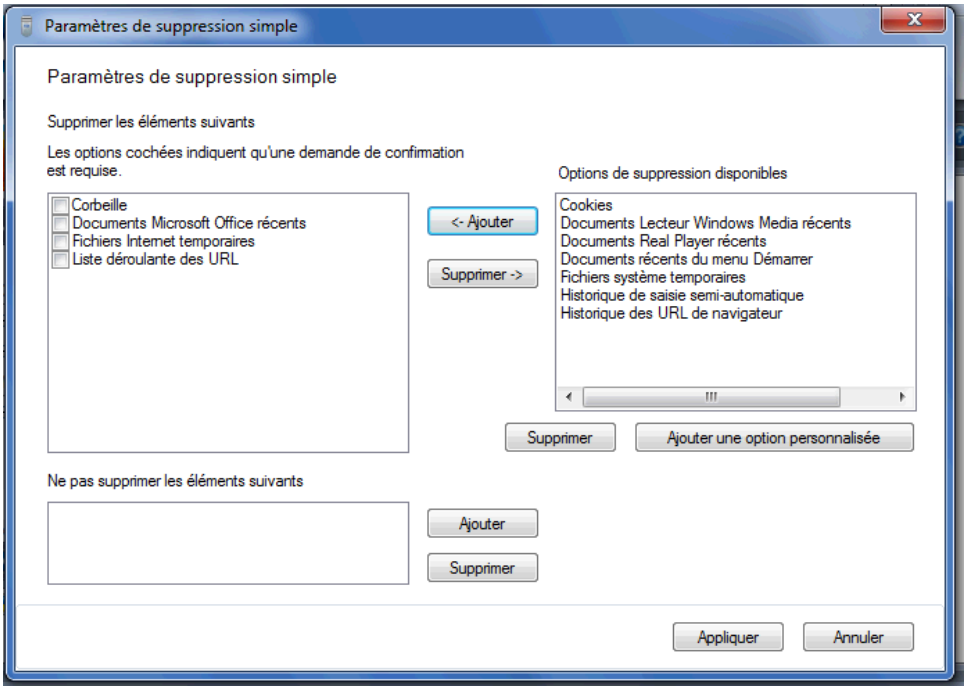
File Sanitizer est conçu pour rendre extrêmement difficile à une personne non autorisée de récupérer les données que vous avez supprimées. Plusieurs options sont disponibles pour vous permettre d'effacer manuellement les données ou d'établir une planification régulière afin d'effacer les fichiers et dossiers sélectionnés, y compris l'historique du navigateur.

Vous trouverez ci-après quelques paramètres de configuration simple.

Pour commencer à supprimer définitivement les données que vous avez effacées, sélectionnez les fichiers ou dossiers dont vous n'avez plus besoin.

1. Accédez à **Security Manager** > **File Sanitizer** > **Paramètres**. Sélectionnez **Paramètres de suppression simple** et cliquez sur le bouton **Détails**.

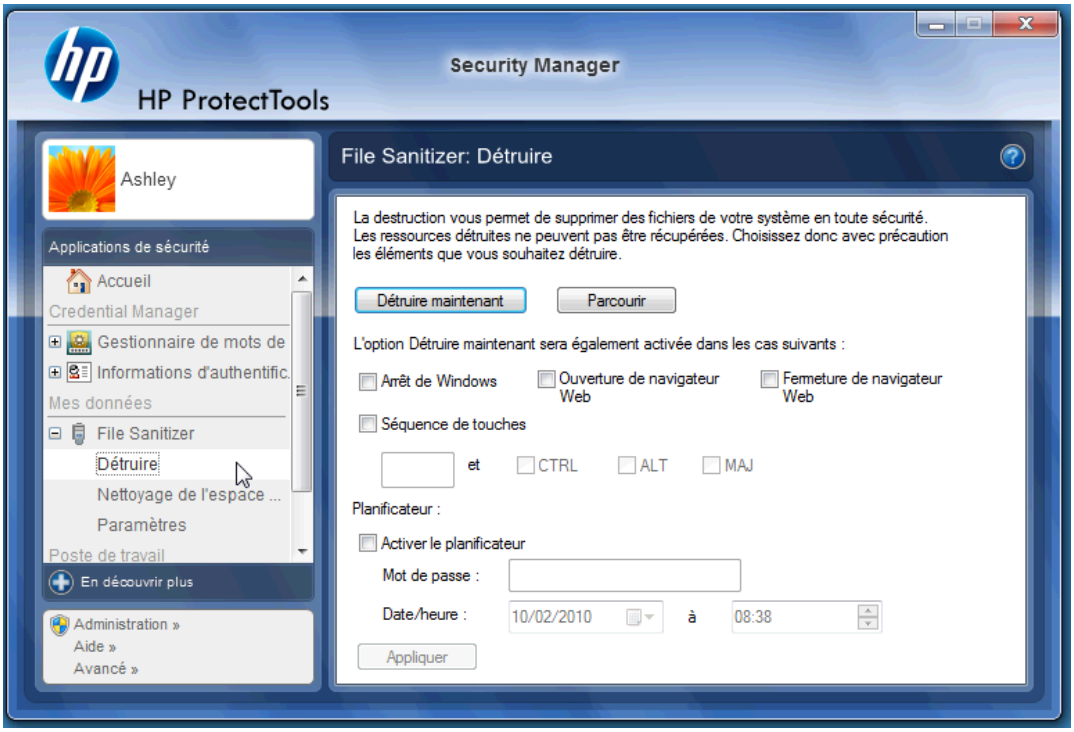
2. Sélectionnez du côté droit de la fenêtre Paramètres de suppression simple les éléments que vous voulez supprimer définitivement de manière régulière, puis cliquez sur le bouton **<- Ajouter** pour déplacer les éléments sélectionnés vers le côté des éléments à supprimer.



3. Commencez par la Corbeille et ajoutez les autres éléments que vous voulez effacer par destruction.

4. Cliquez sur le bouton **Appliquer** lorsque vous avez sélectionné tous les éléments que vous voulez effacer définitivement.

5. Accédez à l'option **Détruire** et configurez le moment voulu pour l'exécution de l'action. Le bouton **Détruire maintenant** efface immédiatement les éléments sélectionnés dans la fenêtre Paramètres de suppression simple que vous venez de configurer.



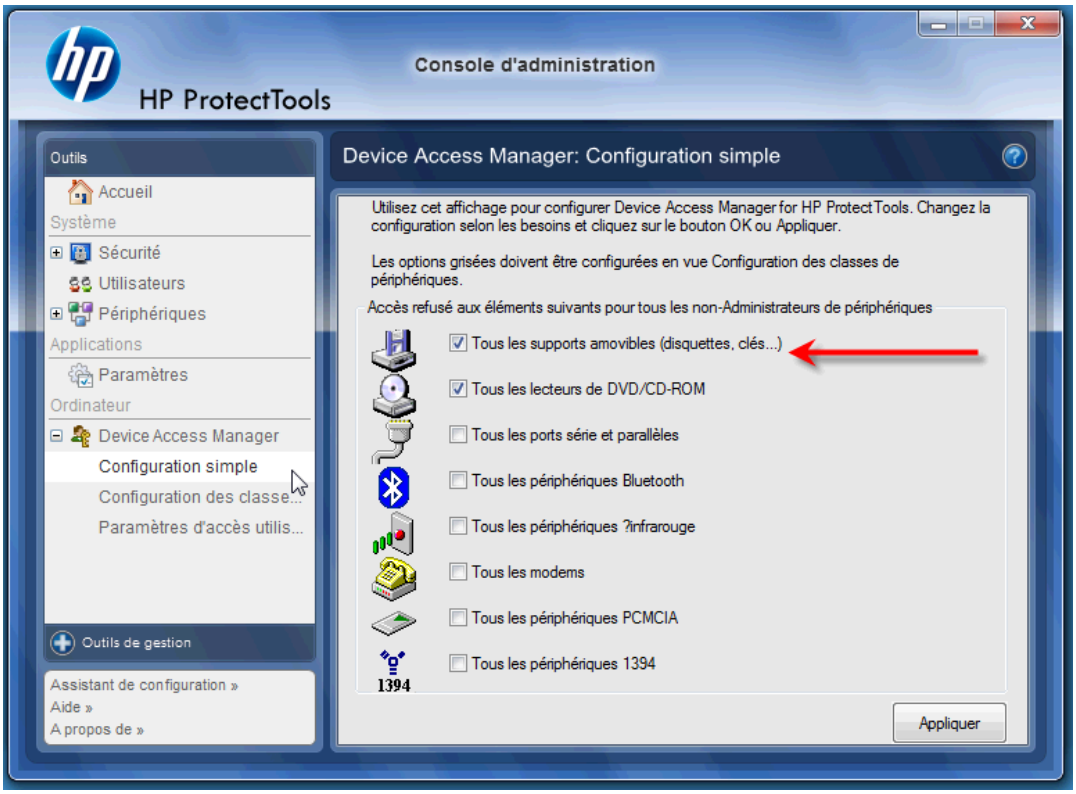
6. Une petite info-bulle s'affiche dans la barre des tâches à chaque fois que l'action Détruire est démarrée et terminée.

Device Access Manager for HP ProtectTools

Vous pouvez utiliser Device Access Manager pour limiter l'utilisation de divers périphériques de stockage internes et externes afin que vos données restent sécurisées sur le disque dur et ne sortent pas de votre entreprise. Par exemple, vous pouvez autoriser un utilisateur à accéder à vos données mais l'empêcher de les copier sur un CD, un lecteur de musique personnel ou un périphérique de mémoire USB. Voici un moyen facile de configurer cette action :

1. Cliquez sur **Démarrer** > **Tous les programmes** > **HP** > **Console d'administration** > **Device Access Manager** > **Configuration simple**.

2. Sélectionnez les périphériques matériels auxquels vous voulez limiter l'accès, puis cliquez sur le bouton **Appliquer** pour terminer le processus.

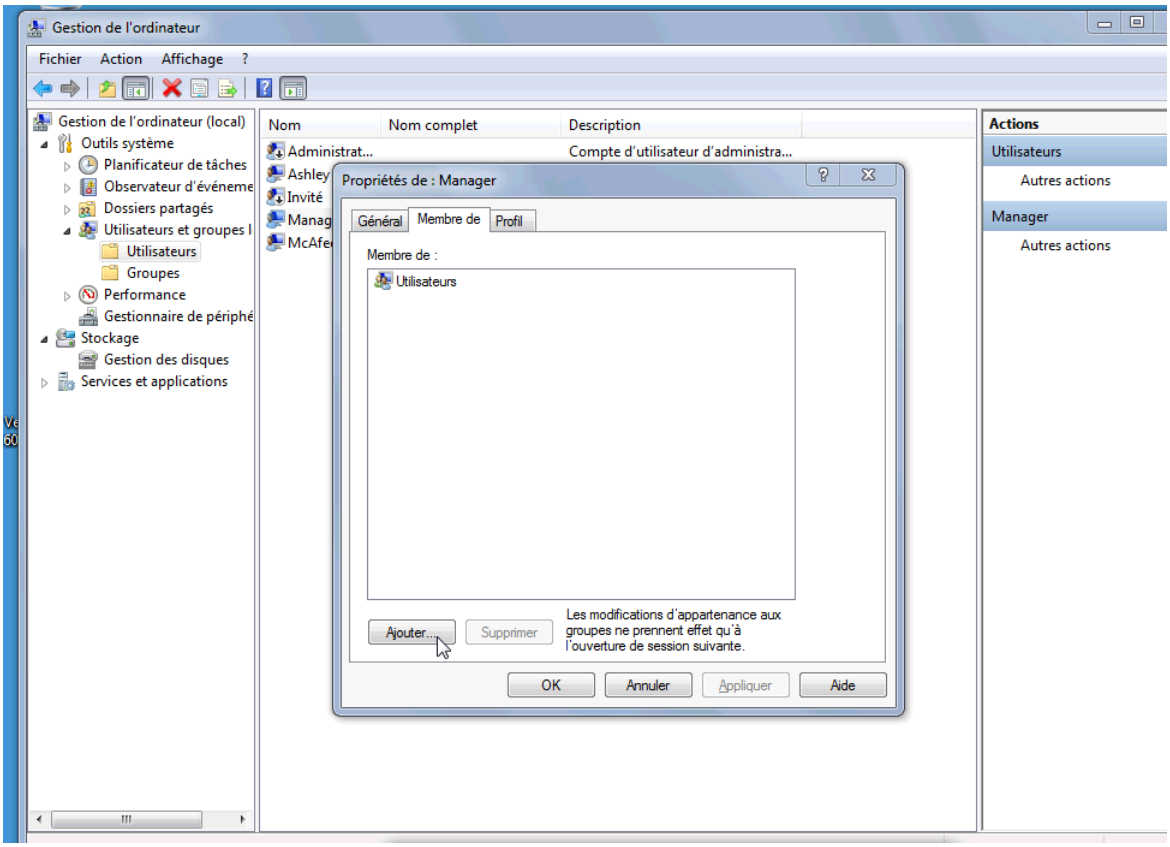


3. L'étape suivante présentée ci-dessous consiste à sélectionner les personnes qui continuent à avoir accès aux périphériques tandis que toutes les autres sont bloquées.

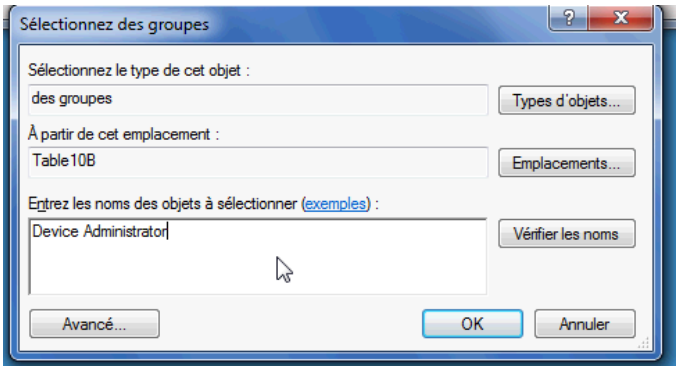
4. Accédez à **Poste de travail**, sélectionnez-le, cliquez avec le bouton droit de la souris et sélectionnez **Gérer** > **Gestion de l'ordinateur** > **Outils système** > **Utilisateurs et groupes locaux** > **Utilisateurs**.

5. Double-cliquez sur l'utilisateur (dans cet exemple, « Manager ») pour lequel vous voulez conserver l'accès au matériel bloqué.

6. Sous l'onglet **Membre de**, cliquez sur le bouton **Ajouter**.



7. Dans la fenêtre **Sélectionnez des groupes**, vous pouvez utiliser l'option **Avancé** ou vous contenter de saisir le groupe « Device Administrators ». Cliquez sur le bouton **OK**, puis finissez de fermer la fenêtre en cliquant sur les boutons OK. Vous devez vous déconnecter, puis vous reconnecter pour obtenir les autorisations.



Dorénavant, tous les périphériques de stockage internes et externes, y compris les lecteurs de CD, les lecteurs USB, les lecteurs de musique personnels, etc., ne fonctionneront plus que pour les personnes incluses dans le groupe « Device Administrators ».

Drive Encryption for HP ProtectTools

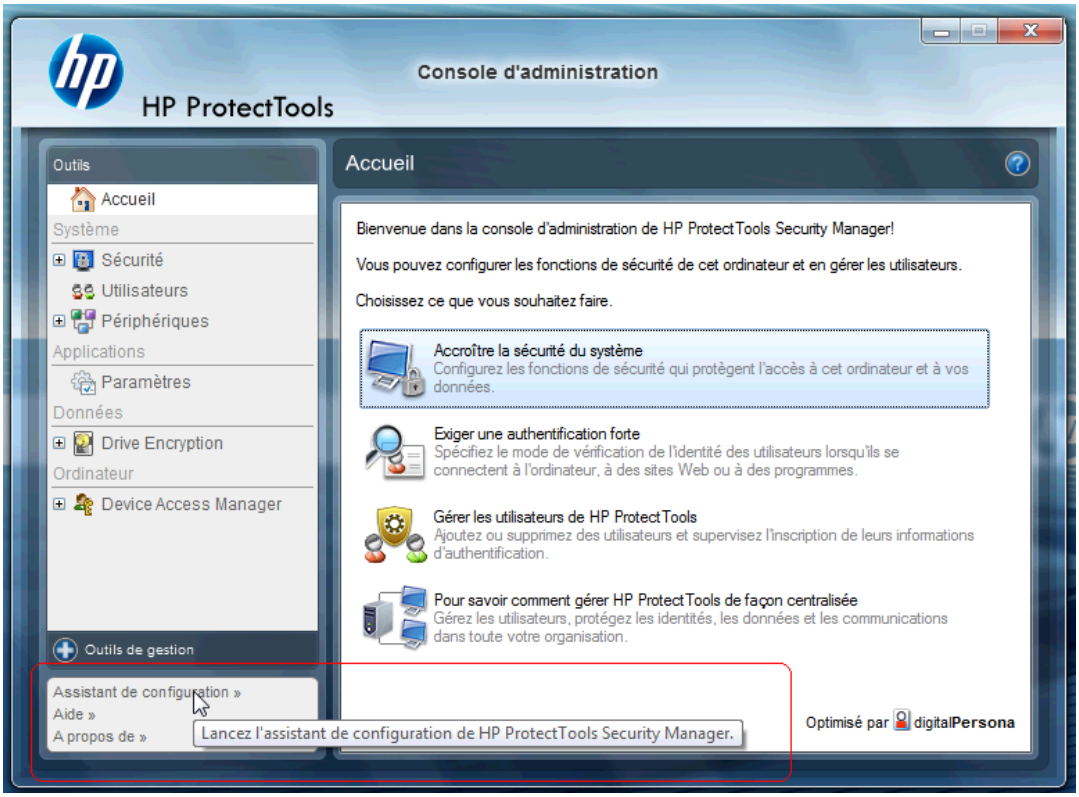
Le logiciel Drive Encryption for HP ProtectTools protège les données en chiffrant l'intégralité du disque dur. Les données sur le disque dur seraient ainsi protégées si l'ordinateur venait à être volé ou si le disque dur était retiré du système d'origine et placé dans un autre système.

Autre avantage de sécurité : Drive Encryption vous oblige à vous authentifier à l'aide de votre nom d'utilisateur et de votre mot de passe avant d'initialiser le système. Ce processus est appelé « authentification préliminaire ».

Afin de vous faciliter la tâche, les utilisateurs de Windows, les domaines, Credential Manager pour HP ProtectTools et HP ProtectTools Security Manager communiquent avec Drive Encryption afin de faciliter la synchronisation du mot de passe.

Procédez comme suit pour activer Drive Encryption for HP ProtectTools.

1. Cliquez sur **Démarrer** > **Tous les programmes** > **HP** > **Console d'administration de HP ProtectTools** > **Outils de gestion** > **Assistant de configuration**. L'écran suivant apparaît :



2. Sélectionnez **Suivant** dans l'écran de bienvenue.
3. Vous devez entrer votre mot de passe Windows pour démarrer l'Assistant d'activation > **Suivant**.
4. Cochez la case **Drive Encryption** et sélectionnez **Suivant**.

5. La fenêtre de configuration de Drive Encryption ci-dessous répertorie les lecteurs pouvant être chiffrés. Un lecteur Flash USB est nécessaire pour stocker la clé de récupération de chiffrement. Conservez cette clé dans un endroit sûr. Vous en aurez besoin pour récupérer les données ou accéder au lecteur au cas où le mot de passe de pré-initialisation venait à être perdu ou échouait.

6. Sélectionnez **Suivant**, terminez le processus, puis sélectionnez **Terminer**. Lorsque vous y êtes invité, retirez le lecteur Flash USB, puis redémarrez le système.

7. Au redémarrage du système sur le disque dur, Drive Encryption exige le mot de passe Windows. Entrez le mot de passe, puis cliquez sur **OK**.

REMARQUE : L'ordinateur peut être lent pendant le chiffrement du lecteur. Il s'exécutera de nouveau normalement une fois le lecteur entièrement chiffré. Les données du lecteur sont chiffrées et déchiffrées au fur et à mesure, selon les besoins.

Par ailleurs, l'authentification Drive Encryption établit un lien direct entre la connexion Windows de Credential Manager et le Bureau, sans que vous ayez à entrer de nouveau votre mot de passe.

3 Avantages de HP ProtectTools for Small Business

Accès au logiciel de sécurité HP ProtectTools for Small Business

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**.

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 :

- 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

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 administrateurs 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 49.

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 :
  - Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) à la page 36
  - Drive Encryption for HP ProtectTools à la page 33
- Credential Manager for HP ProtectTools permet de 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 :
  - Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) à la page 36
- Device Access Manager for HP ProtectTools permet aux administrateurs 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 48
- 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 41

Création de stratégies de mot de passe fort

Si vous avez besoin d'utiliser une stratégie de mot de passe fort (c'est-à-dire un mot de passe compliqué difficile à usurper) pour des douzaines d'applications Web et de bases de données, Credential Manager for HP ProtectTools fournit un référentiel protégé pour les mots de passe et l'authentification unique. Consultez le chapitre suivant :

- Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) à la page 36

Éléments de sécurité supplémentaires

Affectation de rôles de sécurité

Pour protéger correctement les données, 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 entreprise ou pour une utilisation individuelle, ces rôles peuvent être tenus par la même personne.

Pour HP ProtectTools for Small Business, les responsabilités et les privilèges de sécurité peuvent être répartis entre les rôles suivants :

- Administrateur : applique et gère les fonctions de sécurité. Peut également activer et désactiver certaines fonctions.
- Utilisateur : utilise les fonctions de sécurité.

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 définis et utilisés par les administrateurs uniquement sont également indiqués dans ce tableau. Tous les autres mots de passe peuvent être définis par les utilisateurs lambda.

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 Computer Setup **REMARQUE :** Également appelé mot de passe de l'administrateur du BIOS, de configuration F10 ou de configuration de la sécurité	BIOS, par l'administrateur	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 pour la connexion manuelle.

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

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.

4 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** : fournit les outils permettant de sauvegarder et de récupérer les clés de chiffrement.
- **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.
  - **A propos de** : affiche les informations relatives à Security Manager, y compris le numéro de version et la mention de droits d'auteur.

Mise en route avec 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. Cependant, la console d'administration de HP ProtectTools Security Manager permet également 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

Pour spécifier les informations d'authentification requises pour accéder à l'ordinateur 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 en regard 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**.

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 en regard 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 a été effectuée au niveau du BIOS.

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 comparées 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 des connexions. 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.

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.

△ **ATTENTION :** Vous devez sauvegarder les clés de chiffrement sur un lecteur Flash USB et conserver ce périphérique dans un endroit sûr. Si vous oubliez votre mot de passe, ce périphérique constituera votre seul moyen d'accès à votre disque dur.

Pour plus d’informations sur l’utilisation de Drive Encryption for HP ProtectTools, consultez la section Drive Encryption for HP ProtectTools à la page 33.

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 48.

5 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
- Détruire ou nettoyer le disque dur
- Afficher l'état du cryptage de l'unité
- Afficher les paramètres d'accès au périphérique
- Sauvegarder et restaurer les données de Security Manager

Gestion de mots de passe

Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) crée et gère des connexions, ce qui vous permet de lancer des sites Web et des programmes et de 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 Credential Manager for HP ProtectTools (Gestionnaire de mots de passe) à la page 36.

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 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**.

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 41.

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.

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 dans un fichier chiffré 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 chiffré 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.

6 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.

Le logiciel Drive Encryption for HP ProtectTools chiffre votre disque dur afin de protéger l'ensemble de vos données. Lorsqu'il est activé, vous devez vous connecter sur l'écran de connexion de Drive Encryption qui s'affiche avant le démarrage de Windows.

Drive Encryption n'empêche pas les accès non autorisés au cours d'une même session de Windows. Une fois l'ordinateur démarré et vos nom d'utilisateur et mot de passe entrés, n'importe quel utilisateur du système peut accéder aux données sur l'unité, bien qu'elles soient toujours chiffrées. Assurez-vous de protéger votre session Windows par mot de passe lorsque vous vous éloignez de l'ordinateur.

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 Dictionary Attack.

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

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

- Gestion de Drive Encryption
  - Crypter ou décrypter des unités individuelles
- Sauvegarde et récupération
  - Créer des clés de sauvegarde
  - Exécuter une restauration

△ **ATTENTION :** Vous devez sauvegarder les clés de chiffrement sur un lecteur Flash USB et conserver ce périphérique dans un endroit sûr. Si vous oubliez votre mot de passe, ce périphérique constituera votre seul moyen d'accès à votre disque dur.

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. Sinon, vous ne pourrez plus accéder aux données sur les unités chiffrées. 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.

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.

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 : Veillez à conserver dans un endroit sûr le périphérique de stockage contenant la clé de sauvegarde. Si vous oubliez votre mot de passe, ce périphérique représentera votre seul et unique moyen d'accès 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.

7 Credential Manager for HP ProtectTools (Gestionnaire de mots de passe)

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 que vous saisissez 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 un accès encore plus rapide, vous pouvez afficher un menu de vos connexions à l'aide d'une simple combinaison de touches de raccourci configurable (par défaut, Ctrl + Windows + H). Dans ce 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 for Small Business, comme votre mot de passe Windows. 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 ni de retenir, et vos comptes sont plus sécurisés.

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 et 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 [nomdedomaine.com] au Gestionnaire de mots de passe : permet d'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 : permet d'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.

Ajout de connexions

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.

8 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 d'historique 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 de fichiers et/ou de dossiers sous Windows ne supprime pas totalement le contenu de votre disque dur. Windows supprime uniquement les références. Le contenu reste sur le disque dur jusqu'à ce qu'un autre fichier écrase la même zone du disque dur avec de nouvelles informations.

La destruction est différente de la suppression Windows standard (également appelée suppression simple dans File Sanitizer) car lorsque vous détruisez des données, il devient pratiquement impossible de récupérer celles-ci.

Lorsque vous choisissez un profil de destruction (Haute sécurité, Sécurité moyenne ou Sécurité basse), une liste prédéfinie de fichiers et/ou de dossiers 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 fichiers à inclure dans la destruction, les fichiers nécessitant une confirmation avant destruction et les fichiers à exclure de la destruction.

Vous pouvez configurer une planification de destruction automatique et vous pouvez également détruire manuellement des fichiers et/ou dossiers quand 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 fichiers supprimés, ce qui empêche les utilisateurs de visualiser le contenu initial des fichiers supprimés.

REMARQUE : Le nettoyage de l'espace libre concerne les fichiers que vous supprimez à l'aide de la Corbeille Windows ou que vous supprimez manuellement. Il ne fournit aucune sécurité supplémentaire pour les fichiers détruits.

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

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** : sélectionnez cette option pour détruire tous les fichiers sélectionnés à l'arrêt de Windows.

     REMARQUE : Lorsque cette option est sélectionnée, une boîte de dialogue s'affiche quand vous arrêtez Windows et vous demande si vous souhaitez poursuivre la destruction des fichiers sélectionnés 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** : sélectionnez cette option pour détruire tous les fichiers liés au Web sélectionnés, tels que l'historique des URL du navigateur, lorsque vous ouvrez un navigateur Web.

- **Fermeture de navigateur Web** : sélectionnez cette option pour détruire tous les fichiers liés au Web sélectionnés, tels que l'historique des URL du navigateur, lorsque vous fermez 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, entrez votre mot de passe Windows, puis entrez le jour et l'heure de destruction des fichiers sélectionnés.

3. Cliquez sur l'icône **Enregistrer**.

Sélection ou création d'un profil de destruction

Vous pouvez spécifier une méthode d'effacement et sélectionner les fichiers et/ou dossiers à détruire en sélectionnant un profil prédéfini ou en créant le vôtre.

Sélection d'un profil de destruction prédéfini

Lorsque vous choisissez un profil de destruction prédéfini (Haute sécurité, Sécurité moyenne ou Sécurité basse), une méthode d'effacement et une liste de fichiers prédéfinies sont automatiquement sélectionnées. Vous pouvez cliquer sur le bouton Détails pour afficher la liste prédéfinie des fichiers qui sont sélectionnés pour être détruits.

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 des fichiers qui sont sélectionnés pour être détruits.
4. Sous **Détruire les éléments suivants**, cochez la case en regard de chaque fichier pour lequel vous souhaitez une confirmation avant 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 fichiers à inclure dans la destruction, les fichiers nécessitant une confirmation avant destruction et les fichiers 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 **Détails**.
2. Spécifiez le nombre de cycles de destruction.

REMARQUE : Le nombre de cycles de destruction sélectionné sera exécuté pour chaque fichier. Par exemple, si vous définissez 3 cycles de destruction, un algorithme qui efface les données est exécuté trois fois. Si vous choisissez un nombre élevé de cycles de destruction, la destruction peut prendre beaucoup de temps, néanmoins plus le nombre de cycles de destruction est élevé et plus l'ordinateur est sécurisé.

3. Sélectionnez les ressources à détruire :

   a. Sous **Options de destruction disponibles**, cliquez sur un fichier, puis sur **Ajouter**.

   b. Pour ajouter un fichier personnalisé, 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 le fichier personnalisé, puis sur **Ajouter**.

   REMARQUE : Pour supprimer un fichier des options de destruction disponibles, cliquez sur ce fichier, puis sur **Supprimer**.

4. Sous **Détruire les éléments suivants**, cochez la case en regard de chaque fichier pour lequel vous souhaitez une confirmation avant destruction.

REMARQUE : Pour supprimer un fichier de la liste des éléments à détruire, cliquez sur ce fichier, puis sur **Supprimer**.

5. Sous **Ne pas détruire les éléments suivants**, cliquez sur **Ajouter** pour sélectionner les fichiers spécifiques que vous souhaitez 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 de fichier standard sans destruction. Lorsque vous personnalisez un profil de suppression simple, vous spécifiez les fichiers à inclure dans la suppression simple, les fichiers nécessitant une confirmation avant l'exécution de la suppression simple et les fichiers 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 **Détails**.

2. Sélectionnez les fichiers à supprimer :

   a. Sous **Options de suppression disponibles**, cliquez sur un fichier, puis sur **Ajouter**.

   b. Pour ajouter un fichier personnalisé, 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 le fichier personnalisé, puis sur **Ajouter**.

   REMARQUE : Pour supprimer un fichier des options de suppression disponibles, cliquez sur ce fichier, puis sur **Supprimer**.

3. Sous **Supprimer les éléments suivants**, cochez la case en regard de chaque fichier pour lequel vous souhaitez une confirmation avant suppression.

REMARQUE : Pour supprimer un fichier de la liste des éléments à supprimer, cliquez sur ce fichier, puis sur **Supprimer**.

4. Sous **Ne pas supprimer les éléments suivants**, cliquez sur **Ajouter** pour sélectionner les fichiers spécifiques que vous souhaitez exclure de la suppression.

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 fichiers détruits ne peuvent pas être récupérés. Sélectionnez donc avec précaution les éléments que vous souhaitez détruire manuellement.

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

Destruction manuelle d'une ressource

△ **ATTENTION :** Les fichiers détruits ne peuvent pas être récupérés. Sélectionnez donc avec précaution les éléments que vous souhaitez détruire manuellement.

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, accédez au fichier à détruire, puis cliquez sur **Ouvrir**.

REMARQUE : Le fichier sélectionné peut être un fichier simple ou un dossier.

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, accédez au fichier 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, accédez au fichier 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

9 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 en 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 en arrière-plan. Cliquez sur **Oui** pour démarrer le service en 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**.

Glossaire

administrateur :
Voir : administrateur Windows.

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

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 exige une certaine forme d'authentification, par exemple un mot de passe, lorsque l'ordinateur est mis sous tension.

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.

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.

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'authentification :
Méthode selon laquelle un utilisateur prouve son habilitation à effectuer une tâche spécifique dans le processus d'authentification, par exemple, un nom d'utilisateur et un mot de passe.

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

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

nettoyage de l'espace libre :
Écriture sécurisée de données aléatoires par-dessus les fichiers supprimés du disque dur afin de déformer le contenu des fichiers supprimés, ce qui rend la récupération des données plus difficile.

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

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.

séquence de touches :
Combinaison de touches spécifique dont l'utilisation permet de démarrer une destruction automatique ; par exemple Ctrl+Alt+S.

suppression simple :
Suppression sécurisée des informations sensibles, notamment les fichiers, l'historique ou le contenu Web, ou d'autres données confidentielles.

Index

A

accès
  contrôle 48
  protection contre un accès non autorisé 19
accès à HP ProtectTools Security Manager 18
accès non autorisé, protection 19
assistant de configuration
  administrateurs 23

B

BIOS, mot de passe administrateur 20

C

chiffrement d'une unité 33
Computer Setup
  mot de passe administrateur 20
configuration de sécurité, mot de passe 20
configuration des utilisateurs 23
configuration initiale 23
connexion Windows
  mot de passe 20
console d'administration de HP ProtectTools Security Manager
  configuration des paramètres des applications 27
  configuration de votre système 24
  fonctions 2
  gestion des utilisateurs 25
  présentation 1
  rejet d'accès au périphérique 27
Console d'administration de HP ProtectTools Security Manager
  cryptage de l'unité 27
contrôle de l'accès au périphérique 48
Credential Manager for HP ProtectTools (Gestionnaire de mots de passe)
  affichage et gestion des authentifications enregistrées 8
  ajout de connexions 37
  catégories de connexion 39
  configuration simple 6
  fonctions 2
  force du mot de passe 40
  gestion des connexions 39
  modification de connexions 38
  mot de passe de connexion 20
  paramètres de l'icône 40
  utilisation du menu Connexions 38

D

déchiffrement d'une unité 33
Device Access Manager for HP ProtectTools
  ajout d'un utilisateur ou groupe 49
  configuration de classes de périphériques 49
  configuration simple 14, 48
  fonctions 3
  service en arrière-plan 48
  suppression d'un utilisateur ou groupe 49
  utilisateur ou groupe, refus d'accès à 50
données, restriction de l'accès 18
Drive Encryption for HP ProtectTools
  activation 34
  chiffrement d'une unité 34
  configuration simple 16
  connexion après activation de Drive Encryption 34
  création de clés de sauvegarde 35
  déchiffrement d'une unité 34
  désactivation 34
  gestion de Drive Encryption 34
  ouverture 34
  sauvegarde et restauration 35

F

F10, mot de passe de configuration de touche 20
File Sanitizer 45
File Sanitizer for HP ProtectTools
  activation manuelle du nettoyage de l'espace libre 46
  affichage des fichiers journaux 47
  annulation d'une opération de destruction ou de nettoyage de l'espace libre 46
  configuration d'une planification de nettoyage 42
  configuration simple 11
  définition d'une planification de destruction 42
  destruction 41

destruction manuelle d'une ressource 45
destruction manuelle de tous les éléments sélectionnés 46
fonctions 3
nettoyage 41
ouverture 42
procédures de configuration 42
profil de destruction 43
profil de destruction (sélection ou création) 43
profil de destruction prédéfini 43
profil de suppression simple 44
utilisation d'une séquence de touches pour démarrer la destruction 45
utilisation de l'icône File Sanitizer 45
fonctions HP ProtectTools 2

G
Guide de configuration simple 4

H
HP ProtectTools, fonctions 2
HP ProtectTools Security Manager
accès au périphérique 29
ajout d'applications 30
configuration d'informations d'authentification 28
destruction ou nettoyage des fichiers 29
état du cryptage de l'unité 29
fonctions 2
gestion de mots de passe 28
modification de votre image 31
modification de votre nom d'utilisateur Windows 31
préférences 30
présentation 1
sauvegarde et restauration 30
HP ProtectTools Security Manager, accès 18

I
Initiation 4

M
mise sous tension, mot de passe
définition 20
modification de votre mot de passe Windows 28
mot de passe
gestion 20
HP ProtectTools 20
instructions 20
sécurisé, création 20
stratégies, création 19

O
objectifs de sécurité 18
objectifs de sécurité fondamentaux 18

P
profil de destruction
personnalisation 43
prédéfini 43
sélection ou création 43
profil de suppression simple
personnalisation 44

R
restriction
accès à des données confidentielles 18
accès au périphérique 48

S
sauvegarde et restauration 30
sécurité
assistant de configuration 23
méthodes de connexion 23
niveaux 23
objectifs fondamentaux 18
rôles 19
service en arrière-plan, Device Access Manager 48

T
tâches avancées
Device Access Manager 49